ASDM ブック 1：Cisco ASA シリーズ ASDM 7.14 コンフィギュレーション ガイド（一般的な操作）

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

本書の目的

このマニュアルの目的は、Adaptive Security Device Manager（ASDM）を使用して、Cisco ASA シリーズ用の一般的な動作の設定を支援することです。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。各 ASA のバージョンでサポートされている ASDM の最小バージョンについては、『*Cisco ASA Series Compatibility*』を参照してください。

関連資料

詳細については、『*Navigating the Cisco ASA Series Documentation*』（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタン ラベル、フィールド名、およびユーザー入力テキストは、**boldface**で示しています。メニューベース コマンドの場合は、メニュー項目を [ ] で囲み、コマンドのフル パスを示しています。
italic	ユーザーが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアル タイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[ ]	角かっこの中の要素は、省略可能です。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
[ ]	システム プロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
< >	パスワードなどの出力されない文字は、山カッコ（< >）で囲んで示しています。
!、#	コードの先頭に感嘆符（!）または番号記号（#）がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント	「問題解決に役立つ情報」です。
注意	「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。
ワンポイント アドバイス	時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	**「警告」の意味です。人身事故を予防するための注意事項が記述されています。**

通信、サービス、およびその他の情報

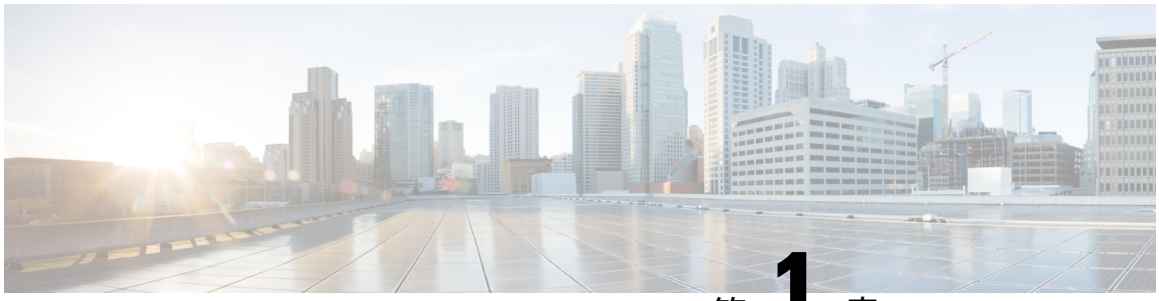
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

第 部

ASA の開始



第 1 章

Cisco ASA の概要

Cisco ASA は、追加モジュールとの統合サービスに加え、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティコンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ3）ファイアウォール オペレーション、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。ASA の各バージョンでサポートされている ASDM の最小バージョンについては、『Cisco ASA Compatibility（Cisco ASA の互換性）』[英語] を参照してください。特殊なサービス非推奨のサービスおよびレガシー サービス （14 ページ） も参照してください。

ASDM 要件

ASDM Java の要件

ASDM は、Oracle JRE 8.0（**asdm-*version*.bin**）または OpenJRE 1.8.x（**asdm-openjre-*version*.bin**）を使用してインストールできます。

（注） ASDM は Linux ではテストされていません。

表 *1*：*ASA* と *ASA FirePOWER*：*ASDM* オペレーティング システムとブラウザの要件

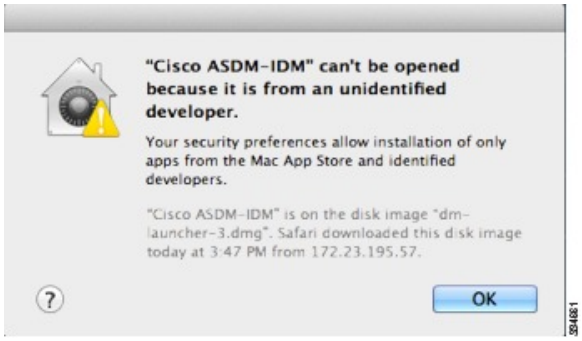
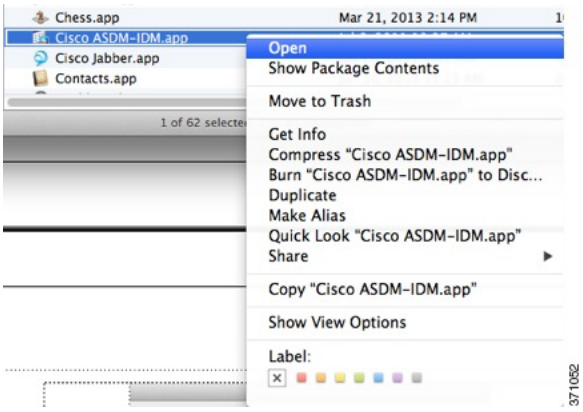
オペレーティング システム	ブラウザ				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
• Microsoft Windows（英語および日本語）： • 10 （注） ASDM ショートカットに問題がある場合は、ASDM の互換性に関する注意事項 （3 ページ）の「Windows 10」を参照してください。 • 8 • 7 • Server 2016 と Server 2019（ASA 管理のみ。FirePOWER モジュールの ASDM 管理はサポートされていません。その代わりに、ASA 管理に ASDM を使用しているときは、Firepower Management Center を使用して FirePOWER モジュールを管理できます。） • Server 2012 R2 • Server 2012 • Server 2008	対応	対応	サポートなし	対応	8.0	1.8 （注） Windows 7 32 ビットのサポートなし

オペレーティング システム	ブラウザ				Oracle JRE	OpenJRE
	Internet Explorer	Firefox	Safari	Chrome		
Apple OS X 10.4 以降	サポートなし	対応	対応	対応（64 ビット バージョンのみ）	8.0	1.8

ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

条件	注意
Windows 10	「**This app can't run on your PC**」エラー メッセージ。 ASDM ランチャをインストールすると、Windows 10 によって ASDM ショートカットターゲットが Windows Scripting Host パスに置き換えられて、このエラーが発生することがあります。ショートカットターゲットを修正するには、次の手順を実行します。 **1.** **[Start]** > **[Cisco ASDM-IDM Launcher]** を選択し、[Cisco ASDM-IDM Launcher] アプリケーションを右クリックします。 **2.** **[More]** > **[Open file location]** を選択します。 Windows は、ショートカットアイコンを使用してディレクトリを開きます。 **3.** ショートカット アイコンを右クリックして、**[Properties]** を選択します。 **4.** [Target] を次のように変更します。 **C:\Windows\System32\wscript.exe invisible.vbs run.bat** **5.** [OK] をクリックします。
OS X	OS X では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。

条件	注意
OS X 10.8 以降	ASDM は Apple Developer ID で署名されていないため、実行できるようにする必要があります。セキュリティの設定を変更しないと、エラー画面が表示されます。  1. ASDM を実行できるようにするには、[Cisco ASDM-IDM Launcher] アイコンを右クリック（または Ctrl キーを押しながらクリック）して、[Open] を選択します。  2. 同様のエラー画面が表示されますが、この画面から ASDM を起動できます。[Open] をクリックします。ASDM-IDM ランチャが起動します。 

条件	注意
ASA では強力な暗号化ライセンス（3DES/AES）が必要 （注） スマートライセンスモデルを使用すると、強力な暗号化ライセンスを使用せずに ASDM での最初のアクセスが可能になります。	ASDM では、ASA に SSL 接続する必要があります。シスコが提供している 3DES ライセンスを要求できます。 1. www.cisco.com/go/license にアクセスします。 2. [Continue to Product License Registration] をクリックします。 3. ライセンシング ポータルで、テキスト フィールドの横にある [Get Other Licenses] をクリックします。 4. ドロップダウン リストから、[IPS, Crypto, Other...] を選択します。 5. [Search by Keyword] フィールドに「ASA」と入力します。 6. [Product] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。 7. ASA のシリアル番号を入力し、プロンプトに従って ASA の 3DES/AES ライセンスを要求します。
• 自己署名証明書または信頼できない証明書 • IPv6 • Firefox および Safari	ASA が自己署名証明書または信頼できない証明書を使用する場合、Firefox と Safari では、IPv6 を介した HTTPS を使用して参照する場合にはセキュリティ例外を追加することはできません。https://bugzilla.mozilla.org/show_bug.cgi?id=633001 を参照してください。この警告は、Firefox または Safari から ASA に発信されるすべての SSL 接続に影響します（ASDM 接続を含む）。この警告を回避するには、信頼できる認証局が ASA に対して発行した適切な証明書を設定します。
• ASA で SSL 暗号化を行うには、RC4-MD5 と RC4-SHA1 を両方とも含めるか、Chrome で SSL false start を無効にする必要があります。 • Chrome	RC4-MD5 および RC4-SHA1 アルゴリズム（これらのアルゴリズムはデフォルトでイネーブル）の両方を除外するために ASA の SSL 暗号化を変更した場合、Chrome の「SSL false start」機能のために Chrome は ASDM を起動できません。これらのアルゴリズムの 1 つを再度有効にすることを推奨します（**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSL Settings]** ペインを参照）。または、Run Chromium with flags に従って **--disable-ssl-false-start** フラグを使用して Chrome の SSL false start を無効にできます。

条件	注意
サーバーの IE9	サーバーの Internet Explorer 9.0 の場合は、[Do not save encrypted pages to disk] オプションがデフォルトで有効になっています（**[Tools]** > **[Internet Options]** > **[Advanced]** を参照）。このオプションでは、最初の ASDM のダウンロードは失敗します。ASDM でダウンロードを行うには、このオプションを確実にディセーブルにしてください。

ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、『Cisco ASA Compatibility』を参照してください。

VPN の互換性

『Supported VPN Platforms, Cisco ASA Series』を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

（注） syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.14(3)/ASDM 7.15(1.150) の新機能

リリース：2021 年 6 月 15 日

このリリースに新機能はありません。

ASA 9.14(2) の新機能

リリース：**2020 年 11 月 9 日**

機能	説明
SNMP 機能	
サイト間 VPN 経由の SNMP ポーリング	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。

ASA 9.14(1.30) の新機能

リリース：**2020 年 9 月 23 日**

機能	説明
ライセンシング機能	
ASAv100 永続ライセンス予約	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。**注**：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。

ASDM 7.14(1.48) の新機能

リリース日：**2020 年 4 月 30 日**

機能	説明
プラットフォーム機能	
ASA 9.12 以前について、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活	この ASDM リリースでは、9.12 以前を実行している場合、ASA 5512-X、5515-X、5585-X、および ASASM に対するサポートが復活しました。これらのモデルの最終 ASA バージョンは 9.12 です。元の 7.13(1) リリースと 7.14(1) リリースでは、これらのモデルでの後方互換性がブロックされていましたが、このバージョンでは互換性が復活しています。

ASAv 9.14(1.6) の新機能

リリース日：**2020** 年 **4** 月 **30** 日

（注） このリリースは、ASAv でのみサポートされます。

機能	説明
プラットフォーム機能	
ASAv100 プラットフォーム	ASAv 仮想プラットフォームに、20 Gbps のファイアウォール スループット レベルを提供するハイエンド パフォーマンス モデルの ASAv100 が追加されました。ASAv100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。 ASAv100 は、VMware ESXi および KVM でのみサポートされます。

ASA 9.14(3)/ASDM 7.15(1.150) の新機能

リリース：**2021** 年 **6** 月 **15** 日

このリリースに新機能はありません。

ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザーによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザー ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバーまたは FTP サーバーなど、外部のユーザーが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによってDMZに許可されるアクセスは限定されますが、DMZにあるのは公開サーバーだけのため、この地帯が攻撃されても影響を受けるのは公開サーバーに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバーと協調するといった手段によって、内部ユーザーが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザーに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイ

スには、多数の内部インターフェイス、多数のDMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

アクセス ルールによるトラフィックの許可または拒否

アクセスルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループ インターフェイスでは、EtherType アクセス ルールを適用して、非 IP トラフィックを許可できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は、IP グラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティチェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバーへの発信アクセスを禁止できますが、このような方法でWebサイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定したり、URL およびその他のフィルタリングサービス（ASA CX や ASA FirePOWER など）を提供する ASA モジュールをインストールすることができます。ASA は、Cisco Web セキュリティ アプライアンス（WSA）などの外部製品とともに使用することも可能です。

アプリケーション インスペクションの適用

インスペクション エンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープ パケット インスペクションの実行を必要とします。

サポート対象のハードウェアモジュールまたはソフトウェアモジュールへのトラフィックの送信

一部の ASA モデルでは、ソフトウェア モジュールの設定、またはハードウェア モジュールのシャーシへの挿入を行うことで、高度なサービスを提供することができます。これらのモジュールを通じてトラフィック インスペクションを追加することにより、設定済みのポリシーに基づいてトラフィックをブロックできます。また、これらのモジュールにトラフィックを送信することで、高度なサービスを利用することができます。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャ

ン検出とは異なり、ASA のスキャニング脅威検出機能は、スキャン アクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- トランスペアレント

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレントモードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレントファイアウォールは、他の場合にはルーテッドモードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレントファイアウォールでは、EtherType アクセス リストを使用するマルチキャスト ストリームが許可されます。

ルーテッド モードでブリッジ グループの設定、およびブリッジ グループと通常インターフェイスの間のルートの設定を行えるように、ルーテッドモードでは Integrated Routing and Bridging をサポートしてます。ルーテッド モードでは、トランスペアレント モードの機能を複製できます。マルチ コンテキスト モードまたはクラスタリングが必要ではない場合、代わりにルーテッド モードを使用することを検討してください。

ステートフル インスペクションの概要

ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケット フィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。

ただし、ASA のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  新規の接続の場合、ASA は、パケットをアクセス リストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロール プレーン パス」も通過する場合があります。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセス リストとの照合チェック
  - ルート ルックアップ
  - NAT 変換（xlates）の割り当て
  - 「ファスト パス」でのセッションの確立

  ASA は、TCP トラフィックのファスト パスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP（ICMP インスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファスト パスを使用できます。

  注 SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

  レイヤ 7 インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

  - IP チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック

- 既存セッションに基づく NAT 変換
- レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

レイヤ7インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザーの認証
- ユーザー アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ユニット上でのみ実行します。コンフィギュレーションは、メンバー ユニットに複製されます。

特殊なサービス非推奨のサービスおよびレガシーサービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンライン ヘルプとは別の場所にあります。

特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティ プロキシを提供したり、ボットネット トラフィック フィルタリングを Cisco アップデート サーバーのダイナミック データベースと組み合わせて提供したり、Cisco Webセキュリティアプライアンス用のWCCPサービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- 『Cisco ASA Botnet Traffic Filter Guide』
- 『Cisco ASA NetFlow Implementation Guide』
- 『Cisco ASA Unified Communications Guide』
- 『Cisco ASA WCCP Traffic Redirection Guide』
- 『SNMP Version 3 Tools Implementation Guide』

非推奨のサービス

非推奨の機能については、ASAバージョンの設定ガイドを参照してください。同様に、設計の見直しが行われた機能（NAT（バージョン 8.2 と 8.3 の間に見直しを実施）、トランスペアレント モードのインターフェイス（バージョン 8.3 と 8.4 の間に見直しを実施）など）については、各バージョンの設定ガイドを参照してください。ASDM は以前の ASA リリースとの後方互換性を備えていますが、設定ガイドおよびオンラインヘルプでは最新のリリースの内容しか説明されていません。

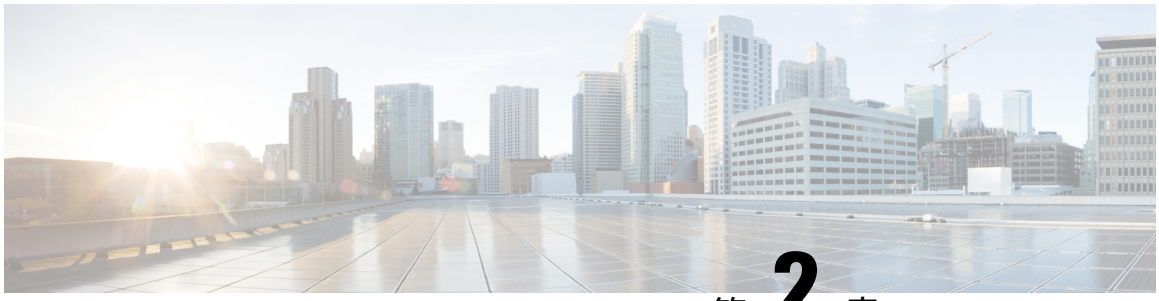
レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシーサービスについては別のガイドで説明されています。

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則
- IP スプーフィングの防止などの保護ツールの使用（**ip verify reverse-path**）、フラグメント サイズの設定（**fragment**）、不要な接続のブロック（**shun**）、TCP オプションの設定（ASDM 用）、および基本 IPS をサポートする IP 監査の設定（**ip audit**）。
- フィルタリング サービスの設定



第 2 章

使用する前に

この章では、Cisco ASA の使用を開始する方法について説明します。

コマンドラインインターフェイス（CLI）のコンソールへのアクセス

ASDM アクセスの基本的な設定を、CLI を使用して行う必要がある場合があります。

初期設定を行うには、コンソール ポートから直接 CLI にアクセスします。その後、#unique_39 に従って Telnet または SSH を使用して、リモート アクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソール ポートにアクセスするとシステムの実行スペースに入ります。

（注） ASAv のコンソール アクセスについては、ASAv のクイック スタート ガイドを参照してください。

ASA ハードウェアまたは ISA 3000 コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

手順

ステップ 1 付属のコンソール ケーブルを使用してコンピュータをコンソール ポートに接続します。ターミナル エミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2 **Enter** キーを押して、次のプロンプトが表示されることを確認します。

```
ciscoasa>
```

このプロンプトは、ユーザー EXEC モードで作業していることを示します。ユーザー EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

Firepower 2100 プラットフォーム モードのコンソールへのアクセス

Firepower 2100 コンソール ポートで FXOS CLI に接続します。次に、FXOS CLI から ASA コンソールに接続し、再度戻ることができます。FXOS に SSH 接続する場合は、ASA CLI にも接続できます。SSH からの接続はコンソール接続ではないため、FXOS SSH 接続から複数の ASA 接続を行うことができます。同様に、ASA に SSH 接続する場合は、FXOS CLI に接続できます。

始める前に

一度に保持できるコンソール接続は 1 つだけです。FXOS コンソールから ASA のコンソールに接続する場合、Telnet または SSH 接続の場合とは異なり、この接続は永続的接続です。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアル ケーブルが付属しているため、接続するためにはサード パーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティング システムに必要な USB シリアル ドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー クレデンシャルを入力します。デフォルトでは、**admin** ユーザーとデフォルトのパスワード **Admin123** を使用してログインできます。

ステップ 2 ASA に接続します。

connect asa

例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 3 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
```

```
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

設定以外のすべてのコマンドは、特権EXECモードで使用できます。特権EXECモードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードからASAの設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

ステップ 5 FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

ステップ 6 ASA に SSH 接続する場合（ASA で SSH アクセスを設定した後）、FXOS CLI に接続します。

connect fxos

FXOSへの認証を求められます。デフォルトのユーザー名：**admin**およびパスワード：**Admin123**を使用します。ASA CLIに戻るには、**exit**と入力するか、またはCtrl-Shift-6、xと入力します。

例：

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
```

```
ciscoasa#
```

Firepower 1000 および 2100 アプライアンス モードのコンソールへのアクセス

Firepower 1000 および 2100 アプライアンス モードのコンソール ポートは、ASA CLI に接続します（FXOS CLI に接続する Firepower 2100 プラットフォーム モードのコンソールとは異なります）。ASA CLI から、トラブルシューティングのために Telnet を使用して FXOS CLI に接続できます。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。 Firepower 1000 には、USB A to B シリアル ケーブルが付属しています。 Firepower 2100 には DB-9 to RJ-45 シリアル ケーブルが付属しているため、接続するためにはサード パーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（次を参照『Firepower 1010 hardware guide』または『Firepower 1100 hardware guide』）。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ASA CLI に接続します。デフォルトでは、コンソール アクセスに必要なユーザー クレデンシャルはありません。

ステップ 2 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

ASA で設定したイネーブル パスワードは、FXOS **管理者**のユーザー パスワードでもあり、ASA の起動に失敗した場合は、FXOS フェールセーフ モードに移行します。

設定以外のすべてのコマンドは、特権EXECモードで使用できます。特権EXECモードからコンフィギュレーション モードに入ることもできます。

特権 EXEC モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit**、**quit**、または **end** コマンドを入力します。

ステップ 4 （任意） FXOS CLI に接続します。

connect fxos [**admin**]

- **admin**：管理者レベルのアクセスを提供します。このオプションを指定しないと、ユーザーのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

FXOS 内では、**scope security/show audit-logs** コマンドを使用してユーザー アクティビティを表示できます。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Firepower 4100/9300 シャーシ 上の ASA コンソールへのアクセス

初期設定の場合、Firepower 4100/9300 シャーシ スーパバイザに（コンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASA セキュリティ モジュールに接続します。

手順

ステップ 1 Firepower 4100/9300 シャーシ スーパバイザ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

初めてモジュールにアクセスするときは、FXOS モジュールの CLI にアクセスします。その後 ASA アプリケーションに接続する必要があります。

connect asa

例：

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

ステップ 2 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
asa# configure terminal
asa(config)#
```

グローバル コンフィギュレーション モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 4 **Ctrl-a、d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

ステップ 5 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) **~** と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ソフトウェア モジュール コンソールへのアクセス

ASA 5506-X に ASA FirePOWER などのソフトウェア モジュールをインストールしている場合、モジュール コンソールへのセッションを実行できます。

（注） **session** コマンドを使用して ASA バックプレーンを介してハードウェア モジュール CLI にアクセスすることはできません。

手順

ASA CLI から、モジュールへのセッションを実行します。

session {**sfr** | **cxsc** | **ips**} **console**

例：

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ASA 5506W-X ワイヤレス アクセス ポイント コンソールへのアクセス

ワイヤレス アクセス ポイント コンソールにアクセスするには、次の手順を実行します。

手順

ステップ 1 ASA CLI から、アクセス ポイントへのセッションを実行します。

session wlan console

例：

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

ステップ 2 アクセス ポイント CLI については、『Cisco IOS Configuration Guide for Autonomous Aironet Access Points』を参照してください。

ASDM アクセスの設定

ここでは、デフォルト設定で ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

ASDM アクセスの工場出荷時のデフォルト設定の使用

工場出荷時のデフォルト コンフィギュレーションでは、ASDM 接続はデフォルトのネットワーク設定で事前設定されています。

手順

次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
  - Firepower 1010：管理 1/1（192.168.45.1）、または内部イーサネット 1/2 ～ 1/8（192.168.1.1）。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
  - アプライアンスモードの Firepower 1100、2100：内部イーサネット 1/2（192.168.1.1）、または管理 1/1（DHCP から）。内部ホストは 192.168.1.0/24 ネットワークに限定されます。管理ホストは任意のネットワークからアクセスできます。

- プラットフォーム モードの Firepower 2100：管理 1/1（192.168.45.1）。管理ホストは 192.168.45.0/24 ネットワークに限定されます。
- Firepower 4100/9300：展開時に定義された管理タイプ インターフェイスと IP アドレス。管理ホストは任意のネットワークからアクセスできます。
- ASA 5506-X、ASA 5506W-X：内部 GigabitEthernett 1/2 ～ 1/8、および Wi-Fi GigabitEthernet 1/9（192.168.10.1）。内部ホストは 192.168.1.0/24 ネットワークに限定され、Wi-Fi ホストは 192.168.10.0/24 に限定されます。
- ASA 5508-X および ASA 5516-X：内部 GigabitEthernet 1/2（192.168.1.1）。Inside hosts are limited to the 192.168.1.0/24 network.
- ASA 5525-X 以降：管理 0/0（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。
- ASA：管理 0/0（導入時に設定）。管理ホストは管理ネットワークに限定されます。
- ISA 3000：管理 1/1（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。

（注） マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理コンテキストから ASDM にアクセスできるようになります。

関連トピック

工場出荷時のデフォルト設定 （32 ページ）
マルチ コンテキスト モードの有効化または無効化 （301 ページ）
ASDM の起動 （29 ページ）

ASDM アクセスのカスタマイズ

次の条件に *1* つ以上当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングル ルーテッド モードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理IPアドレスを設定できるオプションを備えた工場出荷時のデフォルト コンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ（トランスペアレント モードやマルチ コンテキスト モードの設定など）がある場合や、他の設定を維持する必要がある場合にのみ使用してください。

（注） ASAv の場合、導入時にトランスペアレント モードを設定できるため、この手順は、設定をクリアする必要がある場合など、導入後に特に役立ちます。

手順

ステップ 1 コンソール ポートで CLI にアクセスします。

ステップ 2 （オプション）トランスペアレント ファイアウォール モードをイネーブルにします。

このコマンドは、設定をクリアします。

firewall transparent

ステップ 3 管理インターフェイスを設定します。

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 4 （直接接続された管理ホスト用）管理ネットワークの DHCP プールを設定します。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

その範囲にインターフェイス アドレスが含まれていないことを確認します。

ステップ 5 （リモート管理ホスト用）管理ホストへのルートを設定します。

route *management_ifc management_host_ip mask gateway_ip* **1**

例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

ステップ 6 ASDM の HTTP サーバーをイネーブルにします。

http server enable

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

http *ip_address mask interface_name*

例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

write memory

ステップ 9 （オプション）モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

関連トピック

工場出荷時のデフォルト設定の復元 （34 ページ）
ファイアウォール モード（シングル モード）の設定 （258 ページ）
ASA ハードウェアまたは ISA 3000 コンソールへのアクセス （17 ページ）
ASDM の起動 （29 ページ）

ASDM の起動

ASDM は、次の 2 つの方法で起動できます。

- ASDM-IDM ランチャ：ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合、ランチャを再度ダウンロードする必要はありません。
- Java Web Start：管理する ASA ごとに Web ブラウザで接続して、Java Web Start アプリケーションを保存または起動する必要があります。任意でコンピュータにショートカットを保存できます。ただし、ASA IP アドレスごとにショートカットを分ける必要があります。

（注） Web Start を使用する場合は、Java キャッシュをクリアしてください。クリアしない場合、Hostscan などのログイン前ポリシーに対する変更が失われる可能性があります。この問題は、ランチャを使用している場合には発生しません。

ASDM では、管理のために別の ASA IP アドレスを選択できます。ランチャと Java Web Start の機能の違いは、主に、ユーザーが最初にどのように ASA に接続し、ASDM を起動するかにあります。

ここでは、まず ASDM に接続する方法について説明します。次にランチャまたは Java Web Start を使用して ASDM を起動する方法について説明します。

ASDM はローカルの \Users\<user_id>\.asdm ディレクトリ内にキャッシュ、ログ、および設定などのファイルを保存し、Temp ディレクトリ内にも AnyConnect プロファイルなどのファイルを保存します。

手順

ステップ 1 ASDM クライアントとして指定したコンピュータで次の URL を入力します。

https://*asa_ip_address*/**admin**

（注） **http://** や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。 ASA は、HTTP 要求を HTTPS に自動的に転送しません。

次のボタンを持つ ASDM 起動ページが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

ステップ 2 ランチャをダウンロードするには、次の手順を実行します。

a) [Install ASDM Launcher and Run ASDM] をクリックします。

b) ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザー名および**イネーブル**パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDM にログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （749 ページ）を参照してください。**注**：HTTPS 認証をイネーブルにした場合、ユーザー名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

c) インストーラをコンピュータに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。

d) 管理 IP アドレス、および同じユーザー名とパスワード（新規インストールの場合は空白）を入力し、[OK] をクリックします。

ステップ 3 Java Web Start を使用するには、次の手順を実行します。

a) [Run ASDM] または [Run Startup Wizard] をクリックします。

b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。

c) ショートカットから Java Web Start を起動します。

d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。

e) ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザー名および**イネーブル**パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDM にログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （749 ページ）を参照してください。**注**：HTTPS 認証をイネーブルにした場合、ユーザー名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

ASDM 動作のカスタマイズ

アイデンティティ証明書をインストールして ASDM を正常に起動するだけでなく、ASDM ヒープメモリを増大することもできるため、より大きいサイズのコンフィギュレーションを処理できます。

ASDM のアイデンティティ証明書のインストール

Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。証明書をインストールするまで、Java Web Start を使用して ASDM を起動することができます。

ASDM で使用するために ASA に自己署名された ID 証明書をインストールし、Java を使用して証明書を登録するには、次のマニュアルを参照してください。

http://www.cisco.com/go/asdm-certificate

ASDM コンフィギュレーション メモリの増大

ASDM でサポートされる最大設定サイズは 512 KB です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータス ダイアログボックスに表示されます。このとき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープ メモリの増大を検討することを推奨します。

Windows での ASDM コンフィギュレーション メモリの増大

ASDM ヒープ メモリ サイズを増大するには、次の手順を実行して **run.bat** ファイルを編集します。

手順

ステップ 1 ASDM インストール ディレクトリ（たとえば、C:\Program Files (x86)\Cisco Systems\ASDM）に移動します。

ステップ 2 任意のテキスト エディタを使用して **run.bat** ファイルを編集します。

ステップ 3 「start javaw.exe」で始まる行で、「-Xmx」のプレフィックスが付いた引数を変更し、目的のヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

ステップ 4 **run.bat** ファイルを保存します。

Mac OS での ASDM コンフィギュレーション メモリの増大

ASDM ヒープ メモリ サイズを増大するには、次の手順を実行して **Info.plist** ファイルを編集します。

手順

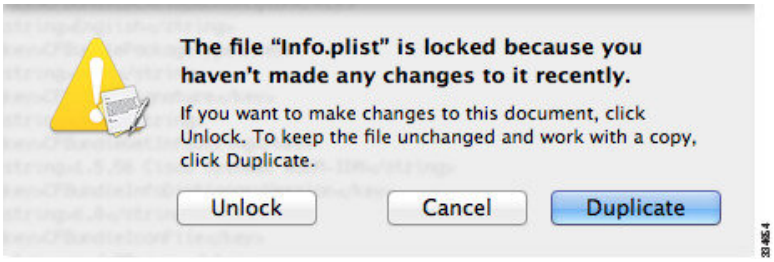
ステップ 1 [Cisco ASDM-IDM] アイコンを右クリックし、[Show Package Contents] を選択します。

ステップ 2 [Contents] フォルダで、Info.plist ファイルをダブルクリックします。開発者ツールをインストールしている場合は、**プロパティ リスト エディタ** で開きます。そうでない場合は、**TextEdit** で開きます。

ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープ サイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

ステップ 4 このファイルがロックされると、次のようなエラーが表示されます。



ステップ 5 [Unlock] をクリックし、ファイルを保存します。

[Unlock] ダイアログボックスが表示されない場合は、エディタを終了します。[Cisco ASDM-IDM] アイコンを右クリックし、[Copy Cisco ASDM-IDM] を選択して、書き込み権限がある場所（デスクトップなど）に貼り付けます。その後、このコピーからヒープ サイズを変更します。

工場出荷時のデフォルト設定

工場出荷時のデフォルト設定とは、シスコが新しい ASA に適用したコンフィギュレーションです。

- ASA 5506-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。内部インターフェイスから ASDM を使用して ASA を管理できます。内部インターフェイスは、統合ルーティングとブリッジングを使用してブリッジ グループに配置されます。
- ASA 5508-X および 5516-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、内部インターフェイスから ASDM を使用して管理できます。
- ASA 5525-X ～ ASA 5555-X：管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- Firepower 1010：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部スイッチ ポートから ASDM を使用して管理できます。
- Firepower 1100：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Firepower 2100：プラットフォーム モード（デフォルト）：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスから Firepower Chassis Manager と ASDM を使用して管理できます。

  アプライアンス モード：アプライアンス モードに変更すると、工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Firepower 4100/9300 シャーシ：ASA のスタンドアロンまたはクラスタを展開する場合、管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- ASAv：ハイパーバイザによっては、導入の一環として、管理用のインターフェイス導入設定（初期の仮想導入設定）によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。フェールオーバー IP アドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。
- ISA 3000：工場出荷時のデフォルト設定は、同じネットワーク上のすべての内部および外部インターフェイスを使用した、ほぼ完全なトランスペアレント ファイアウォール モード設定です。ASDM を使用して管理インターフェイスに接続し、ネットワークの IP アドレスを設定できます。ハードウェアバイパスは 2 つのインターフェイスペアに対して有効になっていて、すべてのトラフィックはインラインタップモニタ専用モードで ASA FirePOWER モジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

アプライアンスの場合、工場出荷時のデフォルト設定は、工場出荷時のデフォルト設定がトランスペアレントモードでのみ使用可能な ISA 3000 を除き、ルーテッド ファイアウォール モードとシングルコンテキストモードのみで使用できます。ASAv および Firepower 4100/9300 シャーシ の場合、導入時にトランスペアレント モードまたはルーテッド モードを選択できます。

（注） イメージ ファイルと（隠された）デフォルト コンフィギュレーションに加え、log/、crypto_archive/、および coredumpinfo/coredump.cfg がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージ ファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

工場出荷時のデフォルト設定の復元

この項では、工場出荷時のデフォルトコンフィギュレーションを復元する方法について説明します。CLI および ASDM の両方の手順が提供されています。ASAv では、この手順を実行することで導入設定が消去され、ASA 5525-X の場合と同じ工場出荷時のデフォルト設定が適用されます。

（注） Firepower 4100/9300 では、工場出荷時のデフォルト設定を復元すると単に設定が消去されるだけです。 デフォルト設定を復元するには、スーパバイザから ASA をもう一度展開する必要があります。

始める前に

この機能は、ISA 3000 を除き、ルーテッドファイアウォールモードでのみ使用できます（ISA 3000 では、このコマンドはトランスペアレントモードでのみサポートされます）。さらに、この機能はシングルコンテキストモードでのみ使用できます。コンフィギュレーションがクリアされた ASA には、この機能を使用して自動的に設定する定義済みコンテキストがありません。

手順

ステップ 1 工場出荷時のデフォルト コンフィギュレーションを復元します。

configure factory-default [*ip_address* [*mask*]]

例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

（注） このコマンドは、Firepower 2100 の現在設定されているモード（アプライアンスまたはプラットフォーム）をクリアしません。

ip_address を指定する場合は、デフォルトの IP アドレスを使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスの IP アドレスを設定します。*ip_address* オプションで設定されているインターフェイスについては、次のモデルのガイドラインを参照してください。

- Firepower 1010：**管理**インターフェイスの IP アドレスを設定します。
- Firepower 1100：**内部**インターフェイスの IP アドレスを設定します。
- アプライアンス モードの Firepower 2100：**内部**インターフェイスの IP アドレスを設定します。
- プラットフォーム モードの Firepower 2100：**管理**インターフェイスの IP アドレスを設定します。
- Firepower 4100/9300：効果はありません。
- ASAv：**管理**インターフェイスの IP アドレスを設定します。
- ASA 5506-X：**内部**インターフェイスの IP アドレスを設定します。
- ASA 5508-X および 5516-X：**内部**インターフェイスの IP アドレスを設定します。
- ASA 5525-X、5545-X、5555-X：**管理**インターフェイスの IP アドレスを設定します。
- ISA 3000：**管理**インターフェイスの IP アドレスを設定します。

http コマンドでは、ユーザーが指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定した IP アドレスよりも大きい使用可能なすべてのアドレスで構成されます。たとえば、サブネットマスク 255.255.255.0 で 10.5.6.78 を指定した場合、DHCP アドレスの範囲は 10.5.6.79 ～ 10.5.6.254 になります。

Firepower 1000、およびアプライアンスモードの Firepower 2100 の場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

プラットフォーム モードの Firepower 2100 の場合：このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。**boot system** コマンドを使用すると、特定のイメージから起動できます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、ASA はブートしません。

例：

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
```

```
WARNING: The new maximum-session limit will take effect after the running-config is saved
 and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

ステップ 2 デフォルト コンフィギュレーションをフラッシュ メモリに保存します。

write memory

このコマンドでは、事前に **boot** config コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションがクリアされると、このパスもクリアされます。

ステップ 3 （ASDM での手順。）メイン ASDM アプリケーション ウィンドウで、次を実行します。

a) **[File]** > **[Reset Device to the Factory Default Configuration]** の順に選択します。

[Reset Device to the Default Configuration] ダイアログボックスが表示されます。

b) （オプション）デフォルトアドレスを使用する代わりに、管理または内部インターフェイスの**管理 IP アドレス**を入力します。

モデルごとに設定されているインターフェイス IP の詳細については、前述の CLI 手順を参照してください。

c) （オプション）ドロップダウン リストから [Management Subnet Mask] を選択します。

d) [OK] をクリックします。

確認用のダイアログボックスが表示されます。

（注） Firepower 1000、およびアプライアンスモードの Firepower 2100 の場合：このコマンドは、残りの設定とともにブートイメージの場所をクリアします（存在する場合）。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

プラットフォームモードの Firepower 2100 の場合：このモデルでは、ブートイメージの場所は使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合：この操作により、残りの設定とともにブートイメージの場所もクリアされます（存在する場合）。[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] ペインでは、外部メモリ上のイメージを含む、特定のイメージからブートできます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュメモリの最初のイメージからブートします。内部フラッシュメモリにイメージがない場合、ASA はブートしません。

e) [Yes] をクリックします。
f) デフォルト設定を復元したら、この設定を内部フラッシュ メモリに保存します。**[File]** > **[Save Running Configuration to Flash]** を選択します。

このオプションを選択すると、以前に別の場所を設定している場合でも、実行コンフィギュレーションがスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションをクリアした場合は、このパスもクリアされています。

ASAv 導入設定の復元

この項では、ASAv の導入（第 0 日）設定を復元する方法について説明します。

手順

ステップ 1 フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニットをリロードし、フェールオーバー リンクを介して再接続すると、古い設定は新しいアクティブユニットから同期し、必要な導入コンフィギュレーションが消去されます。

ステップ 2 リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

write erase

（注） ASAv が現在の実行イメージをブートするため、元のブート イメージには戻りません。元のブートイメージを使用するには、**boot image** コマンドを参照してください。

コンフィギュレーションは保存しないでください。

ステップ 3 ASAv をリロードし、導入設定をロードします。

reload

ステップ 4 フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

ASA 5506-X シリーズのデフォルト設定

ASA 5506-X シリーズの出荷時のデフォルトのコンフィギュレーションは、次のとおりです。

- Integrated Routing and Bridging 機能：GigabitEthernet 1/2 ~ 1/8 はブリッジ グループ 1 に所属、ブリッジ仮想インターフェイス（BVI） 1
- 内部 --> 外部へのトラフィック フロー：GigabitEthernet 1/1（外部）、BVI 1（内部）
- DHCP の外部 IP アドレス、内部 IP アドレス：192.168.1.1
- （ASA 5506W-X）WiFi<--> 内部のトラフィック フロー、WiFi --> 外部へのトラフィック フロー：GigabitEthernet 1/9（WiFi）
- （ASA 5506W-X）WiFi の IP アドレス：192.168.10.1
- 内部および WiFi 上のクライアントに対する DHCP。アクセス ポイント自体とそのすべてのクライアントが ASA を DHCP サーバーとして使用します。
- ASDM アクセス：内部ホストと Wi-Fi ホストが許可されます。
- NAT：内部、WiFi、および管理から外部へのすべてのトラフィックのインターフェイス PAT。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface GigabitEthernet1/2
```

```
  nameif inside_1
  security-level 100
  bridge-group 1
  no shutdown
interface GigabitEthernet1/3
  nameif inside_2
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/4
  nameif inside_3
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/5
  nameif inside_4
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/6
  nameif inside_5
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/7
  nameif inside_6
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/8
  nameif inside_7
  security-level 100
  no shutdown
  bridge-group 1
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
object network obj_any1
 subnet 0.0.0.0 0.0.0.0
 nat (inside_1,outside) dynamic interface
object network obj_any2
 subnet 0.0.0.0 0.0.0.0
 nat (inside_2,outside) dynamic interface
object network obj_any3
 subnet 0.0.0.0 0.0.0.0
 nat (inside_3,outside) dynamic interface
object network obj_any4
 subnet 0.0.0.0 0.0.0.0
 nat (inside_4,outside) dynamic interface
object network obj_any5
 subnet 0.0.0.0 0.0.0.0
 nat (inside_5,outside) dynamic interface
object network obj_any6
 subnet 0.0.0.0 0.0.0.0
 nat (inside_6,outside) dynamic interface
object network obj_any7
 subnet 0.0.0.0 0.0.0.0
 nat (inside_7,outside) dynamic interface
!
same-security-traffic permit inter-interface
!
```

```
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5506W-X の場合は、次のコマンドも含まれます。

```
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
object network obj_any_wifi
 subnet 0.0.0.0 0.0.0.0
 nat (wifi,outside) dynamic interface
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5508-Xおよび 5516-X のデフォルト設定

ASA 5508-Xおよび 5516-X の工場出荷時のデフォルト設定は、次のとおりです。

- **内部 --> 外部**へのトラフィックフロー：GigabitEthernet 1/1（外部）、GigabitEthernet 1/2（内部）
- DHCP からの**外部 IP アドレス**
- **内部 IP アドレス**：192.168.1.1
- 内部。
- 外部 DHCP からの**デフォルト ルート**
- **管理 1/1 インターフェイス**が稼働しているが、そうでない場合は未設定。ASA FirePOWER モジュールは、このインターフェイスを使用して ASA 内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。
- **ASDM** アクセス：内部ホストと ホストが許可されます。
- **NAT**：内部および管理から外部へのすべてのトラフィックのインターフェイス PAT。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface GigabitEthernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5525-X ～ ASA 5555-X デフォルト設定

ASA 5525-X ～ ASA 5555-X の工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイス：Management 0/0（管理）。
- IP アドレス：管理アドレスは 192.168.1.1/24 です。
- DHCP サーバー：管理ホストでは DHCP サーバーがイネーブルにされているため、管理インターフェイスに接続するコンピュータには、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM アクセス：管理ホストに許可されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
```

```
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Firepower 1010 のデフォルト設定

Firepower 1010 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェア スイッチ**：イーサネット 1/2 ～ 1/8 は VLAN 1 に属しています。
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、内部 IP アドレス：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
```

```
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 1100 のデフォルト設定

Firepower 1100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス

- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 2100 プラットフォームモードのデフォルト設定

Firepower 2100 はプラットフォーム モードで実行するように設定できます。デフォルトはアプライアンス モードです。

（注） 9.13(1) 以前のバージョンでは、プラットフォームモードがデフォルトであり、唯一のオプションでした。プラットフォーム モードからアップグレードする場合、このモードが維持されます。

ASA の設定

Firepower 2100 上の ASA の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、内部 IP アドレス：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP からの**デフォルト ルート**
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- **ASDM** アクセス：管理ホストに許可されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **FXOS 管理**トラフィックの開始：FXOS シャーシは、ASA 外部インターフェイス上で管理トラフィックを開始できます。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
```

```
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
```

FXOS の設定

Firepower 2100 上の FXOS の工場出荷時のデフォルト設定は、次のとおりです。

- **管理 1/1**：IP アドレス 192.168.45.45
- **デフォルト ゲートウェイ**：ASA データ インターフェイス
- **Firepower Chassis Manager および SSH アクセス**：管理ネットワークからのみ。
- **デフォルトのユーザー名**：**admin**、デフォルトのパスワード：**Admin123**
- **DHCP サーバー**：クライアント IP アドレス範囲 192.168.45.10 ～ 192.168.45.12
- **NTP** サーバー：Cisco NTP サーバー：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org
- **DNS** サーバー：OpenDNS：208.67.222.222、208.67.220.220
- **イーサネット 1/1 およびイーサネット 1/2**：有効

Firepower 2100 アプライアンス モードのデフォルト設定

デフォルトでは、Firepower 2100 はアプライアンス モードで実行されます。

（注） 9.13(1)以前のバージョンでは、プラットフォーム モードがデフォルトであり、唯一のオプションでした。プラットフォーム モードからアップグレードする場合、プラットフォーム モードが維持されます。

アプライアンス モードの Firepower 2100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス、内部 IP アドレス**：192.168.1.1
- DHCP からの**管理 IP アドレス**：管理 1/1（管理）
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**

- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 4100/9300 シャーシ デフォルト設定

Firepower 4100/9300 シャーシ 上に ASA を展開した場合、ASDM を使用して管理インターフェイスへの接続が可能になる多くのパラメータを事前設定できます。一般的な構成には次の設定があります。

- 管理インターフェイス：
  - Firepower 4100/9300 シャーシ スーパバイザ上で定義された任意の管理タイプ インターフェイス

- 名前は「management」
- 任意の IP アドレス
- セキュリティ レベル 0
- 管理専用

- 管理インターフェイス内のデフォルト ルート
- ASDM アクセス：すべてのホストが許可されます。

スタンドアロン ユニットの設定は、次のコマンドで構成されます。クラスタ ユニットの追加の設定については、ASA クラスタの作成 （528 ページ） を参照してください。

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- **トランスペアレント ファイアウォール モード**：トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。
- **1 ブリッジ仮想インターフェイス**：すべてのメンバーインターフェイスは同じネットワーク内に存在しています（**IP アドレスは事前設定されていません。ネットワークと一致するように設定する必要があります**）：GigabitEthernet 1/1 （outside1）、GigabitEthernet 1/2 （inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての**内部および外部**インターフェイスは相互通信できます。
- **管理 1/1** インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する **DHCP**。
- **ASDM** アクセス：管理ホストに許可されます。

- **ハードウェアバイパス**は、次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4

(注) ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイス ペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASA がフローを引き継ぐため、接続が短時間中断されます。

- **ASA FirePOWER モジュール**：すべてのトラフィックが、Inline Tap Monitor-Only モードのモジュールに送信されます。このモードでは、モニターリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。
- **高精度時間プロトコル**：PTP トラフィックは、Firepowerのモジュールに送信されません。

このコンフィギュレーションは次のコマンドで構成されています。

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface
```

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

object-group service bypass_sfr_inspect
  service-object udp destination range 319 320
access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any
access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
  sfr fail-open monitor-only
service-policy global_policy global
```

ASAv 導入設定

ASAv 上に ASA を展開した場合、ASDM を使用して管理 0/0 インターフェイスへの接続が可能になる多くのパラメータを前もって設定できます。一般的な構成には次の設定があります。

- ルーテッド ファイアウォール モードまたはトランスペアレント ファイアウォール モード
- Management 0/0 インターフェイス：
  - 名前は「management」
  - IP アドレスまたは DHCP
  - セキュリティ レベル 0
- 管理ホスト IP アドレスのスタティック ルート（管理サブネット上にない場合）
- HTTP サーバーの有効または無効
- 管理ホスト IP アドレス用の HTTP アクセス
- （オプション）GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、Management0/0 のスタンバイ IP アドレス
- DNS サーバー
- スマート ライセンス ID トークン
- スマート ライセンスのスループット レベルおよび標準機能ティア
- （オプション）Smart Call Home HTTP プロキシ URL およびポート
- （オプション）SSH 管理設定：
  - クライアント IP アドレス

- ローカル ユーザー名とパスワード
- ローカル データベースを使用する SSH に必要な認証

- （オプション）REST API の有効または無効

（注） Cisco 認証局に正常に登録するには、ASAv をインターネット アクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

スタンドアロン ユニットについては、次の設定例を参照してください。

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

フェールオーバー ペアのプライマリ ユニットについては、次の設定例を参照してください。

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
```

```
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

アプライアンスまたはプラットフォーム モードへの Firepower 2100 の設定

Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティング システムを実行します。Firepower 2100 は、次のモードで実行できます。

- アプライアンスモード（デフォルト）：アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。
- プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Firepower Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

この手順では、モードの変更方法について説明します。モードを変更すると、設定がクリアされ、システムをリロードする必要があります。デフォルト設定は、リロード時に適用されます。**clear configure all** および **configure factory-default** コマンドは、現在のモードをクリアしません。

始める前に

モードは、CLI でのみ変更できます。

手順

ステップ 1 （任意）現在の設定をバックアップします。コンフィギュレーションまたはその他のファイルのバックアップと復元 （1209 ページ）を参照してください。

アプライアンス モードの設定とプラットフォーム モードの設定には多少の違いがありますが、古い設定のコピーを出発点にすることをお勧めします。たとえば、プラットフォーム モードの場合、NTP、DNS、および EtherChannel の設定は ASA 設定の一部ではないため、バックアップには含まれませんが、その他のほとんどの ASA 設定は両方のモードで有効です。

ステップ 2 現在のモードを表示します。

show fxos mode

例：

```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

ステップ 3 モードをプラットフォームモードに設定します。

no fxos mode appliance

write memory

reload

モードを設定したら、設定を保存してデバイスをリロードする必要があります。リロードする前に、中断することなく、モードを元の値に戻すことができます。

例：

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system
 has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

ステップ 4 モードをアプライアンス モードに設定します。

fxos mode appliance

write memory

reload

モードを設定したら、設定を保存してデバイスをリロードする必要があります。リロードする前に、中断することなく、モードを元の値に戻すことができます。

例：

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system
 has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
```

```
Proceed with reload? [confirm]
```

設定の開始

ASA を設定してモニターするには、次の手順を実行します。

（注） ASDM では、最大 512 KB の設定をサポートしています。このサイズを超えると、パフォーマンスの問題が生じることがあります。ASDM コンフィギュレーション メモリの増大 （31 ページ）を参照してください。

手順

ステップ 1 Startup Wizard を使用して初期設定を行うには、[Wizards] > [Startup Wizard] を選択します。

ステップ 2 IPsec VPN Wizard を使用して IPsec VPN 接続を設定するには、[Wizards] > [IPsecVPN Wizard] を選択して、表示される各画面で設定を行います。

ステップ 3 SSL VPN Wizard を使用して SSL VPN 接続を設定するには、[Wizards] > [SSL VPN Wizard] を選択して、表示される各画面で設定を行います。

ステップ 4 高可用性とスケーラビリティに関する設定値を設定するには、[Wizards] > [High Availability and Scalability Wizard] を選択します。

ステップ 5 Packet Capture Wizard を使用してパケット キャプチャを設定するには、[Wizards] > [Packet Capture Wizard] を選択します。

ステップ 6 ASDM GUI で使用できるさまざまな色とスタイルを表示するには、**[View]** > **[Office Look and Feel]** を選択します。

ステップ 7 機能を設定するには、ツールバーの [Configuration] ボタンをクリックし、いずれかの機能ボタンをクリックして、関連する設定ペインを表示します。

（注） [Configuration] 画面が空白の場合は、ツールバーで [Refresh] をクリックして、画面のコンテンツを表示します。

ステップ 8 ASA をモニターするには、ツールバーの [Monitoring] ボタンをクリックし、機能ボタンをクリックして、関連するモニターリング ペインを表示します。

ASDMでのコマンドライン インターフェイス ツールの使用

この項では、ASDMを使用してコマンドを入力する方法およびCLIの使用方法について説明します。

コマンドライン インターフェイス ツールの使用

この機能には、コマンドを ASA に送信して結果を表示する、テキストベースのツールが用意されています。

CLIツールによって入力可能なコマンドは、ユーザー権限によって異なります。メインASDMアプリケーション ウィンドウの下部にあるステータスバーの権限レベルを見て、CLI特権コマンドを実行するために必要な特権があるかどうかを確認してください。

始める前に

- ASDM の CLI ツールから入力するコマンドは、ASA の接続ターミナルから入力するコマンドと動作が異なる場合があります。
- コマンドエラー：誤った入力コマンドによってエラーが発生した場合、その誤ったコマンドはスキップされ、その他のコマンドは処理されます。[Response] 領域には、他の関連情報とともに、エラーが発生したかどうかについての情報を示すメッセージが表示されます。
- インタラクティブ コマンド：インタラクティブ コマンドは、CLI ツールではサポートされていません。これらのコマンドをASDMで使用するには、次のコマンドに示すように、**noconfirm** キーワード（使用可能な場合）を使用します。

```
crypto key generate rsa modulus 1024 noconfirm
```

- 他の管理者との競合を回避：複数の管理ユーザーが ASA の実行コンフィギュレーションをアップデートできます。ASDMのCLIツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザーが同時に ASA を設定した場合、最新の変更が有効になります。

  同じASAで現在アクティブな他の管理セッションを表示するには、[Monitoring] > [Properties] > [Device Access] の順に選択します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[Command Line Interface]** の順に選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 2 必要なコマンドのタイプ（1 行または複数行）を選択し、ドロップダウン リストからコマンドを選択するか、または表示されたフィールドにコマンドを入力します。

ステップ 3 [Send] をクリックしてコマンドを実行します。

ステップ 4 新しいコマンドを入力するには、[Clear Response] をクリックしてから、実行する別のコマンドを選択（または入力）します。

ステップ 5 この機能の状況依存ヘルプを表示するには、[Enable context-sensitive help (?)] チェックボックスをオンにします。文脈依存ヘルプをディセーブルにするには、このチェックボックスをオフにします。

ステップ 6 設定を変更した場合は、[Command Line Interface] ダイアログボックスを閉じた後に、[Refresh] をクリックして ASDM での変更内容を表示します。

ASDM によって無視されるコマンドのデバイス上での表示

この機能により、ASDM がサポートしていないコマンドの一覧を表示できます。通常 ASDM は、これらのコマンドを無視します。ASDM は、実行コンフィギュレーションのこれらのコマンドを変更、削除することはありません。詳細については、「サポートされていないコマンド（100 ページ）」を参照してください。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[Show Commands Ignored by ASDM on Device]** の順に選択します。

ステップ 2 完了したら、[OK] をクリックします。

接続の設定変更の適用

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続は、接続の確立時に設定されたポリシーを引き続き使用します。古い接続の **show** コマンド出力には古い設定が反映され、古い接続に関するデータを含まない場合があります。

たとえば、インターフェイスから QoS **service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている QoS カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

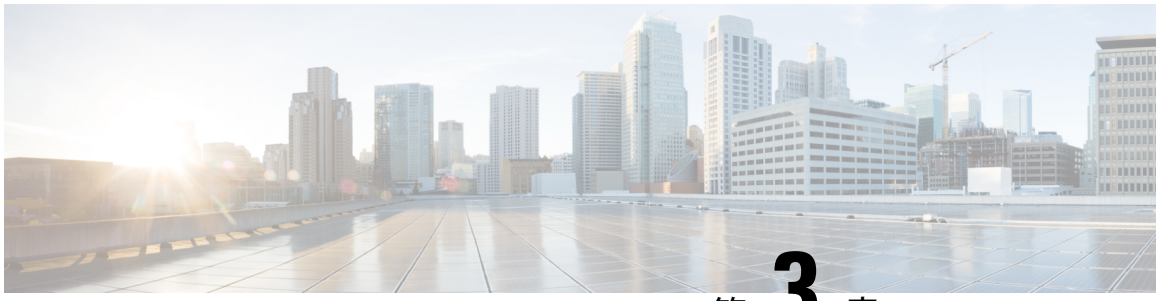
すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のコマンドを入力します。

- **clear conn**[**all**] [**protocol** {**tcp** |**udp**}] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*] [**port** *src_port* [*-src_port*] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*] [**port** *dest_port* [*-dest_port*]

  このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

  引数を指定しないと、このコマンドはすべての through-the-box 接続をクリアします。to-the-box 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。



第 3 章

ASDM グラフィカル ユーザー インターフェイス

この章では、ASDM ユーザー インターフェイスの使用方法について説明します。

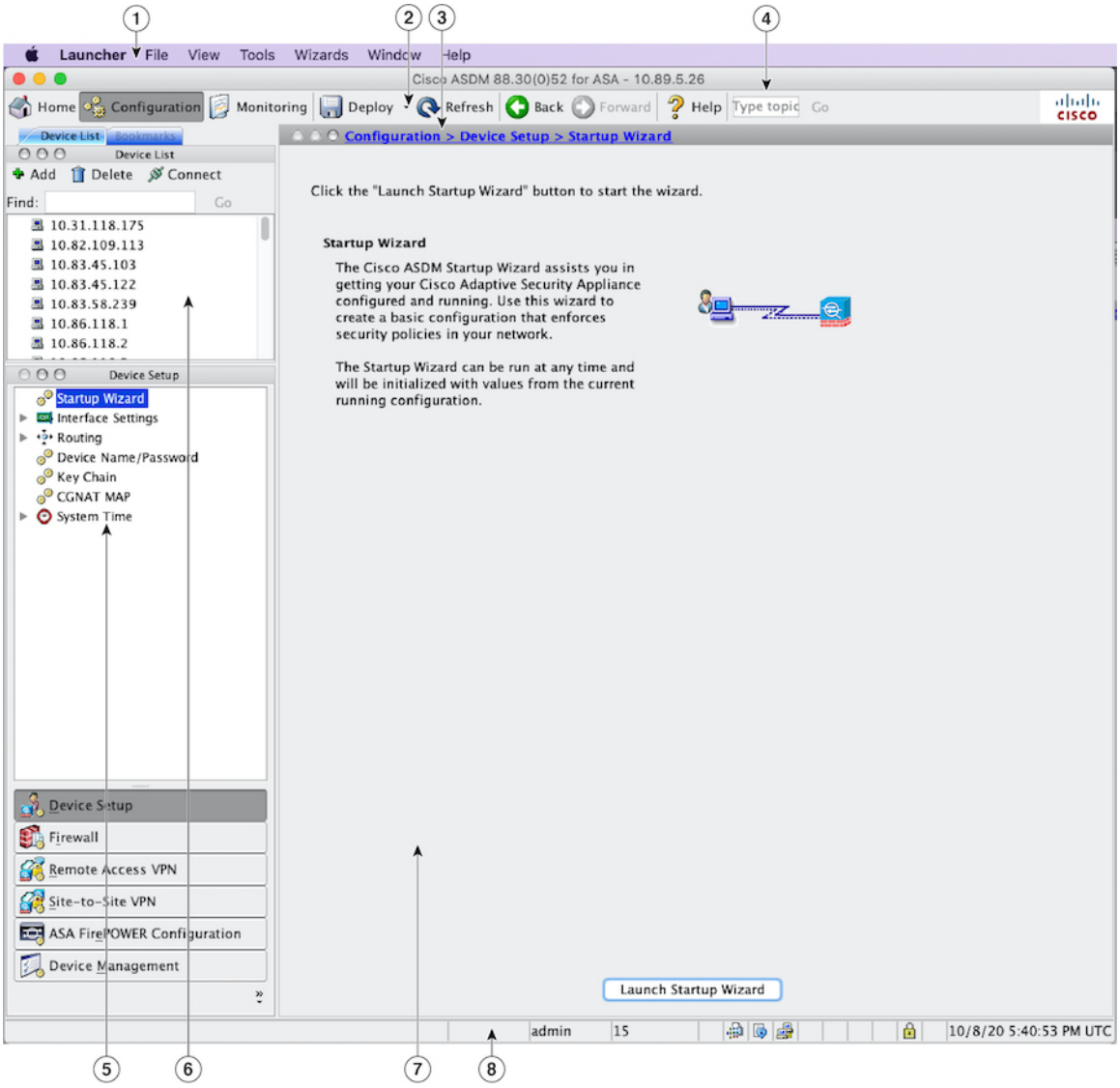
ASDM ユーザー インターフェイスについて

ASDM ユーザー インターフェイスは、ASA がサポートしているさまざまな機能に簡単にアクセスできるように設計されています。ASDM ユーザー インターフェイスには次の要素があります。

- ファイル、ツール、ウィザード、およびヘルプにすぐにアクセスできるメニューバー。メニュー項目の多くにはキーボード ショートカットもあります。
- ASDM の操作のためのツールバー。ツールバーから [Home] ペイン、[Configuration] ペイン、および [Monitoring] ペインにアクセスできます。また、ヘルプの参照やペイン間のナビゲーションもできます。
- ドッキング可能な左側の [Navigation] ペイン。[Configuration] ペインや [Monitoring] ペイン内の移動に使用します。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティング ペインへの変更、ペインの非表示化、またはペインを閉じることができます。[Configuration] ペインおよび [Monitoring] ペインにアクセスするには、次のいずれかを実行します。
  - アプリケーション ウィンドウの左端にある左側の [Navigation] ペインのリンクをクリックします。選択した [Content] ペインのタイトルバーにパスが表示されます（[Configuration] > [Device Setup] > [Startup Wizard] など）。
  - 正確なパスがわかっている場合、左側の [Navigation] ペインでリンクをクリックしなくても、アプリケーション ウィンドウの右側にある [Content] ペインのタイトルバーに直接入力できます。
- 左側の [Navigation] ペインを非表示/表示できる [Content] ペインの右端にある [maximize and restore] ボタン。
- ドッキング可能な [Device List] ペイン。ASDM からアクセスできるデバイスのリストを表示します。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティング ペインへの変更、ペインの非表示化、またはペインを閉じることができます。
- 時間、接続ステータス、ユーザー、メモリ ステータス、実行コンフィギュレーション ステータス、権限レベル、および SSL ステータスをアプリケーション ウィンドウの下部に表示するステータス バー。
- 左側の [Navigation] ペイン。アクセス ルール、NAT ルール、AAA ルール、フィルタ ルール、およびサービス ルールの作成時にルール テーブルで使用できるさまざまなオブジェクトを表示します。ペイン内のタブ タイトルは、表示している機能に応じて変わります。また、このペインには **ASDM Assistant** が表示されます。

次の図に、ASDM ユーザー インターフェイスの要素を示します。

図 *1* : *ASDM* ユーザー インターフェイス



凡例

GUI 要素	説明
1	メニュー バー
2	ツールバー
3	ナビゲーション パス
4	検索フィールド
5	左側のナビゲーション ペイン

GUI 要素	説明
6	[Device List] ペイン
7	[Content] ペイン
8	ステータス バー

（注） ツール ヒントが、[Wizards] 、[Configuration] ペイン、[Monitoring] ペイン、**ステータス バー**を含む、GUI のさまざまな部分に追加されています。ツール ヒントを表示するには、マウスをステータスバーにあるアイコンなど、特定のユーザーインターフェイス要素の上に置きます。

ASDM ユーザー インターフェイスのナビゲーション

ASDM ユーザー インターフェイスを効率的に移動するために、前の項で説明したメニュー、ツールバー、ドッキング可能ペイン、および左側と右側の [Navigation] ペインを組み合わせて使用できます。使用できる機能は、[Device List] ペインの下のボタン リストに表示されます。リスト例には、次の機能ボタンが入っている場合があります。

- **Device Setup**
- **Firewall**
- **Botnet Traffic Filter**
- **Remote Access VPN**
- **Site to Site VPN**
- **Device Management**

表示される機能ボタンのリストは、購入したライセンス機能に基づいて表示されます。コンフィギュレーション ビューまたはモニターリング ビューの選択した機能の最初のペインにアクセスするには、それぞれのボタンをクリックします。ホーム ビューでは、機能ボタンは使用できません。

機能ボタンの表示を変える場合は、次の手順を実行します。

手順

ステップ 1 最後の機能ボタンの下にあるドロップダウン リスト ボタンを選択して、コンテキスト メニューを表示します。

ステップ 2 次のいずれかのオプションを選択します。

- 表示するボタンを増やすには、[Show More Buttons] をクリックします。

- 表示するボタンを減らすには、[Show Fewer Buttons] をクリックします。
- ボタンを追加または削除するには、[Add or Remove Buttons] をクリックし、表示されたリストから追加または削除するボタンをクリックします。
- [Option] を選択すると [Option] ダイアログボックスが表示され、ボタンのリストが現在の順序で表示されます。次のいずれかを選択します。
  - リスト内のボタンを上に移動するには、[Move Up] をクリックします。
  - リスト内のボタンを下に移動するには、[Move Down] をクリックします。
  - リスト内の項目の順序をデフォルト設定に戻すには、[Reset] をクリックします。

ステップ 3 [OK] をクリックして設定を保存し、ダイアログボックスを閉じます。

メニュー

ASDM の各メニューには、マウスまたはキーボードを使用してアクセスできます。

[File] メニュー

[File] メニューでは、ASA のコンフィギュレーションを管理できます。

[File] メニュー項目	説明
Refresh ASDM with the Running Configuration on the Device	実行コンフィギュレーションのコピーを ASDM にロードします。
Reset Device to the Factory Default Configuration	コンフィギュレーションを工場出荷時のデフォルトに復元します。
Show Running Configuration in New Window	現在の実行コンフィギュレーションを新しいウィンドウに表示します。
Save Running Configuration to Flash	実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
Save Running Configuration to TFTP Server	現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバーに保存します。
Save Running Configuration to Standby Unit	プライマリ装置の実行コンフィギュレーション ファイルのコピーを、フェールオーバー スタンバイ装置の実行コンフィギュレーションに送信します。

[File] メニュー項目	説明
Save Internal Log Buffer to Flash	内部ログ バッファをフラッシュ メモリに保存します。
Deploy Firepower Changes	モジュールに対して行った、ASA Firepower モジュール ポリシーへの設定変更を保存します。このオプションは、ASA Firepowerモジュールをインストールして、ASDM で管理するときにのみ使用できます。
Print	現在のページを印刷します。ルールを印刷する場合、ページを横方向にすることをお勧めします。Internet Explorer の場合は、署名付きアプレットを最初に承認した時点で印刷権限が与えられています。
Clear ASDM Cache	ローカル ASDM イメージを削除します。ASDM に接続すると、ASDM によりイメージがローカルにダウンロードされます。
Clear ASDM Password Cache	新しいパスワードを定義した後に、それとは異なる既存のパスワードがまだ残っている場合は、パスワード キャッシュを削除します。
Clear Internal Log Buffer	syslog メッセージ バッファを空にします。
Exit	ASDM を閉じます。

[View] メニュー

[View] メニューでは、ASDM ユーザー インターフェイスのさまざまな部分を表示できます。現在のビューに応じた特定の項目が表示されます。現在のビューに表示できない項目は選択できません。

[View] メニュー項目	説明
Home	ホーム ビューを表示します。
Configuration	コンフィギュレーション ビューを表示します。
Monitoring	モニターリング ビューを表示します。
Device List	ドッキング可能なペインにデバイスのリストを表示します。
Navigation	コンフィギュレーション ビューおよびモニターリング ビューで [Navigation] ペインを表示または非表示にします。

[View] メニュー項目	説明
ASDM Assistant	タスクに応じた ASDM の使用方法のヘルプを検索し、見つけます。
Latest ASDM Syslog Messages	ホーム ビューで [Latest ASDM Syslog Messages] ペインを表示または非表示にします。このペインは、ホーム ビューでのみ使用できます。最新のリリースにアップグレードするためのメモリが不足している場合は、syslog メッセージ %ASA-1-211004 が生成され、インストールされているメモリ、および必要なメモリが示されます。このメッセージは、メモリがアップグレードされるまで、24 時間ごとに再表示されます。
Addresses	[Addresses] ペインを表示または非表示にします。[Addresses] ペインは、コンフィギュレーション ビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
Services	[Services] ペインを表示または非表示にします。[Services] ペインは、コンフィギュレーション ビューの [Access Rules]、[NAT Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
Time Ranges	[Time Ranges] ペインを表示または非表示にします。[Time Ranges] ペインは、コンフィギュレーション ビューの [Access Rules]、[Service Policy Rules]、[AAA Rules]、および [Filter Rules] ペインでのみ使用できます。
Select Next Pane	マルチペイン画面で次のペインを強調表示します。たとえば、[Service Policies Rules] ペインからその隣の [Address] ペインに移動します。
Select Previous Pane	マルチペイン画面で前のペインを強調表示します。
Back	前のペインに戻ります。
Forward	以前に表示した次のペインに移動します。
Find in ASDM	機能や **ASDM Assistant** などの項目を検索します。

[View] メニュー項目	説明
Reset Layout	レイアウトをデフォルトのコンフィギュレーションに戻します。
Office Look and Feel	画面のフォントと色を Microsoft Office 設定に変更します。

[Tools] メニュー

[Tools] メニューは、ASDM で使用できる次の一連のツールを提供します。

[Tools] メニュー項目	説明
Command Line Interface	コマンドを ASA に送信して結果を表示します。
Show Commands Ignored by ASDM on Device	ASDM に無視されたサポート対象外のコマンドを表示します。
Packet Tracer	指定した送信元アドレスとインターフェイスから宛先まで、パケットをトレースします。プロトコルおよびポートをデータ タイプに関わりなく指定でき、そこで実行された処理の詳細データを含むパケットの一部始終を表示できます。詳細については、ファイアウォールの設定ガイドを参照してください。
ping	ASAおよび関係する通信リンクのコンフィギュレーションや動作を検証し、他のネットワーク デバイスの基本的なテストを実行します。詳細については、ファイアウォールの設定ガイドを参照してください。
traceroute	パケットが宛先に到着するまでのルートを判断します。詳細については、ファイアウォールの設定ガイドを参照してください。
File Management	フラッシュ メモリに保存されたファイルを表示、移動、コピー、および削除します。また、フラッシュ メモリにディレクトリを作成することもできます。また、TFTP、フラッシュ メモリ、ローカル PC などさまざまなファイル システム間でファイル転送ができます。

[Tools] メニュー項目	説明
Check for ASA/ASDM Updates	ウィザードを使用して ASA ソフトウェアおよび ASDM ソフトウェアをアップグレードします。
Upgrade Software from Local Computer	ASA イメージ、ASDM イメージ、またはユーザー PC の他のイメージをフラッシュ メモリにアップロードします。
Downgrade Software	現在実行中のものよりも古い ASA イメージをロードします。
Backup Configurations	ASA のコンフィギュレーション、Cisco Secure Desktop イメージ、および SSL VPN Client イメージおよびプロファイルをバックアップします。
Restore Configurations	ASA のコンフィギュレーション、Cisco Secure Desktop イメージ、および SSL VPN Client イメージおよびプロファイルを復元します。
System Reload	ASDM を再起動し、保存したコンフィギュレーションをメモリにリロードします。
Administrator's Alert to Clientless SSL VPN Users	管理者が、クライアントレス SSL VPN ユーザーにアラート メッセージを送信できるようにします。詳細については、VPN 構成ガイドを参照してください。

[Tools] メニュー項目	説明
Migrate Network Object Group Members	8.3 以降に移行する場合、ASA は名前付きネットワーク オブジェクトを作成して、一部の機能のインライン IP アドレスを置き換えます。名前付きオブジェクトに加えて、ASDM はコンフィギュレーションで使用されているすべての IP アドレスに対して名前なしオブジェクトを自動的に作成します。これらの自動作成されるオブジェクトは *IP* アドレスによってのみ識別され、名前がなく、プラットフォーム設定に名前付きオブジェクトとしては存在しません。 移行の一部として名前付きオブジェクトを ASA が作成する場合、合致する非名前付き ASDM 専用オブジェクトは、名前付きオブジェクトに置換されます。唯一の例外は、ネットワーク オブジェクト グループの非名前付きオブジェクトです。ネットワーク オブジェクト グループ内にある IP アドレスの名前付きオブジェクトを ASA が作成する場合、ASDM は非名前付きオブジェクトを維持したまま、重複したオブジェクトを ASDM で作成します。これらのオブジェクトをマージするには、[Tools] > [Migrate Network Object Group Members] を選択します。 詳細については、「Cisco ASA 5500 Migration to Version 8.3 and Later」を参照してください。
Preferences	セッション間での特定の ASDM 機能の動作を変更します。
ASDM Java Console	Java コンソールを表示します。

[Wizards] メニュー

[Wizards] メニューにより、さまざまな機能を設定するウィザードを実行できます。

[Wizards] メニュー項目	説明
Startup Wizard	ASA の初期設定を段階的にガイドします。
VPN Wizard	さまざまな VPN 設定用のウィザードが用意されています。詳細については、VPN 構成ガイドを参照してください。

[Wizards] メニュー項目	説明
High Availability and Scalability Wizard	フェールオーバーの設定が可能になります：VPN クラスタ ロードバランシングまたは ASA 上の ASA クラスタリング
Unified Communication Wizard	ASA 上で、IP 電話などのユニファイド コミュニケーション機能の設定が可能になります。詳細については、ファイアウォールの設定ガイドを参照してください。
ASDM Identity Certificate Wizard	Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。このウィザードを使用して証明書をインストールするまでは、Java Web Start を使用して ASDM を起動することができます。詳細については、http://www.cisco.com/go/asdm-certificate を参照してください。
Packet Capture Wizard	ASA 上で、パケット キャプチャの設定が可能になります。このウィザードは、入出力インターフェイスのそれぞれでパケット キャプチャを 1 回実行します。キャプチャの実行後、キャプチャをコンピュータに保存し、パケット アナライザを使用してキャプチャを調査および分析できます。

[Window] メニュー

[Window] メニューを使用して、ASDM のウィンドウ間を移動できます。アクティブなウィンドウが選択されたウィンドウとして表示されます。

[Help] メニュー

[Help] メニューでは、オンライン ヘルプへのリンクの他に、ASDM と ASA の情報も提供されます。

[Help] メニュー項目	説明
Help Topics	新しいブラウザ ウィンドウが開いて ASDM のオンライン ヘルプが表示されます。ASDM で ASA Firepower モジュールを管理している場合は、この項目に **[ASDM Help Topics]** というラベルが表示されます。
ASA FirePOWER Help Topics	新しいブラウザ ウィンドウが開いて、ASA Firepower モジュールのオンライン ヘルプが表示されます。この項目は、ASDM でモジュールをインストールして管理している場合にだけ使用できます。
Help for Current Screen	表示されている画面に関する状況依存ヘルプが開きます。または、ツールバーの [? Help] ボタンをクリックすることもできます。
Release Notes	Cisco.com にある最新バージョンの [ASDM release notes] を開きます。リリース ノートには、ASDM のソフトウェアとハードウェア要件の最新情報、およびソフトウェア変更に関する最新情報が記載されています。
Cisco ASA Series Documentation	入手可能なすべての製品マニュアルへのリンクを含む Cisco.com 上のドキュメントが開きます。
ASDM Assistant	Cisco.com からダウンロード可能なコンテンツを検索でき、特定のタスクの実行に関する詳細がわかる **ASDM Assistant** を開きます。
About Cisco Adaptive Security Appliance (ASA)	ソフトウェア バージョン、ハードウェア構成、スタートアップ時にロードされるコンフィギュレーション ファイルやソフトウェア イメージなど、ASA に関する情報を表示します。これらはトラブルシューティングの際に役立つ情報です。
About Cisco ASDM	ソフトウェア バージョン、ホスト名、権限レベル、オペレーティング システム、デバイス タイプ、Java のバージョンなど、ASDM に関する情報を表示します。

ツールバー

メニューの下にある**ツールバー**から、ホーム ビュー、コンフィギュレーション ビュー、およびモニターリング ビューにアクセスできます。また、マルチ コンテキスト モードでシステムとセキュリティ コンテキストを選択したり、ナビゲーションおよびその他よく使用する機能を実行できます。

ツールバー ボタン	説明
Home	インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、ASA の重要な情報を表示できる [Home] ペインを表示します。マルチ モードの場合、[Home] ペインはありません。
Configuration	ASA を設定します。左側の [Navigation] ペインの機能ボタンをクリックして機能を設定します。
Monitoring	ASA をモニターします。左側の [Navigation] ペインの機能ボタンをクリックして、さまざまな要素をモニターします。
Save	書き込みアクセスが可能なコンテキストに限り、実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存します。 デバイス上に ASA FirePOWER モジュールがインストールされており、それを ASDM 経由で設定している場合は、このボタンに [Deploy] ボタンに置き換えられます。
Deploy	デバイス上に ASA FirePOWER モジュールがインストールされており、ASDM を経由で設定してる場合は、[Deploy] ボタンは [Save] ボタンを置き換え、次のオプションを含みます。 • [Deploy FirePOWER Changes]：モジュールに対する ASA FirePOWER モジュール ポリシーへの設定変更を保存します。 • [Save Running Configuration to Flash]：ASA 実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。これは、ASA FirePOWER モジュールを含まないデバイスの [Save] ボタンと同等です。
Refresh	現在の実行コンフィギュレーションで ASDM をリフレッシュします。ただし、モニターリング ペインのグラフはリフレッシュしません。
Back	直前に表示した ASDM のペインに戻ります。
Forward	直前に表示した ASDM のペインに進みます。
Help	その時点で表示されている画面の状況依存ヘルプを表示します。

ツールバー ボタン	説明
Search	ASDM内で機能を検索します。検索機能は、各ペインのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、該当ペインがただちに表示されます。[Back] または [Forward] をクリックすると、検出した2つのペインをすばやく切り替えることができます。

ASDM Assistant

ASDM Assistant では、タスクに応じた ASDM の使用方法のヘルプを検索し、表示できます。この機能は、シングル コンテキストとシステム コンテキストのルーテッド モードおよびトランスペアレント モードで使用できます。

[View] > **[ASDM Assistant]** > **[How Do I?]** の順に選択するか、メニューバーの [Look For] フィールドから検索リクエストを入力して情報にアクセスします。[Find] ドロップダウン リストから [How Do I?] を選択すると、検索が開始します。

ASDM Assistant を使用するには、次の手順を実行します。

手順

ステップ 1 **[View]** > **[ASDM Assistant]** を選択します。

[ASDM Assistant] ペインが表示されます。

ステップ 2 [Search] フィールドに検索する情報を入力して [Go] をクリックします。

要求された情報が [Search Results] ペインに表示されます。

ステップ 3 [Search Results] 領域および [Features] 領域に表示される任意のリンクをクリックし、詳細情報を入手します。

ステータス バー

ステータス バーは ADSM ウィンドウの下部に表示されます。次の表に、左から右に表示される領域を示します。

エリア	説明
Status	コンフィギュレーションのステータス（「Device configuration loaded successfully.」など）。

エリア	説明
Failover	フェールオーバー装置のステータスで、アクティブまたはスタンバイのいずれか。
User Name	ASDM ユーザーのユーザー名。ユーザー名なしでログインした場合、ユーザー名は「admin」です。
User Privilege	ASDM ユーザーの特権。
Commands Ignored by ASDM	アイコンをクリックすると、ASDM で処理されなかったコンフィギュレーションのコマンドのリストが表示されます。これらのコマンドはコンフィギュレーションから削除されません。
Connection to Device	ASDM の ASA との接続ステータス。
Syslog Connection	syslog 接続が動作しており、ASA が監視されています。
SSL Secure	ASDM への接続に SSL を使用し、安全であることを示します。
時刻	ASA に設定された時刻。

Connection to Device

ASDM は ASA との接続を常に維持し、[Monitoring] ペインおよび [Home] ペインのデータを最新に保ちます。このダイアログボックスに接続ステータスが表示されます。コンフィギュレーションを変更する場合、変更している間 ASDM は接続をもう一つ開き、変更が終わるとその接続を閉じますが、このダイアログボックスには 2 つ目の接続は表示されません。

Device List

[Device List] はドッキング可能なペインです。ヘッダーにある 3 つのボタンをそれぞれクリックすると、ペインの最大化または復元、移動可能なフローティングペインへの変更、ペインの非表示化、またはペインを閉じることができます。このペインはホーム、コンフィギュレーション、モニターリング、およびシステムの各ビューで使用できます。このペインを使用して、別のデバイスに切り替えたり、システムとコンテキスト間で切り替えたりすることができますが、現在実行中のものと同じバージョンの ASDM がそのデバイスでも動作している必要があります。ペインを完全に表示するには、少なくとも 2 つのデバイスがリストに表示されている必要があります。このペインは、シングル コンテキスト、マルチ コンテキストおよびシステム コンテキストのルーテッド モードおよびトランスペアレント モードで使用できます。

このペインを使用して別のデバイスに接続するには、次の手順を実行します。

手順

ステップ 1 [Add] をクリックしてリストに別のデバイスを追加します。

[Add Device] ダイアログボックスが表示されます。

ステップ 2 デバイス名またはデバイスの IP アドレスを入力し、[OK] をクリックします。

ステップ 3 リストから選択したデバイスを削除するには、[Delete] をクリックします。

ステップ 4 [Connect] をクリックして別のデバイスに接続します。

[Enter Network Password] ダイアログボックスが表示されます。

ステップ 5 ユーザー名とパスワードを該当するフィールドに入力し、[Login] をクリックします。

共通ボタン

多くの ASDM ペインには、次の表に示すボタンが含まれています。目的の作業を完了するには、該当するボタンをクリックします。

ボタン	説明
適用	ASDM での変更内容を ASA に送信し、実行コンフィギュレーションに適用します。
Save	実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
Reset	変更内容を破棄して、変更前、または [Refresh] や [Apply] を最後にクリックした時点の表示情報に戻します。[Reset] をクリックした後、[Refresh] をクリックして、現在の実行コンフィギュレーションの情報が表示されていることを確認します。
Restore Default	選択した設定をクリアしてデフォルト設定に戻します。
Cancel	変更内容を破棄して、前のペインに戻ります。
Enable	機能について読み取り専用の統計情報を表示します。
Close	開いているダイアログボックスを閉じます。

ボタン	説明
Clear	フィールドから情報を削除します。または、チェックボックスをオフにします。
Back	前のペインに戻ります。
Forward	次のペインに移動します。
Help	選択したペインまたはダイアログボックスを表示します。

キーボードのショートカット

キーボードを使用して ASDM ユーザー インターフェイスをナビゲートできます。

次の表に、ASDM ユーザー インターフェイスの 3 つの主要な領域間を移動するために使用可能なキーボード ショートカットの一覧を示します。

表 *2:* メイン ウィンドウ内のキーボード ショートカット

表示対象	Windows/Linux	MacOS
[Home] ペイン	Ctrl+H	Shift+Command+H
[Configuration] ペイン	Ctrl+G	Shift+Command+G
[Monitoring] ペイン	Ctrl+M	Shift+Command+M
Help	F1	Command+?
Back	Alt+左矢印	Command+[
Forward	Alt+右矢印	Command+]
表示のリフレッシュ	F5	Command+R
Cut	Ctrl+X	Command+X
Copy	Ctrl+C	Command+C
Paste	Ctrl+V	Command+V
コンフィギュレーションの保存	Ctrl+S	Command+S
ポップアップ メニュー	Shift+F10	—
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W

表示対象	Windows/Linux	MacOS
Find	Ctrl+F	Command+F
Exit	Alt+F4	Command+Q
テーブルまたはテキスト領域の終了	Ctrl_Shift または Ctrl+Shift+Tab	Ctril+Shift または Ctrl+Shift+Tab

次に表に、ペイン内部のナビゲーションに使用可能なキーボードショートカットの一覧を示します。

表 *3:* ペイン内のキーボード ショートカット

フォーカスの移動先	キー
次のフィールド	タブ
前のフィールド	Shift+Tab
次のフィールド（テーブル内にフォーカスがある場合）	Ctrl+Tab
前のフィールド（テーブル内にフォーカスがある場合）	Shift+Ctrl+Tab
次のタブ（タブにフォーカスがある場合）	右矢印
前のタブ（タブにフォーカスがある場合）	左矢印
テーブル内の次のセル	タブ
テーブル内の前のセル	Shift+Tab
次のペイン（複数のペインが表示されている場合）	F6
前のペイン（複数のペインが表示されている場合）	Shift+F6

次の表に、Log Viewer で使用可能なキーボード ショートカットの一覧を示します。

表 *4:* ログ ビューアのキーボード ショートカット

目的	Windows/Linux	MacOS
Real-Time Log Viewer の一時停止および再開	Ctrl+U	Command+
ログ バッファ ペインのリフレッシュ	F5	Command+R

目的	Windows/Linux	MacOS
内部ログバッファの消去	Ctrl+Delete	Command+Delete
選択したログ エントリのコピー	Ctrl+C	Command+C
ログの保存	Ctrl+S	Command+S
印刷	Ctrl+P	Command+P
セカンダリ ウィンドウを閉じる	Alt+F4	Command+W

次の表に、メニュー項目へのアクセスに使用可能なキーボードショートカットの一覧を示します。

表 *5:* メニュー項目にアクセスするためのキーボード ショートカット

アクセス対象	Windows/Linux
メニュー バー	Alt
次のメニュー	右矢印
前のメニュー	左矢印
次のメニュー オプション	下矢印
前のメニュー オプション	上矢印
選択したメニュー オプション	Enter

ASDM ペインの検索機能

一部の ASDM ペインには、多くの要素を持つテーブルが含まれています。特定のエントリを簡単に検索および強調表示して編集するために、複数の ASDM ペインには、これらのペイン内のオブジェクトを検索できる検索機能が含まれています。

検索を実行する場合は、[Find] フィールドにフレーズを入力し、特定のペイン内のすべてのカラムを検索できます。フレーズにはワイルドカード文字の「*」および「?」を含めることができます。* は 1 つ以上の文字と一致し、? は 1 つの文字と一致します。[Find] フィールドの右にある上矢印と下矢印を使用して、次（上）または前（下）のフレーズの出現に移動します。[Match Case] チェックボックスをオンにすると、入力した大文字および小文字に正確に一致するエントリを検索します。

たとえば、B*ton-L* と入力すると、次の一致が返されます。

```
Boston-LA, Boston-Lisbon, Boston-London
```

Bo?ton と入力すると、次の一致が返されます。

```
Boston, Bolton
```

ルール リストの検索機能

ACL や ACE およびその他のルールにはさまざまなタイプの多数の要素が含まれているため、ルールを表示する任意のペインの検索機能では、他のペインの検索機能よりも対象を絞った検索を実行できます。これには、アクセス ルール、サービス ポリシー ルール、ACL Manager、ACL ルールを一覧表示するその他のペイン、および NAT ルールも含まれます。

ルール リスト内で要素を検索するには、次の手順を実行します。

手順

ステップ 1 [Find] をクリックします。

ステップ 2 [Filter] フィールドで、ドロップダウン リストから次のオプションのいずれかを選択します。

検索可能な項目は、ルール タイプによって異なり、表の列に対応しています。複数のフィールドを使用する複雑な検索を作成する場合は、[Query] を選択します。

ステップ 3 [Query] を選択しなかった場合は、2 番目のフィールドで、ドロップダウン リストから次のいずれかのオプションを選択します。

- [is]：検索文字列に対する完全一致を指定します。 これは常にクエリのオプションです。
- [contains]：検索文字列の一部または全部を含む任意のルールに対する一致を指定します。

ステップ 4 3 番目のフィールドに、検索する文字列を入力します。**...** をクリックすると、リストからオブジェクトを選択できます。クエリを使用している場合は、[Define Query] をクリックします。

IP アドレスを検索する場合は、ASDM によって作成されたオブジェクトまたはグループである限り、ネットワーク オブジェクトまたはグループ内のアドレスに一致するものを取得できます。つまり、グループ名は DM_INLINE で始まります。検索機能は、ユーザーが作成したオブジェクト内の IP アドレスを検索できません。

ステップ 5 検索を実行するには、[Filter] をクリックします。

ビューが更新され、一致するルールのみが表示されます。ルール番号は、ルール リスト内の絶対位置を確認できるように維持されます。

ステップ 6 [Clear] をクリックすると、フィルタが削除され、リスト全体が再度表示されます。

ステップ 7 完了したら、赤色の **x** をクリックして検索コントロールを閉じます。

拡張スクリーン リーダ サポートの有効化

デフォルトでは、Tab キーを押してペイン内を移動するときに、ラベルと説明はタブの移動先から除外されます。JAWS のような一部のスクリーン リーダだけが、フォーカスのある画面オブジェクトを読み取ります。拡張スクリーン リーダ サポートをイネーブルにすると、ラベルと説明にもタブを移動させることができます。

拡張スクリーン リーダ サポートをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 **[Tools]** > **[Preferences]** の順に選択します。

[Preferences] ダイアログボックスが表示されます。

ステップ 2 [General] タブの [Enable screen reader support] チェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 スクリーン リーダ サポートをアクティブにするには、ASDM を再起動します。

整理用フォルダー

コンフィギュレーション ビューおよびモニターリング ビューのナビゲーション ペインに含まれる一部のフォルダには、関連付けられたコンフィギュレーション ペインやモニターリング ペインがありません。これらのフォルダは、関連するコンフィギュレーション タスクやモニターリング タスクを整理するために使用します。これらのフォルダをクリックすると、右側の [Navigation] ペインにサブ項目のリストが表示されます。サブ項目の名前をクリックするとその項目に移動できます。

[Home] ペイン（シングル モードとコンテキスト）

ASDM の [Home] ペインでは、ASA に関する重要な情報を表示できます。[Home] ペインのステータス情報は 10 秒間隔で更新されます。このペインには通常、[Device Dashboard] と [Firewall Dashboard] の 2 つのタブがあります。

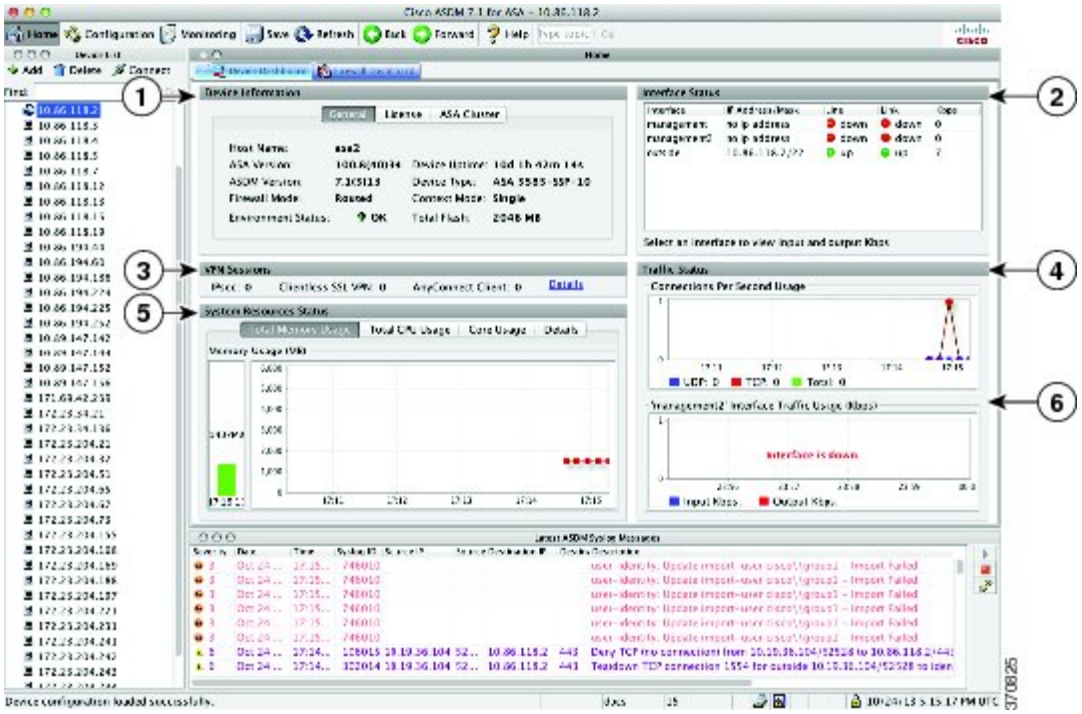
IPS モジュール、CX モジュール、ASA Firepower モジュールなどのハードウェアまたはソフトウェア モジュールがデバイスにインストールされている場合は、それ専用のタブが表示されます。

[Device Dashboard] タブ

[Device Dashboard] タブでは、インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、ASA の重要な情報を一目で確認できます。

次の図に、[Device Dashboard] タブの要素を示します。

図 *2 : [Device Dashboard]* タブ



凡例

GUI 要素	説明
1	[Device Information] ペイン （81 ページ）
2	[Interface Status] ペイン （82 ページ）
3	[VPN Sessions] ペイン （82 ページ）
4	[Traffic Status] ペイン （83 ページ）
5	[System Resources Status] ペイン （83 ページ）
6	[Traffic Status] ペイン （83 ページ）
—	Device List （73 ページ）

GUI 要素	説明
—	[Latest ASDM Syslog Messages] ペイン （83 ページ）

[Device Information] ペイン

[Device Information] ペインには、[General] タブと [License] タブというデバイス情報を表示する 2 つのタブがあります。[General] タブでは、システム ヘルスが一目でわかる [Environment Status] ボタンにアクセスできます。

[General] タブ

このタブには、ASA に関する次の基本情報が表示されます。

- [Host name]：デバイスのホスト名を表示します。
- [ASA version]：デバイス上で実行されている ASA ソフトウェアのバージョンを示します。
- [ASDM version]：デバイス上で実行されている ASDM ソフトウェアのバージョンを表示します。
- [Firewall mode]：デバイスが実行されているファイアウォール モードを表示します。
- [Total flash]：現在使用されている RAM の合計を表示します。
- [ASA Cluster Role]：クラスタリングが有効の場合に、この装置のロール（マスターまたはスレーブ）を表示します。
- [Device uptime]：最後にソフトウェアをアップロードしてから、デバイスが動作している時間を表示します。
- [Context mode]：デバイスが実行されているコンテキスト モードを表示します。
- [Total Memory]：ASA にインストールされている DRAM を表示します。
- [Environment status]：システム ヘルスを表示します。[General] タブの [Environment Status] というラベルの右側にあるプラス記号（+）をクリックして、ハードウェア統計情報を表示します。設置されている電源装置数の確認、ファンと電源モジュールの動作ステータスの追跡、および CPU の温度とシステムの周囲温度の追跡を実行できます。

  一般に、[Environment Status] ボタンでシステム ヘルスが一目でわかります。システム内のモニター対象のすべてのハードウェア コンポーネントが正常な範囲内で動作している場合、プラス記号（+）ボタンには [OK] が緑で表示されます。一方、ハードウェア システム内のコンポーネントが 1 つでも正常な範囲外で動作している場合は、プラス記号（+）ボタンが赤色の丸になってクリティカル ステータスを示し、ハードウェア コンポーネントに関してすぐに対処が必要であることを示します。

  特定のハードウェアの統計情報に関する詳細については、そのデバイスの『ハードウェア ガイド』を参照してください。

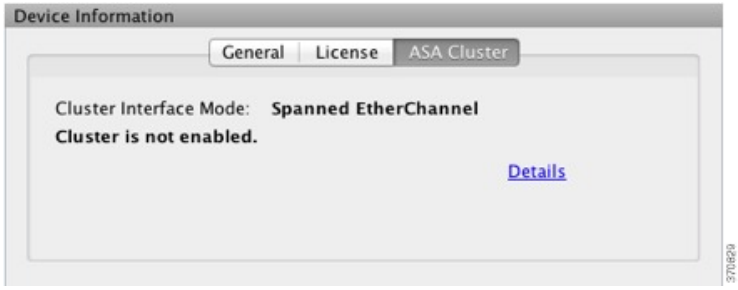
（注） 最新リリースの ASA にアップグレードするにはメモリが不足している場合は、[Memory Insufficient Warning] ダイアログボックスが表示されます。このダイアログボックスに表示される指示に従って、サポートされている方法で ASA および ASDM を継続して使用します。[OK] をクリックして、このダイアログボックスを閉じます。

[License] タブ

このタブには、ライセンス機能のサブセットが表示されます。詳細なライセンス情報の表示または新しいアクティベーション キーの入力を行うには、[More Licenses] をクリックします。[Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインが表示されます。

[Cluster] タブ

このタブには、クラスタのインターフェイス モードおよびクラスタのステータスが表示されます。



[Virtual Resources] タブ（ASAv）

このタブは、ASA によって使用されている仮想リソースを表示します。vCPU の数、RAM、ASA のプロビジョニングの過不足が含まれます。

[Interface Status] ペイン

このペインには、各インターフェイスのステータスが表示されます。インターフェイスの行を選択すると、入力および出力スループットが Kbps 単位でテーブルの下に表示されます。

[VPN Sessions] ペイン

このペインには、VPN トンネル ステータスが表示されます。[Details] をクリックすると、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] ペインに移動します。

[Failover Status] ペイン

このペインには、フェールオーバー ステータスが表示されます。

[Configure] をクリックして、High Availability and Scalability Wizard を起動します。このウィザードを完了すると、フェールオーバー コンフィギュレーション ステータス（[Active/Active] または [Active/Standby]）が表示されます。

フェールオーバーが設定されている場合は、[Details] をクリックすると、[Monitoring] > [Properties] > [Failover] > [Status] ペインが開きます。

[System Resources Status] ペイン

このペインには、CPU およびメモリの使用状況に関する統計情報が表示されます。

[Traffic Status] ペイン

このペインには、インターフェイス全体の接続数/秒と、最も遅いセキュリティ インターフェイスのトラフィック スループットのグラフが表示されます。

コンフィギュレーションにセキュリティ レベルが最も低いインターフェイスが複数含まれており、そのいずれかの名前が「outside」である場合、そのインターフェイスがトラフィック スループットのグラフに使用されます。それ以外の場合、ASDM はセキュリティ レベルが最も低いインターフェイスのアルファベット順のリストから最初のインターフェイスを選択します。

[Latest ASDM Syslog Messages] ペイン

このペインには、ASA が生成した最新のシステム メッセージが 100 個まで表示されます。ロギングがディセーブルになっている場合は、[Enable Logging] をクリックしてイネーブルにします。

次の図に、[Latest ASDM Syslog Messages] ペインの要素を示します。

図 *3 : [Latest ASDM Syslog Messages]* ペイン

凡例

GUI 要素	説明
1	ペインのサイズを変更するには、**ディバイダ**を上または下にドラッグします。
2	ペインを展開します。ペインをデフォルトのサイズに戻すには、**二重の正方形**のアイコンをクリックします。

GUI 要素	説明
3	フローティング ペインを作成します。ペインをドッキングするには、**ドッキングしたペイン** アイコンをクリックします。
4	自動非表示をイネーブルまたはディセーブルにします。自動非表示がイネーブルな場合は、左下隅にある [Latest ASDM Syslog Messages] ボタンの上にカーソルを移動すると、ペインが表示されます。カーソルをペインから離すと、ペインは非表示になります。
5	ペインを閉じます。ペインを表示するには、[View Latest ASDM Syslog Messages] を選択します。
6	右側にある**緑**のアイコンをクリックすると、syslogメッセージの表示の更新を続行します。
7	右側にある**赤い**アイコンをクリックすると、syslogメッセージの表示の更新を停止します。
8	右側にある**フィルタ** アイコンをクリックすると、[Logging Filters] ペインが開きます。

- イベントを右クリックして [Clear Content] を選択すると、現在のメッセージを消去します。
- イベントを右クリックして [Save Content] をクリックすると、現在のメッセージを PC 上のファイルに保存します。
- イベントを右クリックして [Copy] を選択すると、現在の内容をコピーします。
- イベントを右クリックして [Color Settings] を選択すると、重大度に基づいて syslog メッセージの背景色と前景色を変更します。

[Firewall Dashboard] タブ

[Firewall Dashboard] タブでは、ASA を通過するトラフィックに関する重要な情報を確認できます。このダッシュボードは、シングル コンテキスト モードまたはマルチ コンテキスト モードのどちらであるかにより異なります。マルチ コンテキスト モードでは、[Firewall Dashboard] は各コンテキスト内に表示できます。

次の図に、[Firewall Dashboard] タブの要素の一部を示します。

図 *4 : [Firewall Dashboard]* タブ

凡例

GUI 要素	説明
1	[Traffic Overview] ペイン （85 ページ）
2	[Top 10 Access Rules] ペイン （86 ページ）
3	[Top Usage Status] ペイン （86 ページ）
（表示なし）	[Top Ten Protected Servers Under SYN Attack] ペイン （87 ページ）
（表示なし）	[Top 200 Hosts] ペイン （87 ページ）
（表示なし）	[Top Botnet Traffic Filter Hits] ペイン （87 ページ）

[Traffic Overview] ペイン

デフォルトでは、イネーブルです。基本脅威検出をディセーブルにすると（『ファイアウォールの設定ガイド』を参照）、この領域には [Enable] ボタンが表示されます。[Enable] ボタンを使用して基本脅威検出をディセーブルにできます。実行時の統計情報には、表示専用の次の情報が含まれます。

- 接続数と NAT 変換数。
- アクセス リストによる拒否およびアプリケーション インスペクションによってドロップされたパケット数/秒。
- ドロップ パケット数/秒。これは、スキャン攻撃の一部として特定される場合と、不完全なセッションとして検出される場合（TCP SYN 攻撃やデータなし UDP セッション攻撃を検出した場合など）があります。

[Top 10 Access Rules] ペイン

デフォルトでは、イネーブルです。アクセスルールの脅威検出統計情報をディセーブルにすると（『ファイアウォールの設定ガイド』を参照）、この領域には [Enable] ボタンが表示されます。[Enable] ボタンを使用してアクセス ルールの統計情報を有効にできます。

テーブル ビューでは、リストからルールを選択して右クリックし、ポップアップ メニュー項目の [Show Rule] を表示できます。この項目を選択して [Access Rules] テーブルに移動し、テーブル内にあるそのルールを選択します。

[Top Usage Status] ペイン

デフォルトでは、ディセーブルです。このペインには、次の 4 つのタブがあります。

- [Top 10 Services]：脅威検出サービス
- [Top 10 Sources]：脅威検出サービス
- [Top 10 Destinations]：脅威検出サービス
- [Top 10 Users]：アイデンティティ ファイアウォール サービス

最初の 3 つのタブ（[Top 10 Services]、[Top 10 Sources]、および [Top 10 Destinations]）では、脅威検出サービスに関する統計情報を提供します。各タブには、それぞれの脅威検出サービスをイネーブルにする [Enable] ボタンがあります。『ファイアウォールの設定ガイド』に従って、これらを有効にできます。

[Top 10 Services Enable] ボタンを使用すると、ポートとプロトコルの両方の統計情報がイネーブルになります（どちらも表示用にイネーブルにする必要があります）。[Top 10 Sources] ボタンおよび [Top 10 Destinations Enable] ボタンを使用すると、ホストの統計情報がイネーブルになります。ホスト（送信元および宛先）の上位使用ステータス統計情報、およびポートとプロトコルが表示されます。

4 番目のタブ [Top 10 Users] では、アイデンティティ ファイアウォール サービスに関する統計情報を提供します。アイデンティティ ファイアウォール サービスでは、ユーザーのアイデンティティに基づくアクセス コントロールを提供します。送信元 IP アドレスではなくユーザー名とユーザー グループ名に基づいてアクセスルールとセキュリティ ポリシーを設定できます。ASA は、IP とユーザーのマッピング データベースにアクセスして、このサービスを提供します。

[Top 10 Users] タブは、次のいずれかを設定した場合のみ、データを表示します。

- Identity Firewall サービス コンフィギュレーション：Microsoft Active Directory および Cisco Active Directory（AD）エージェンの追加コンポーネントの設定を含みます。Identity Firewall サービスは、**user-identity enable** コマンド（デフォルトで有効）および **user-accounting statistics** コマンドを衣装して有効化されます。
- VPN ユーザーの認証、認可またはアカウンティングを行うために RADIUS サーバーを使用する VPN コンフィギュレーション。

選択したオプションに応じて、[Top 10 Users] タブに、上位 10 ユーザーの受信した EPS パケット、送信した EPS パケット、および送信された攻撃に関する統計情報が表示されます。（*domain\user_name* として表示される）各ユーザーに関して、このタブには、そのユーザーの平均 EPS パケット、現在の EPS パケット、トリガー、および合計イベント数が表示されます。

⚠

注意 拡張統計情報を有効にすると、有効にする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きな影響があります。トラフィックの負荷が高い場合は、このタイプの統計情報は一時的にイネーブルにすることを検討してください。ただし、ポートの統計情報をイネーブルにしても、それほど影響はありません。

[Top Ten Protected Servers Under SYN Attack] ペイン

デフォルトでは、ディセーブルです。この領域に表示されている [Enable] ボタンを使用して、この機能を有効にできます。または、『ファイアウォール設定ガイド』に従って有効にすることもできます。攻撃を受けて保護された上位 10 サーバーの統計情報が表示されます。

平均攻撃レートの場合、ASA はレート間隔（デフォルトは 30 分）に対して 30 秒ごとにデータをサンプリングします。

複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。

[Detail] をクリックして、10 台のサーバーだけでなく、すべてのサーバー（最大 1000 台）の統計情報を表示します。履歴サンプリング データを確認することもできます。ASA はレート間隔の間に攻撃の数を 60 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

[Top 200 Hosts] ペイン

デフォルトでは、ディセーブルです。ASA を介して接続中の上位 200 のホストを表示します。ホストの各エントリには、ホストの IP アドレスと、ホストによって開始された接続の数が含まれ、このエントリは 120 秒ごとにアップデートされます。この表示をイネーブルにするには **hpm topnenable** コマンドを入力します。

[Top Botnet Traffic Filter Hits] ペイン

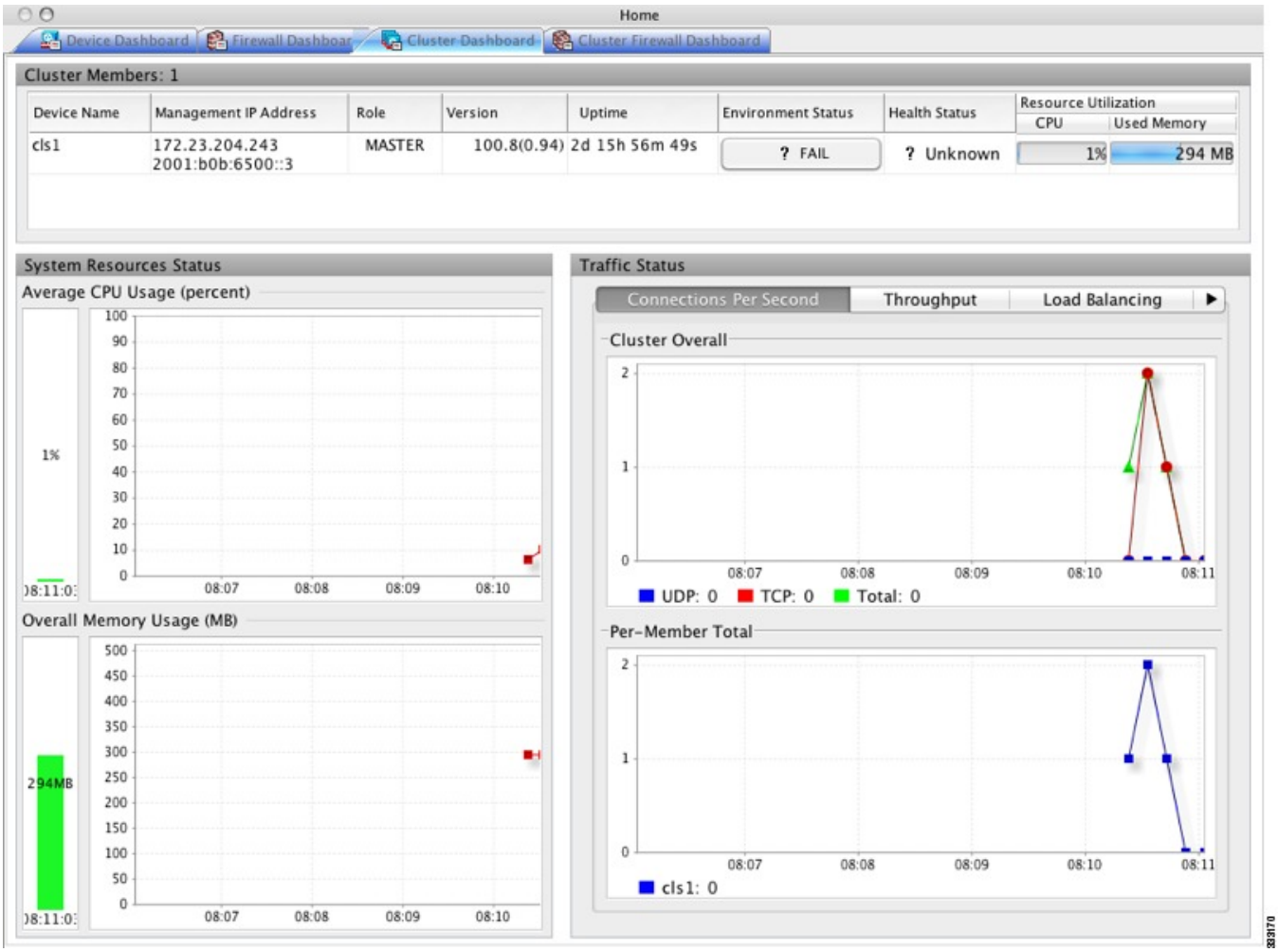
デフォルトでは、ディセーブルです。この領域には、ボットネット トラフィック フィルタを設定するためのリンクが含まれています。上位 10 個のボットネット サイト、ポート、および感染ホストのレポートは、データのスナップショットを提供し、統計情報の収集開始以降の上

位 10 項目に一致しない場合があります。IP アドレスを右クリックすると、whois ツールが起動してボットネット サイトの詳細が表示されます。

詳細については、『ボットネット設定ガイド』を参照してください。

[Cluster Dashboard] タブ

ASA クラスタリングをイネーブルにして、マスター ユニットに接続している場合は、[Cluster Dashboard] タブにクラスタのメンバーシップとリソース使用率の概要が表示されます。



- [Cluster Members]：クラスタを構成するメンバーの名前と基本情報（管理 IP アドレス、バージョン、クラスタ内のロールなど）およびメンバーのヘルス ステータス（環境ステータス、ヘルス ステータス、およびリソース使用率）を表示します。

(注) マルチコンテキストモードでは、管理コンテキストにASDMを接続し、次に別のコンテキストに変更しても、リスト表示されている管理IPアドレスは現在のコンテキストの管理IPアドレスに変更されません。ASDMが現在接続されているメインクラスタのIPアドレスを含む管理コンテキストの管理IPアドレスを、引き続き表示し続けます。

- [System Resource Status]：クラスタ全体のリソース使用率（CPU およびメモリ）とトラフィックのグラフ（クラスタ全体およびデバイスごと）を表示します。
- [Traffic Status]：各タブには次のグラフがあります。
  - [Connections Per Second] タブ

    [Cluster Overal]：クラスタ全体の秒単位の接続数が表示されます。

    [Per-Member Total]：各メンバーの秒単位の平均接続数が表示されます。
  - [Throughput] タブ

    [Cluster Overall]：クラスタ全体の総出力スループットが表示されます。

    [Per-Member Throughput]：メンバーのスループットが、メンバーごとに 1 行ずつ表示されます。
  - [Load Balancing] タブ

    [Per-Member Percentage of Total Traffic]：メンバーが受信した総クラスタ トラフィックの割合が、メンバーごとに表示されます。

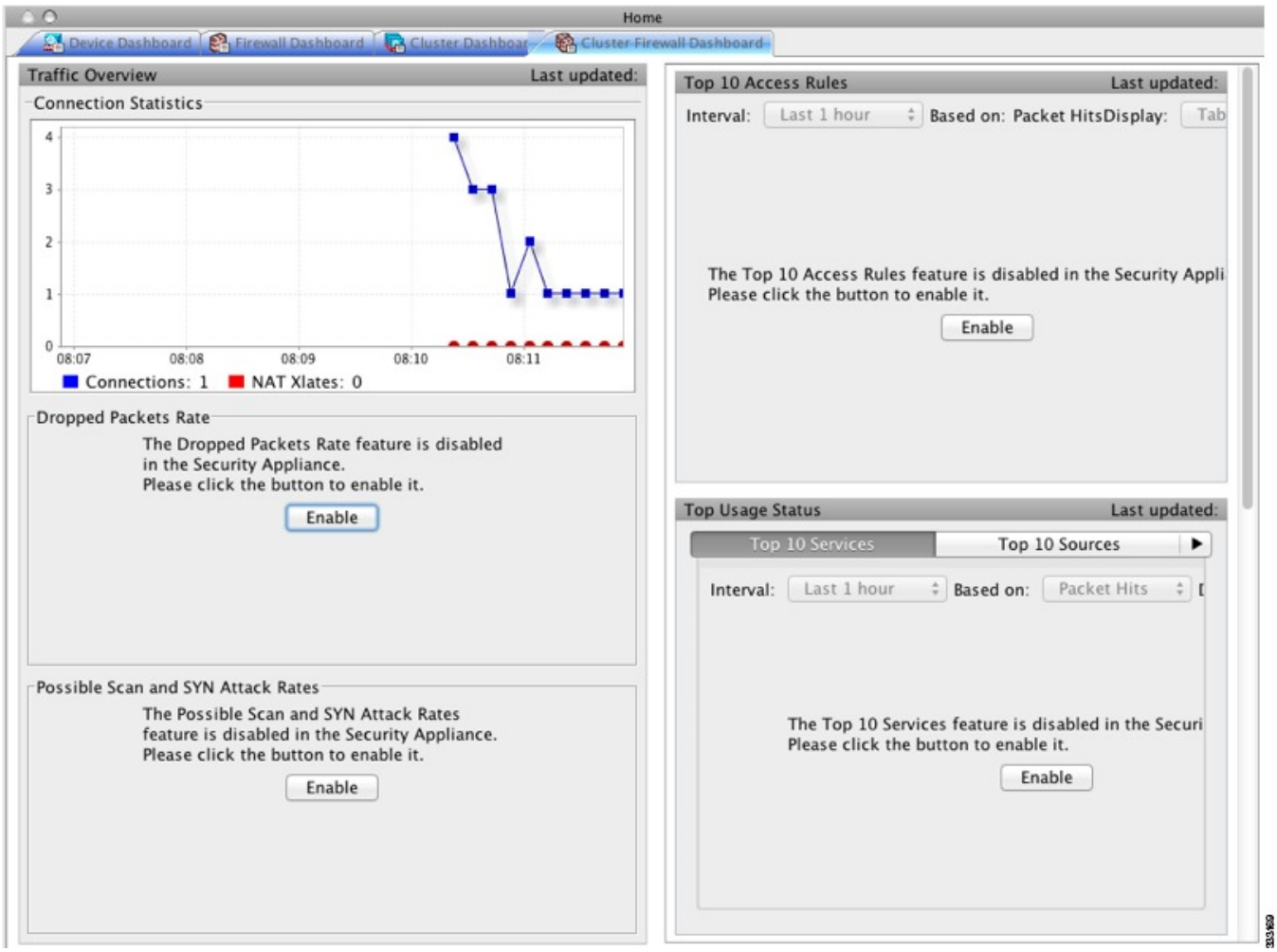
    [Per-Member Locally Processed Traffic]：ローカルに処理されたトラフィックの割合が、メンバーごとに表示されます。
  - [Control Link Usage] タブ

    [Per-Member Receival Capacity Utilization]：送信容量の使用率が、メンバーごとに表示されます。

    [Per-Member Transmittal Capacity Utilization]：受信容量の使用率が、メンバーごとに表示されます。

[Cluster Firewall Dashboard] タブ

[Cluster Firewall Dashboard] タブには、[Firewall Dashboard] に表示される情報と同様のトラフィックの概要および「top N」統計情報が表示されますが、クラスタ全体にわたる総計は表示されません。



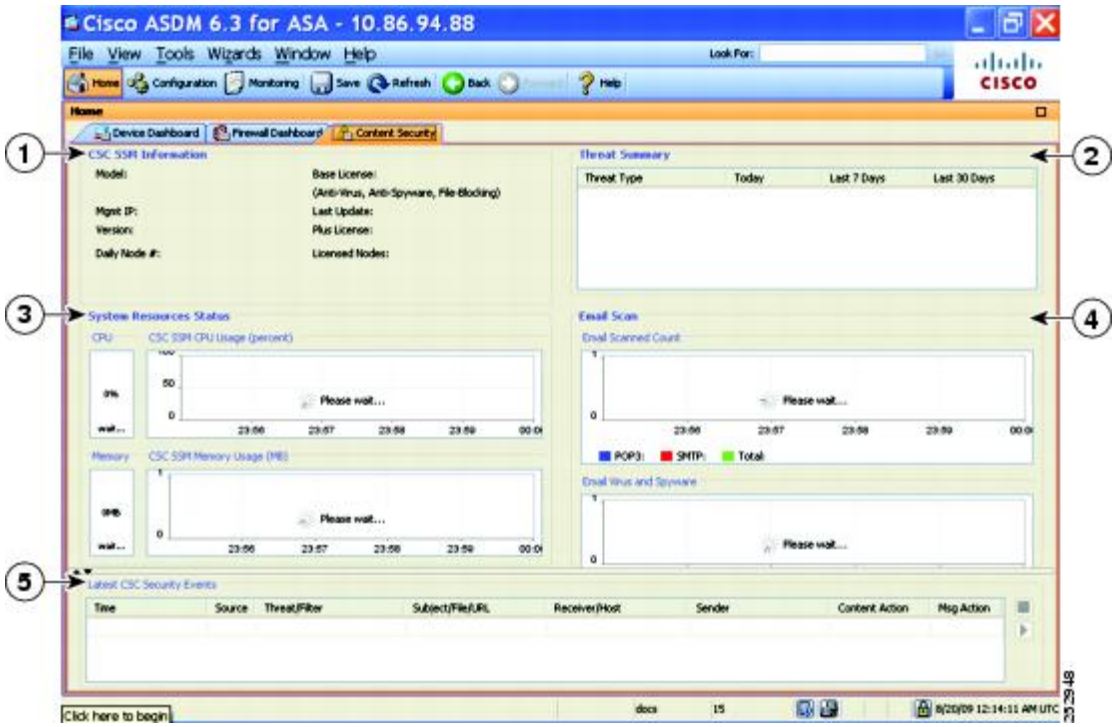
[Content Security] タブ

[Content Security] タブでは、CSC（Content Security and Control）SSM に関する重要な情報を確認できます。このペインは、CSC SSM で動作している CSC ソフトウェアが ASA にインストールされている場合のみ表示されます。

（注） [Configuration] > [Trend Micro Content Security] > [CSC Setup] を選択して **CSC Setup Wizard** を完了していないと、[Home] > [Content Security] の下にあるペインにアクセスできません。代わりにダイアログボックスが表示され、この場所から **CSC Setup Wizard** に直接アクセスできます。

次の図に、[Content Security] タブの要素を示します。

図 *5 : [Content Security]* タブ



凡例

GUI 要素	説明
1	[CSC SSM Information] ペイン。
2	[Threat Summary] ペイン。CSC SSM により検出された脅威の集約データを表示します。ウイルス、スパイウェア、フィルタリングまたはブロックされた URL、ブロックされたスパム、ブロックされたファイル、損害制御サービスなどがあります。
3	[System Resources Status] ペイン。
4	[Email Scan] ペイン。グラフには、10 秒間隔でデータが表示されます。
5	[Latest CSC Security Events] ペイン。

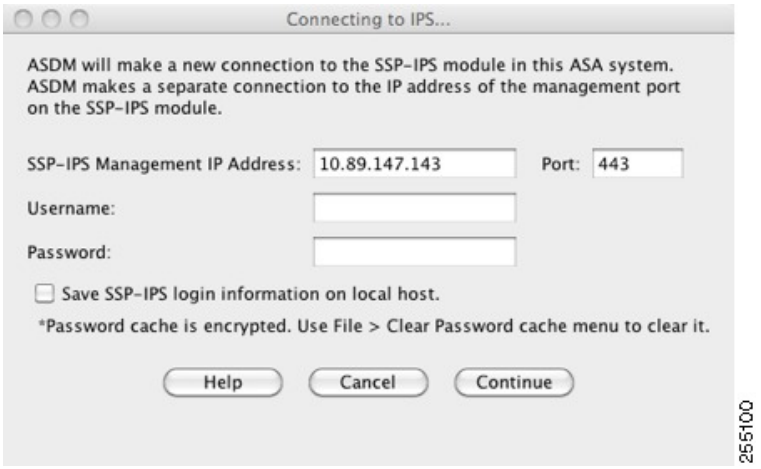
[Intrusion Prevention] タブ

[Intrusion Prevention] タブでは、IPS に関する重要な情報を確認できます。このタブは、ASA に IPS モジュールがインストールされている場合にのみ表示されます。

IPS モジュールに接続するには、次の手順を実行します。

1. [Intrusion Prevention] タブをクリックします。

   [Connecting to IPS] ダイアログボックスが表示されます。

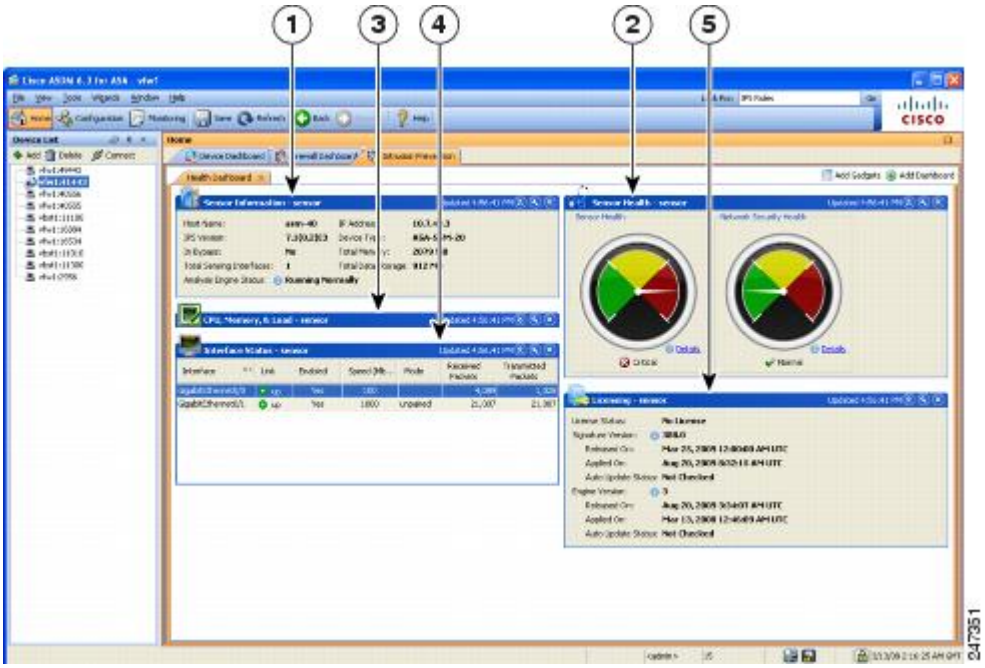


2. IP アドレス、ポート、ユーザー名、およびパスワードを入力します。デフォルトの IP アドレスとポートは 192.168.1.2:443 です。デフォルトのユーザー名およびパスワードは、**cisco** と **cisco** です。
3. ログイン情報をローカル PC に保存するには、[Save IPS login information on local host] チェックボックスをオンにします。
4. [Continue] をクリックします。

侵入防御に関する詳細については、『IPS クイック スタート ガイド』を参照してください。

次の図に、[Intrusion Prevention] タブにある [Health Dashboard] タブの要素を示します。

図 *6 : [Intrusion Prevention]* タブ（*Health Dashboard*）

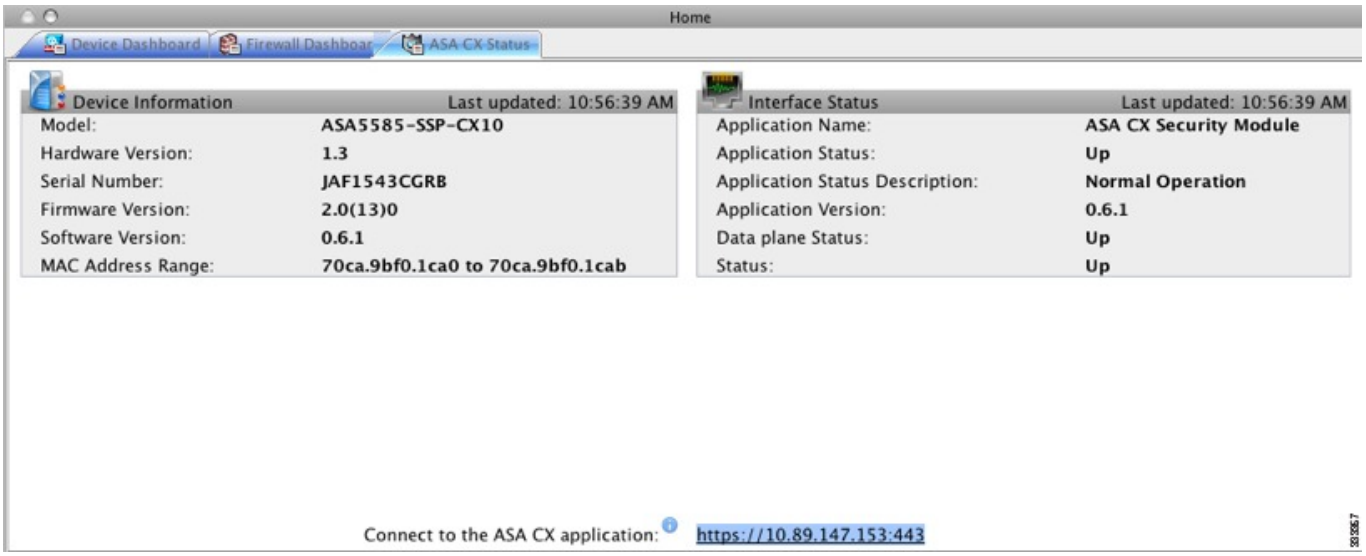


凡例

GUI 要素	説明
1	[Sensor Information] ペイン。
2	[Sensor Health] ペイン。
3	[CPU, Memory, and Load] ペイン。
4	[Interface Status] ペイン。
5	[Licensing] ペイン。

[ASA CX Status] タブ

[ASA CX Status] タブには、ASA CX モジュールに関する重要な情報が表示されます。このタブは、ASA に ASA CX モジュールがインストールされている場合にのみ表示されます。



[ASA Firepower Status] タブ

[ASA FirepowerStatus] タブには、このモジュールに関する情報が表示されます。この情報には、モデル、シリアル番号、ソフトウェア バージョンなどのモジュール情報と、アプリケーション名、アプリケーション ステータス、データ プレーン ステータス、全体のステータスなどのモジュール ステータスが含まれます。モジュールが FireSIGHT Management Center に登録されている場合は、リンクをクリックしてアプリケーションを開き、詳細な分析やモジュールの設定を行うことができます。

このタブは、ASA Firepower モジュールがデバイスにインストールされている場合にのみ表示されます。

FireSIGHT Management Center ではなく ASDM を使用して ASA Firepower モジュールを管理している場合は、追加のタブが表示されます。

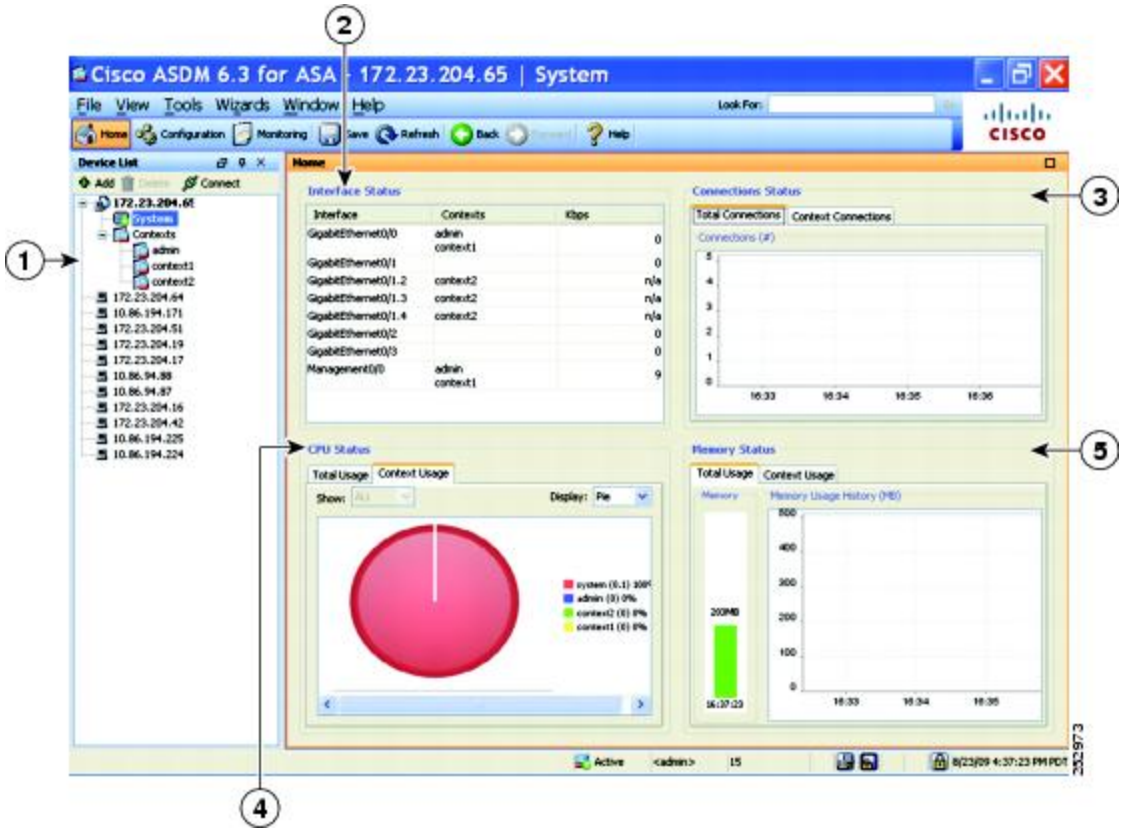
- **[ASA Firepower Dashboard]**：ダッシュボードには、モジュールで実行中のソフトウェア、製品のアップデート、ライセンシング、システムの負荷、ディスクの使用、システム時間、およびインターフェイスのステータスについての概要情報が提示されます。
- **[ASA FirepowerReporting]**：レポート作成のページには、Web カテゴリ、ユーザー、送信元、モジュールを通じてトラフィックが渡される宛先など、さまざまなモジュールの統計に対して上位 10 個のダッシュボードが提示されます。

[Home] ペイン（システム）

ASDM システムの [Home] ペインでは、ASA に関する重要なステータス情報を表示できます。ASDM システムの [Home] ペインに表示される詳細のほとんどは、ASDM の他の場所でも参照できますが、このペインでは ASA の動作状態を一目で確認できます。システムの [Home] ペインのステータス情報は 10 秒間隔で更新されます。

次の図に、システムの [Home] ペインの要素を示します。

図 *7*: システムの *[Home]* ペイン



凡例

GUI 要素	説明
1	システムとコンテキストの選択。
2	[Interface Status] ペイン。インターフェイスを通過するトラフィックの総数を表示するには、インターフェイスを選択します。
3	[Connection Status] ペイン。
4	[CPU Status] ペイン。
5	[Memory Status] ペイン。

ASDM 設定の定義

特定の ASDM 設定の動作を定義できます。

ASDM のさまざまな設定を変更するには、次の手順を実行します。

手順

ステップ 1 **[Tools]** > **[Preferences]** の順に選択します。

[General]、[Rules Table]、および [Syslog] の 3 つのタブのある [Preferences] ダイアログボックスが表示されます。

ステップ 2 設定を定義するには、これらのタブの 1 つをクリックします。[General] タブでは汎用プリファレンスを指定し、[Rules Table] タブでは [Rules] テーブルのプリファレンスを指定します。また、[Syslog] タブでは、[Home] ペインに表示される syslog メッセージの外観を指定したり、NetFlow 関連の syslog メッセージの警告メッセージの表示をイネーブルにしたりできます。

ステップ 3 [General] タブでは、次の項目を指定します。

- スタートアップ コンフィギュレーションと実行コンフィギュレーションが同期していないときに通知されるようにする場合は、[Warn that configuration in ASDM is out of sync with the configuration in ASA] チェックボックスをオンにします。
- 起動時に read-only ユーザーに対して次のメッセージを表示する場合は、[Show configuration restriction message to read-only user] チェックボックスをオンにします。このオプションは、デフォルトでオンです。

```
"You are not allowed to modify the ASA configuration,
because you do not have sufficient privileges."
```

- スレーブ ユニットに接続されたユーザーに設定制限メッセージを表示するには、[Show configuration restriction message on a slave unit in an ASA cluster] チェックボックスをオンにします。
- ASDM を閉じるときに終了を確認するプロンプトが表示されるようにするには、[Confirm before exiting from] チェックボックスをオンにします。このオプションは、デフォルトでオンです。
- スクリーン リーダーをイネーブルにするには、[Enable screen reader support (requires ASDM restart)] チェックボックスをオンにします。このオプションをイネーブルにするには、ASDM を再起動する必要があります。
- ASA メモリの最小空き容量が、ASDM アプリケーションの完全な機能を実行するには不十分である場合に通知を受信するには、[Warn of insufficient ASA memory when ASDM loads] チェックボックスをオンにします。ASDM は、起動時にテキスト バナー メッセージにメモリ警告を表示し、ASDM のタイトル バー テキストにメッセージを表示し、24 時間ごとに syslog アラートを送信します。

- [Communications] 領域で：
  - ASDM によって生成される CLI コマンドを表示するには、[Preview commands before sending them to the device] チェックボックスをオンにします。
  - ASA に複数のコマンドを 1 つのグループとして送信するには、[Enable cumulative (batch) CLI delivery] チェックボックスをオンにします。
  - [Minimum Configuration Sending Timeout] フィールドにタイムアウト メッセージの送信設定の最短時間を秒単位で入力します。デフォルトは 60 秒です。
  - マルチコンテキスト モードのシステムでは、[Graph User time interval in System Context] フィールドに、[Home] ペインのグラフの更新間隔の時間を 1 ~ 40 秒の範囲で入力します。デフォルトは 10 秒です。
- [Logging] 領域で：
  - Java ロギングを設定するには、[Enable logging to the ASDM Java console] チェックボックスをオンにします。
  - ドロップダウン リストから [Logging Level] を選択して、重大度を設定します。
- [Packet Capture Wizard] 領域で、キャプチャされたパケットを表示するには、[Network Sniffer Application] に名前を入力するか、[Browse] をクリックしてファイル システムで検索します。
- [SFR Location Wizard] 領域で、ASA FirePOWER モジュールのローカル管理ファイルをインストールする場所を指定します。設定された場所に対して読み取り/書き込み権限を持っている必要があります。

ステップ 4 [Rules Table] タブで、次の項目を指定します。

- [Display settings] では、[Rules] テーブルでのルールの表示方法を変更できます。
  - Auto-Expand Prefix 設定に基づいて自動展開されたネットワークおよびサービス オブジェクト グループを表示するには、[Auto-expand network and service object groups with specified prefix] チェックボックスをオンにします。
  - [Auto-Expand Prefix] フィールドに、表示するときに自動的に展開するネットワークおよびサービス オブジェクト グループのプレフィックスを入力します。
  - ネットワークおよびサービス オブジェクト グループのメンバーとそのグループ名を [Rules] テーブルに表示するには、[Show members of network and service object groups] チェックボックスをオンにします。チェックボックスがオフの場合は、グループ名だけが表示されます。
  - [Limit Members To] フィールドに、表示するネットワークおよびサービス オブジェクト グループの数を入力します。オブジェクト グループ メンバーが表示されるときには、最初の *n* 個のメンバーだけが表示されます。

- [Rules] テーブルにすべてのアクションを表示するには、[Show all actions for service policy rules] チェックボックスをオンにします。オフの場合は、サマリーが表示されます。

- [Deployment Settings] では、[Rules] テーブルに変更内容を適用するときの ASA の動作を設定できます。
  - 新しいアクセス リストを適用するときに NAT テーブルをクリアするには、[Issue "clear xlate" command when deploying access lists] チェックボックスをオンにします。この設定により、ASA で設定されるアクセス リストが、すべての変換アドレスに対して確実に適用されるようにします。

- [Access Rule Hit Count Settings] では、[Access Rules] テーブルのヒット数をアップデートする頻度を設定できます。ヒット数は、明示的なルールにだけ適用されます。暗黙的なルールのヒット数は、[Access Rules] テーブルには表示されません。
  - [Access Rules] テーブルでヒット数が自動的にアップデートされるようにするには、[Update access rule hit counts automatically] チェックボックスをオンにします。
  - [Access Rules] テーブルに、ヒット数カラムを更新する頻度を秒単位で指定します。有効値の範囲は 10 ～ 86400 秒です。

ステップ 5 [Syslogl] タブでは、次の項目を指定します。

- [Syslog Colors] 領域では、重大度レベルごとに背景色と前景色を設定し、メッセージ表示をカスタマイズできます。[Severity] カラムには、各重大度レベルが名前および番号ごとに表示されます。各重大度レベルでメッセージの背景色または前景色を変更するには、対応するカラムをクリックします。[Pick a Color] ダイアログボックスが表示されます。次のいずれかのタブをクリックします。
  - [Swatches] タブでパレットから色を選択し、[OK] をクリックします。
  - [HSB] タブで H、S、B の設定を指定し、[OK] をクリックします。
  - [RGB] タブで赤、緑、青の設定を指定し、[OK] をクリックします。

- 冗長な syslog メッセージをディセーブルにするよう警告するメッセージの表示をイネーブルにするには、[NetFlow] 領域で [Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule] チェックボックスをオンにします。

ステップ 6 これら 3 つのタブの設定を指定した後で、[OK] をクリックして設定を保存し、[Preferences] ダイアログボックスを閉じます。

（注） プリファレンス設定をオンまたはオフにするたびに、変更内容は .conf ファイルに保存され、その時点でワークステーション上で実行中のその他の ASDM セッションから利用できるようになります。すべての変更を有効にするには、ASDM を再起動する必要があります。

ASDM Assistant での検索

ASDM Assistant ツールでは、タスクに応じた ASDM の使用方法のヘルプを検索し、表示できます。

情報にアクセスするには **[View]** > **[ASDM Assistant]** > **[How Do I?]** の順に選択するか、メニューバーの [Look For] フィールドから検索要求を入力します。[Find] ドロップダウン リストから [How Do I?] を選択して検索を開始します。

ASDM Assistant を表示するには、次の手順を実行します。

手順

ステップ 1 **[View]** > **[ASDM Assistant]** を選択します。

[ASDM Assistant] ペインが表示されます。

ステップ 2 [Search] フィールドに検索する情報を入力して [Go] をクリックします。

要求された情報が [Search Results] ペインに表示されます。

ステップ 3 [Search Results] セクションおよび [Features] セクションに表示される任意のリンクをクリックし、詳細情報を入手します。

履歴メトリックの有効化

[History Metrics] ペインでは、さまざまな統計情報の履歴を保存するように ASA を設定でき、ASDM を使用してそれをグラフやテーブルに表示できます。履歴メトリックをイネーブルにしない場合、監視できるのはリアルタイムの統計情報だけです。履歴メトリックをイネーブルにすると、直前の 10 分間、60 分間、12 時間、5 日間の統計グラフを表示できます。

履歴メトリックを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Advanced]** > **[History Metrics]** を選択します。

[History Metrics] ペインが表示されます。

ステップ 2 [ASDM History Metrics] チェックボックスをオンにして履歴メトリックをイネーブルにし、[Apply] をクリックします。

サポートされていないコマンド

ASA で使用可能なコマンドはほとんどすべて ASDM でサポートされますが、既存のコンフィギュレーションのコマンドの一部はで無視される場合があります。これらのコマンドのほとんどはコンフィギュレーションに残すことができます。詳細については、[Tools]>[Show Commands Ignored by ASDM on Device] を参照してください。

無視される表示専用コマンド

次の表に、CLI 経由で追加された場合に ASDM のコンフィギュレーションでサポートされるが、ASDM で追加または編集できないコマンドの一覧を示します。ASDM で無視されるコマンドは ASDM の GUI に一切表示されません。表示専用コマンドは GUI に表示されますが、編集はできません。

表 *6:* サポートされていないコマンドの一覧

サポートされていないコマンド	ASDM の動作
capture	無視されます。
coredump	無視されます。これは、CLI を使用してのみ設定できます。
crypto engine large-mod-accel	無視されます。
dhcp-server（トンネル グループ名一般属性）	ASDM では、すべての DHCP サーバーに対して 1 つの設定のみが許可されます。
eject	サポート対象外
established	無視されます。
failover timeout	無視されます。
fips	無視されます。
nat-assigned-to-public-ip	無視されます。
pager	無視されます。

サポートされていないコマンド	ASDM の動作
pim accept-register route-map	無視されます。ASDM では [List] オプションだけ設定可。

service-policy global	**match access-list** クラスで使用されている場合は無視。次に例を示します。
	
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`  inspect ftp`
	`service-policy mypm global`

set metric	無視されます。
sysopt nodnsalias	無視されます。
sysopt uauth allow-http-cache	無視されます。
terminal	無視されます。
threat-detection rate	無視されます。

サポートされていないコマンドの影響

既存の実行コンフィギュレーションを ASDM にロードした場合、そこにサポート対象外のコマンドがあっても、ASDM の操作には影響しません。サポート対象外のコマンドを表示するには、[Tools] > [Show Commands Ignored by ASDM on Device] を選択します。

サポート対象外の連続していないサブネット マスク

ASDM では、255.255.0.255 のように連続していないサブネット マスクはサポートされていません。たとえば、次は使用できません。

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM CLI ツールでサポートされていないインタラクティブ ユーザー コマンド

ASDM CLI ツールは、インタラクティブ ユーザー コマンドをサポートしていません。インタラクティブな確認を必要とする CLI コマンドを入力すると、「[yes/no]」の入力を要求するプロンプトが表示されますが、入力内容は認識されません。続いて ASDM は、応答の待機をタイムアウトします。

次に例を示します。

1. **[Tools]** > **[Command Line Interface]** を選択します。
2. **crypto key generate rsa** コマンドを入力します。

   デフォルトの 1024 ビット RSA キーが生成されます。
3. **crypto key generate rsa** コマンドを再度入力します。

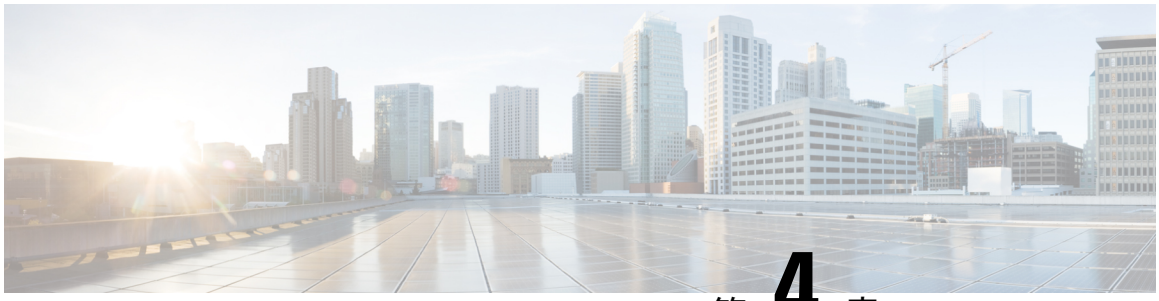
   以前の RSA キーを上書きして再生成するのではなく、次のエラーが表示されます。

```
Do you really want to replace them? [yes/no]:WARNING: You already have
RSA ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

回避策：

- [ASDM] ペインから、ユーザー介入が必要なほとんどのコマンドを設定できます。
- **noconfirm** オプションがある CLI コマンドについては、CLI コマンド入力時にこのオプションを使用します。次に例を示します。

```
crypto key generate rsa noconfirm
```



第 4 章

ライセンス：製品認証キーライセンス

ライセンスでは、特定の Cisco ASA 上でイネーブルにするオプションを指定します。このマニュアルでは、ASA ハードウェアモデルと ISA 3000 の製品認証キー（PAK）のライセンスについて説明します。その他のモデルについては、ライセンス：スマート ソフトウェア ライセンシング （155 ページ）を参照してください。

PAK ライセンスについて

ライセンスでは、特定の ASA 上でイネーブルにするオプションを指定します。ライセンスは、160 ビット（32 ビットのワードが 5 個、または 20 バイト）値であるアクティベーション キーで表されます。この値は、シリアル番号（11 文字の文字列）とイネーブルになる機能とを符号化します。

事前インストール済みライセンス

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。

関連トピック

PAK ライセンスのモニターリング （142 ページ）

永続ライセンス

永続アクティベーション キーを 1 つインストールできます。永続アクティベーション キーは、1 つのキーにすべてのライセンス機能を格納しています。時間ベース ライセンスもインストールすると、ASA は永続ライセンスと時間ベース ライセンスを 1 つの実行ライセンスに結合します。

関連トピック

永続ライセンスと時間ベース ライセンスの結合 （105 ページ）

時間ベース ライセンス

永続ライセンスに加えて、時間ライセンスを購入したり、時間制限のある評価ライセンスを入手したりできます。たとえば、SSL VPN の同時ユーザの短期増加に対処するために時間ベースの AnyConnect Premium ライセンスを購入したり、1 年間有効なボットネット トラフィック フィルタ時間ベースライセンスを注文したりできます。

（注） ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

時間ベース ライセンス有効化ガイドライン

- 複数の時間ベース ライセンスをインストールし、同じ機能に複数のライセンスを組み込むことができます。ただし、一度にアクティブ化できる時間ベース ライセンスは、1 機能につき 1 つだけです。非アクティブのライセンスはインストールされたままで、使用可能な状態です。たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション AnyConnect Premium ライセンスをインストールした場合、これらのライセンスのうちいずれか 1 つだけをアクティブにできます。
- キーの中に複数の機能を持つ評価ライセンスをアクティブにした場合、そこに含まれている機能のいずれかに対応する時間ベース ライセンスを同時にアクティブ化することはできません。 たとえば、評価ライセンスにボットネット トラフィック フィルタと 1000 セッション AnyConnect Premium ライセンスが含まれる場合、スタンドアロンの時間ベース 2500 セッション AnyConnect Premium ライセンスをこの評価ライセンスと同時にアクティブ化することはできません。

時間ベース ライセンス タイマーの動作

- 時間ベース ライセンスのタイマーは、ASA 上でライセンスをアクティブにした時点でカウント ダウンを開始します。
- タイムアウト前に時間ベース ライセンスの使用を中止すると、タイマーが停止します。時間ベース ライセンスを再度アクティブ化すると、タイマーが再開します。
- 時間ベース ライセンスがアクティブになっているときに ASA をシャットダウンすると、タイマーはカウント ダウンを停止します。時間ベース ライセンスでは、ASA が動作して

いる場合にのみカウント ダウンします。システム クロック設定はライセンスに影響しません。つまり、ASA 稼働時間ではライセンス継続期間に対してのみカウントします。

永続ライセンスと時間ベース ライセンスの結合

時間ベース ライセンスをアクティブにすると、永続ライセンスと時間ベース ライセンスに含まれる機能を組み合わせた実行ライセンスが作成されます。永続ライセンスと時間ベース ライセンスの組み合わせ方は、ライセンスのタイプに依存します。次の表に、各機能ライセンスの組み合わせルールを示します。

（注） 永続ライセンスが使用されていても、時間ベース ライセンスがアクティブな場合はカウントダウンが続行されます。

表 7: 時間ベース ライセンスの組み合わせルール

時間ベース機能	結合されたライセンスのルール
AnyConnect Premium セッション	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。たとえば、永続ライセンスが 1000 セッション、時間ベース ライセンスが 2500 セッションの場合、2500 セッションがイネーブルになります。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。
Unified Communications Proxy セッション	時間ベースライセンスのセッションは、プラットフォームの制限数まで永続セッションに追加されます。たとえば、永続ライセンスが 2500 セッション、時間ベース ライセンスが 1000 セッションの場合、時間ベース ライセンスがアクティブである限り、3500 セッションがイネーブルになります。
セキュリティ コンテキスト	時間ベース ライセンスのコンテキストは、プラットフォームの制限数まで永続コンテキストに追加されます。たとえば、永続ライセンスが 10 コンテキスト、時間ベース ライセンスが 20 コンテキストの場合、時間ベース ライセンスがアクティブである限り、30 コンテキストがイネーブルになります。

時間ベース機能	結合されたライセンスのルール
Botnet Traffic Filter	使用可能な永続ボットネット トラフィック フィルタ ライセンスはありません。時間ベース ライセンスが使用されます。
その他	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。数値ティアを持つライセンスの場合、高い方の値が使用されます。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。

関連トピック

PAK ライセンスのモニターリング （142 ページ）

時間ベース ライセンスのスタッキング

多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。

すでにインストールされているのと同じ時間ベース ライセンスをインストールすると、それらのライセンスは結合され、有効期間は両者を合わせた期間になります。

次に例を示します。

1. 52 週のボットネット トラフィック フィルタ ライセンスをインストールし、このライセンスを 25 週間使用します（残り 27 週）。
2. 次に、別の 52 週ボットネット トラフィック フィルタ ライセンスを購入します。2 つめのライセンスをインストールすると、ライセンスが結合され、有効期間は 79 週（52＋27 週）になります。

同様の例を示します。

1. 8 週 1000 セッションの AnyConnect Premium ライセンスをインストールし、これを 2 週間使用します（残り 6 週）。

2. 次に、別の 8 週 1000 セッションのライセンスをインストールすると、これらのライセンスは結合され、14 週（8 + 6 週）1000 セッションのライセンスになります。

これらのライセンスが同一でない場合（たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンス）、これらのライセンスは結合されません。1 つの機能につき時間ベース ライセンスを 1 つだけアクティブにできるので、ライセンスのうちいずれか 1 つだけをアクティブにすることができます。

同一でないライセンスは結合されませんが、現在のライセンスの有効期限が切れた場合、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。

関連トピック

キーのアクティブ化または非アクティブ化 （123 ページ）
時間ベース ライセンスの有効期限 （107 ページ）

時間ベース ライセンスの有効期限

機能に対応する現在のライセンスが期限切れになると、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。その機能に使用できる時間ベース ライセンスが他にない場合は、永続ライセンスが使用されます。

その機能に対して複数の時間ベース ライセンスを追加でインストールした場合、ASA は最初に検出されたライセンスを使用します。どのライセンスを使用するかは、ユーザーが設定することはできず、内部動作に依存します。ASA がアクティブ化したライセンスとは別の時間ベース ライセンスを使用するには、目的のライセンスを手動でアクティブにする必要があります。

たとえば、2500 セッションの時間ベース AnyConnect Premium ライセンス（アクティブ）、1000 セッションの時間ベース AnyConnect Premium ライセンス（非アクティブ）、500 セッションの永続 AnyConnect Premium ライセンスを所有しているとします。2500 セッション ライセンスの有効期限が切れた場合、ASA は 1000 セッション ライセンスを有効化します。1000 セッション ライセンスの有効期限が切れた後、ASA は 500 セッション永久ライセンスを使用します。

関連トピック

キーのアクティブ化または非アクティブ化 （123 ページ）

ライセンスに関する注意事項

次の項で、ライセンスに関する追加情報について説明します。

AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザー プールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。https://www.cisco.com/go/license を参照し、各 ASA に個別に PAK を割り当てます。ASA に取得したアクティベーション キーを適用すると、VPN 機能が最大許容数に切り替わりますが、ライセンスを共有するすべての

ASA 上の実際の一意のユーザー数はライセンス限度を超えることはできません。詳細については、以下を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

（注） マルチ コンテキスト モードには AnyConnect Apex ライセンスが必要です。さらに、マルチ コンテキスト モードでは、フェールオーバー ペアの各ユニットにこのライセンスを適用する必要があります。ライセンスは集約されません。

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。
- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

VPN ロード バランシング

VPN ロード バランシングには、強力な暗号化（3DES/AES）ライセンスが必要です。

レガシー VPN ライセンス

ライセンスに関するすべての関連情報については、「Supplemental end User License Agreement for AnyConnect」を参照してください。

（注） マルチ コンテキスト モードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

暗号化ライセンス

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

キャリア ライセンス

キャリア ライセンスでは、以下のインスペクション機能が有効になります。

- Diameter
- GTP/GPRS
- SCTP

合計 TLS プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザー数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザー数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

AnyConnect Premium 共有ライセンス（AnyConnect 3 以前）

（注） ASAの共有ライセンス機能は、AnyConnect 4 以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバーまたは参加ライセンスは不要になりました。

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバーとして、残りを共有ライセンス参加システムとして設定します。

フェールオーバーまたは ASA クラスタライセンス

いくつかの例外を除き、フェールオーバーおよびクラスタユニットは、各ユニット上で同一のライセンスを必要としません。以前のバージョンについては、お使いのバージョンに該当するライセンシング マニュアルを参照してください。

フェールオーバー ライセンスの要件および例外

ほとんどのモデルでは、フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	• アクティブ/スタンバイ：両方のユニットの Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
Asa 5525- x ～ asa 5555-X	• 基本ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	ASAv のフェールオーバー ライセンス （165 ページ）を参照してください。

モデル	ライセンス要件
Firepower 1010	両方のユニットの Security Plus ライセンス。Firepower 1010 のフェールオーバー ライセンス （166 ページ）を参照してください。
Firepower 1100	Firepower 1100 のフェールオーバー ライセンス （166 ページ）を参照してください。
Firepower 2100	Firepower 2100 のフェールオーバー ライセンス （168 ページ）を参照してください。
Firepower 4100/9300	Firepower 4100/9300のフェールオーバーライセンス （170 ページ）を参照してください。
ISA 3000	両方のユニットの Security Plus ライセンス。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

ASA クラスタ ライセンスの要件および例外

クラスタ ユニットは、各ユニット上で同じライセンスを必要としません。一般的には、制御ユニット用のライセンスのみを購入します。データユニットは制御ユニットのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5516-X	基本ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
Firepower 4100/9300 シャーシ	Firepower 4100/9300 の ASA クラスタライセンス （172 ページ）を参照してください。

モデル	ライセンス要件
他のすべてのモデル	サポートしない

フェールオーバーまたは ASA クラスタライセンスの結合方法

フェールオーバーペアまたは ASA クラスタでは、各ユニットのライセンスが結合されて 1 つの実行クラスタライセンスとなります。ユニットごとに別のライセンスを購入した場合は、結合されたライセンスには次のルールが使用されます。

- 数値ティアを持つライセンスの場合は（セッション数など）、各ユニットのライセンスの値が合計されます。ただし、プラットフォームの制限を上限とします。使用されているライセンスがすべて時間ベースの場合は、ライセンスのカウント ダウンは同時に行われます。

  たとえば、フェールオーバーの場合は次のようになります。

  - 2 つの ASA があり、それぞれに 10 個の TLS プロキシ セッションが設定されている場合、ライセンスは結合され、合計で 20 個の TLS プロキシ セッションになります。
  - 1 つの ASA 5545-X には 1000 の TLS プロキシセッションがあり、もう 1 つには 2000 のセッションがあるとします。プラットフォームの限度は 2000 であるため、結合されたライセンスは 2000 の TLS プロキシセッションに対応できます。
  - 2 つの ASA 5545-X ASA があり、一方は 20 コンテキスト、もう一方は 10 コンテキストである場合、結合されたライセンスでは 30 コンテキストを使用できます。アクティブ/アクティブ フェールオーバーの場合は、コンテキストが 2 つのユニットに分配されます。たとえば、一方のユニットが 18 コンテキストを使用し、他方が 12 コンテキストを使用します（合計 30 の場合）。

  たとえば、ASA クラスタリングの場合は次のようになります。

  - デフォルトの 2 コンテキストの 2 つの ASA 5516-X ASA があります。プラットフォームの制限が 5 であるため、結合されたライセンスでは最大 4 のコンテキストが許容されます。したがって、プライマリ ユニット上で最大 4 のコンテキストを設定できます。各セカンデリ ユニットも、コンフィギュレーションの複製経由で 4 のコンテキストを持つことになります。
  - 4 つの ASA 5516-X ASA があります。これは、それぞれが 5 コンテキストの 3 つのユニットと、デフォルトの 2 コンテキストの 1 つのユニットです。プラットフォームの制限が 5 であるため、ライセンスは合計で 5 コンテキストに結合されます。したがって、プライマリ ユニット上で最大 5 のコンテキストを設定できます。各セカンデリ ユニットも、コンフィギュレーションの複製経由で 5 のコンテキストを持つことになります。

- ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。

- イネーブルまたはディセーブル状態（かつ数値ティアを持たない）の時間ベースライセンスの場合、有効期間はすべてのライセンスの期間の合計となります。最初にプライマリ/制御ユニットのライセンスがカウントダウンされ、期限切れになると、セカンダリ/データユニットのライセンスのカウントダウンが開始し、以下も同様です。このルールは、アクティブ/アクティブ フェールオーバーと ASA クラスタリングにも適用されます（すべてのユニットがアクティブに動作していても適用されます）。

  たとえば、2 つのユニットのボットネット トラフィック フィルタ ライセンスの有効期間が 48 週残っている場合は、結合された有効期間は 96 週です。

関連トピック

PAK ライセンスのモニターリング （142 ページ）

フェールオーバーまたは ASA クラスタユニット間の通信の途絶

ユニットの通信が途絶えてからの期間が 30 日を超えた場合は、各ユニットにはローカルにインストールされたライセンスが適用されます。30 日の猶予期間中は、結合された実行ライセンスが引き続きすべてのユニットで使用されます。

30 日間の猶予期間中に通信が復旧した場合は、時間ベースライセンスについては、経過した時間がプライマリ/制御ライセンスから差し引かれます。プライマリ/制御ライセンスが期限切れになるまでは、セカンダリ/データライセンスのカウントダウンが開始することはありません。

30 日間の期間が終了しても通信が復旧しなかった場合は、時間ベース ライセンスについては、その時間がすべてのユニットのライセンスから差し引かれます（インストールされている場合）。これらはそれぞれ別のライセンスとして扱われ、ライセンスの結合によるメリットはありません。経過時間には 30 日の猶予期間も含まれます。

次に例を示します。

1. 52 週のボットネット トラフィック フィルタ ライセンスが 2 つのユニットにインストールされています。結合された実行ライセンスでは、合計期間は 104 週になります。
2. これらのユニットが、1 つのフェールオーバーユニット/ASA クラスタとして 10 週間動作すると、結合ライセンスの期間の残りは 94 週となります（プライマリ/制御に 42 週、セカンダリ/データに 52 週）。
3. ユニットの通信が途絶えた場合（たとえば、プライマリ/制御ユニットが停止した場合）は、セカンダリ/データユニットは結合されたライセンスを引き続き使用し、94 週からカウントダウンを続行します。
4. 時間ベース ライセンスの動作は、通信がいつ復元されるかによって次のように異なります。
   - 30 日以内：経過した時間がプライマリ/制御ユニットのライセンスから差し引かれます。この場合、通信は 4 週間後に復元されます。したがって、4 週がプライマリ/制御ライセンスから差し引かれて、残りは合計 90 週となります（プライマリに 38 週、セカンダリに 52 週）。
   - 30 日経過以降：経過時間が両方の装置から差し引かれます。この場合、通信は 6 週間後に復元されます。したがって、6 週がプライマリ/制御とセカンダリ/データの両方の

ライセンスから差し引かれて、残りは合計 84 週となります（プライマリ/制御に 36 週、セカンダリ/データに 46 週）。

フェールオーバー ペアのアップグレード

フェールオーバーペアでは、両方の装置に同一のライセンスがインストールされている必要はないので、ダウンタイムなしに各装置に新しいライセンスを適用できます。リロードが必要な永続ライセンスを適用する場合、リロード中に他の装置へのフェールオーバーを実行できます。両方の装置でリロードが必要な場合は、各装置を個別にリロードするとダウンタイムは発生しません。

関連トピック

キーのアクティブ化または非アクティブ化 （123 ページ）

ペイロード暗号化機能のないモデル

ペイロード暗号化機能のないモデルを購入することができます。輸出先の国によっては、Cisco ASA シリーズでペイロード暗号化をイネーブルにできません。ASA ソフトウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセーブルにします。

- ユニファイド コミュニケーション
- VPN

このモデルでも管理接続用に高度暗号化（3DES/AES）ライセンスをインストールできます。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使用できます。ボットネット トラフィック フィルタ（SSL を使用）用のダイナミック データベースをダウンロードすることもできます。

ライセンスを表示すると、VPN およびユニファイド コミュニケーションのライセンスはリストに示されません。

関連トピック

PAK ライセンスのモニターリング （142 ページ）

ライセンスの FAQ

AnyConnect Premium とボットネット トラフィック フィルタなど、複数の時間ベースライセンスをアクティブにできますか。

はい。一度に使用できる時間ベースライセンスは、1 機能につき 1 つです。

複数の時間ベースライセンスを「スタック」し、時間制限が切れると自動的に次のライセンスが使用されるようにできますか。

はい。ライセンスが同一の場合は、複数の時間ベースライセンスをインストールすると、時間制限が結合されます。ライセンスが同一でない場合（1000 セッション AnyConnect

Premium ライセンスと 2500 セッションライセンスなど）、ASA はその機能に対して検出された次の時間ベースライセンスを自動的にアクティブにします。

アクティブな時間ベースライセンスを維持しながら、新しい永続ライセンスをインストールできますか。

はい。永続ライセンスをアクティブ化しても、時間ベースライセンスには影響しません。

フェールオーバーのプライマリ装置として共有ライセンスサーバを、セカンダリ装置として共有ライセンス バックアップ サーバを使用できますか。

いいえ。セカンダリ装置は、プライマリ装置と同じ実行ライセンスを使用します。共有ライセンスサーバには、サーバライセンスが必要です。バックアップサーバには、参加ライセンスが必要です。バックアップサーバは、2 つのバックアップサーバの別々のフェールオーバーペアに配置できます。

フェールオーバーペアのセカンダリ装置用に、同じライセンスを購入する必要がありますか。

いいえ。バージョン 8.3(1) から、両方の装置に同一のライセンスをインストールする必要はなくなりました。一般的に、ライセンスはプライマリ装置で使用するために購入されます。セカンダリ装置は、アクティブになるとプライマリライセンスを継承します。セカンダリ装置に別のライセンスを持っている場合は（たとえば、8.3 よりも前のソフトウェアに一致するライセンスを購入した場合）、ライセンスは実行フェールオーバー クラスタ ライセンスに結合されます。ただし、モデルの制限が最大数になります。

AnyConnect Premium（共有）ライセンスに加えて、時間ベースまたは永続の AnyConnect Premium ライセンスを使用できますか。

はい。ローカルにインストールされたライセンス（時間ベースライセンスまたは永続ライセンス）のセッション数を使い果たした後、共有ライセンスが使用されます。

（注） 共有ライセンスサーバでは、永続 AnyConnect Premium ライセンスは使用されません。ただし、共有ライセンスサーバライセンスと同時に時間ベースライセンスを使用することはできます。この場合、時間ベースライセンスのセッションは、ローカルの AnyConnect Premium セッションにだけ使用できます。共有ライセンスプールに追加して参加システムで使用することはできません。

PAK ライセンスのガイドライン

コンテキスト モードのガイドライン

マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。

フェールオーバーのガイドライン

フェールオーバーまたは ASA クラスタライセンス （111 ページ）を参照してください。

モデルのガイドライン

- スマート ライセンスは、ASAv でのみサポートされます。
- 共有ライセンスは、ASAv、ASA 5506-X、ASA 5508-X および ASA 5516-X ではサポートされません。
- ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2* よりも前に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2* 以降で導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 以前のバージョンでアクティベーション キーを入力した場合は、ASA はそのキーを使用します（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくても、アクティブ ライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。
  - フェールオーバーペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
  - 1 つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブなままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

その他のガイドライン

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーションキーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要があり、このことが Cisco TAC によってカバーされている場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- ライセンシングで使うシリアル番号は、（[Activation Key] ページ内）で表示されるものです。このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- 1 つのユニット上で、同じ機能の 2 つの別個のライセンスを加算することはできません。たとえば、25 セッション SSL VPN ライセンスを購入した後で 50 セッション ライセンスを購入しても、75 個のセッションを使用できるわけではなく、使用できるのは最大 50 個のセッションです。（アップグレード時に、数を増やしたライセンスを購入できることがあります。たとえば 25 セッションから 75 セッションへの増加です。このタイプのアップグレードは、2 つのライセンスの加算とは別のものです）。
- すべてのライセンス タイプをアクティブ化できますが、機能によっては、機能どうしの組み合わせができないものがあります。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。AnyConnect Premium ライセンス、AnyConnect Premium（共有）ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスをインストールした場合（使用中のモデルで利用できる場合）、このライセンスが前述のライセンスの代わりに使用されます。 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用して、設定で AnyConnect Essentials ライセンスを無効にし、他のライセンスを使用できます。

PAK ライセンスの設定

この項では、アクティベーション キーを取得する方法とそれをアクティブ化する方法について説明します。また、キーを非アクティブ化することもできます。

ライセンスの PAK の注文とアクティベーション キーの取得

ASA にライセンスをインストールするには製品認証キーが必要です。その後、それを Cisco.com に登録してアクティベーション キーを取得することができます。次に、ASA のアクティベー

ション キーを入力できます。機能ライセンスごとに個別の製品認証キーが必要になります。PAK が組み合わせられて、1 つのアクティベーション キーになります。デバイス発送時に、すべてのライセンス PAK が提供されている場合もあります。ASA には基本ライセンスまたは Security Plus ライセンスがプリインストールされ、ご使用資格を満たしている場合には Strong Encryption（3DES/AES）ライセンスも提供されます。無料の Strong Encryption ライセンスを手動でリクエストする必要がある場合は、http://www.cisco.com/go/license を参照してください。

始める前に

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

手順

ステップ 1 追加ライセンスを購入するには、http://www.cisco.com/go/ccw を参照してください。次の AnyConnect 発注ガイドおよび FAQ を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

ライセンスを購入した後、製品認証キー（PAK）が記載された電子メールを受け取ります。AnyConnect ライセンスの場合、ユーザー セッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。場合によっては、PAK が記載された電子メールを受け取るまで数日かかることがあります。

ASA FirePOWER モジュールは、ASA とは別のライセンス メカニズムを使用します。詳しくは、ご使用のモデルのクイック スタート ガイドを参照してください。

ステップ 2 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Activation Key]** を選択して、ご使用の ASA のシリアル番号を取得します（マルチ コンテキスト モードでは、システム実行スペースにシリアル番号を表示します）。

ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。

ステップ 3 アクティベーション キーを取得するには、以下のライセンス Web サイトに移動します。

http://www.cisco.com/go/license

ステップ 4 プロンプトが表示されたら、次の情報を入力します。

- 製品認証キー（キーが複数ある場合は、まず 1 つを入力します。キーごとに個別のプロセスとして入力する必要があります）

- ASA のシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。時間ベース ライセンスの場合は、ライセンスごとに個別のアクティベーション キーがあります。

ステップ 5 さらに追加の製品認証キーがある場合は、製品認証キーごとにこの手順を繰り返します。すべての製品認証キーを入力した後、最後に送信されるアクティベーションキーには、登録した永続機能がすべて含まれています。

ステップ 6 キーのアクティブ化または非アクティブ化 （123 ページ）に基づいて、アクティベーション キーをインストールします。

高度暗号化ライセンスの取得

ASDM（および他の多数の機能）を使用するには、高度暗号化（3DES/AES）ライセンスをインストールする必要があります。ASA に高度暗号化ライセンスがプリインストールされていない場合は、ライセンスを無料で入手できます。高度暗号化ライセンスに関するそれぞれ国の資格を満たす必要があります。

手順

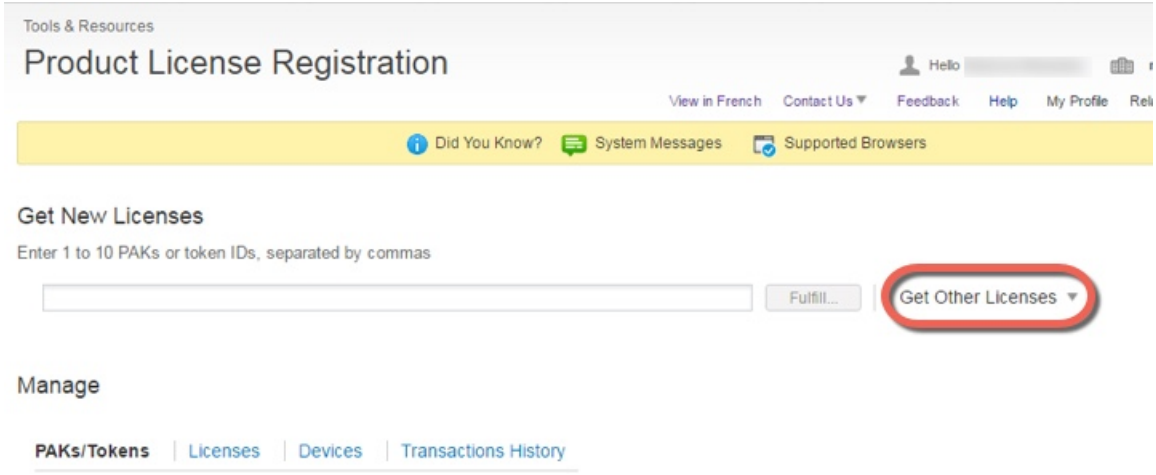
ステップ 1 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。

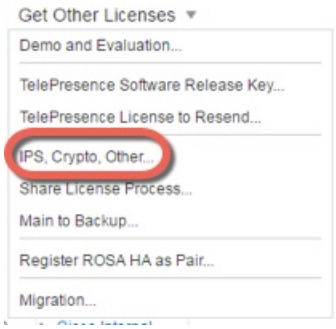
ステップ 2 Https://www.cisco.com/go/license を参照し、[Get Other Licenses] をクリックしてください。

図 *8 :* 他のライセンスの取得



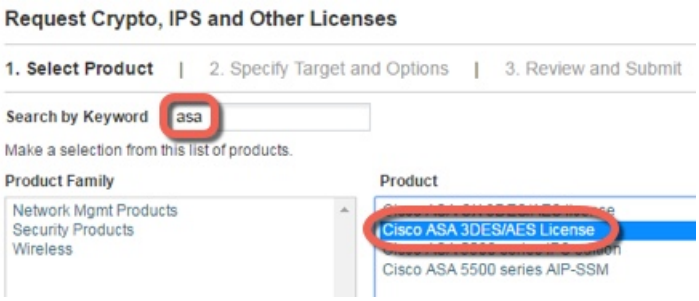
ステップ 3 [IPS, Crypto, Other] を選択します。

図 *9 : IPS*、*Crypto*、その他



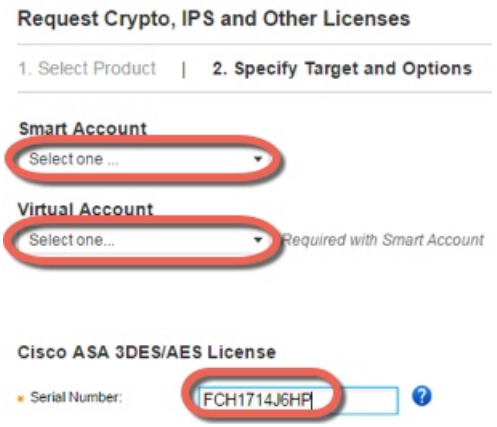
ステップ 4 [Search by Keyword] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 *10 : Cisco ASA 3DES/AES* ライセンス



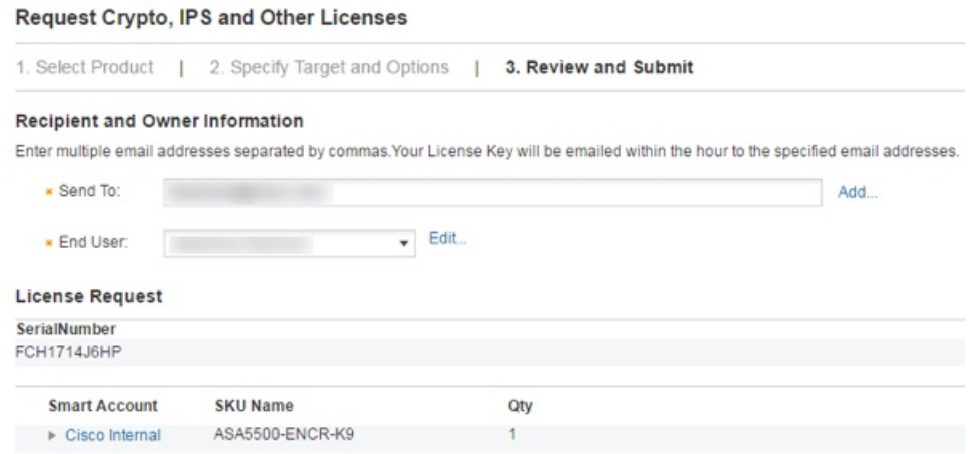
ステップ 5 [Smart Acfcount] 、[Virtual Account] を選択し、ASA の [Serial Number] を入力して、[Next] をクリックします。

図 *11* : スマート アカウント、バーチャル アカウント、シリアル番号



ステップ 6 送信先の電子メールアドレスとエンドユーザー名は自動的に入力されます。必要に応じて追加の電子メール アドレスを入力します。[I Agree] チェックボックスをオンにして、[Submit] をクリックします。

図 *12* : 送信



ステップ 7 その後、アクティベーション キーの記載された電子メールが届きますが、**[Manage]** > **[Licenses]** エリアからキーをすぐにダウンロードすることもできます。

ステップ 8 キーのアクティブ化または非アクティブ化（123 ページ）に基づいて、アクティベーションキーを適用します。

キーのアクティブ化または非アクティブ化

この項では、新しいアクティベーション キーの入力と、時間ベース キーのアクティブ化および非アクティブ化の方法について説明します。

始める前に

- すでにマルチ コンテキスト モードに入っている場合は、システム実行スペースにこのアクティベーション キーを入力します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。次の表に、リロードが必要なライセンスを示します。

表 *8*：永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード

手順

ステップ 1 **[Configuration]** > **[Device Management]** の順に選択し、モデルに応じて、**[Licensing]** > **[Activation Key]** または [Licensing Activation Key] ペインを選択します。

ステップ 2 永続または時間ベースの新しいアクティベーション キーを入力するには、[New Activation Key] フィールドで新しいアクティベーション キーを入力します。

キーは、5 つの要素で構成される 16 進ストリングで、各要素は 1 つのスペースで区切られています。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。次に例を示します。

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。新しい時間ベース キーを入力した場合、デフォルトでアクティブになり、[Time-based License Keys Installed] テーブルに表示されます。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。

ステップ 3 インストール済みの時間ベース キーをアクティブ化または非アクティブ化するには、そのキーを [Time-based License Keys Installed] テーブルで選択し、[Activate] または [Deactivate] をクリックします。

各機能でアクティブにできる時間ベース キーは 1 つのみです。

ステップ 4 [Update Activation Key] をクリックします。

永続ライセンスによっては、新しいアクティベーション キーの入力後に ASA をリロードする必要があります。必要な場合は、リロードするよう求められます。

関連トピック

時間ベース ライセンス （104 ページ）

共有ライセンスの設定（AnyConnect 3 以前）

（注） ASAの共有ライセンス機能は、AnyConnect 4 以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバーまたは参加ライセンスは不要になりました。

この項では、共有ライセンス サーバーと参加システムを設定する方法について説明します。

共有ライセンスについて

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバーとして、残りを共有ライセンス参加システムとして設定します。

共有ライセンスのサーバーと参加システムについて

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバーのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバーを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバーとして指定します。バックアップ サーバーには 1 台のみ指定できます。

   （注） 共有ライセンス バックアップ サーバーに必要なのは参加ライセンスのみです。
4. 共有ライセンス サーバー上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバーに登録します。

   （注） 参加者は IP ネットワークを経由してサーバーと通信できる必要がありますが、同じサブネット上にある必要はありません。
6. 共有ライセンス サーバーは、参加者がサーバーにポーリングするべき頻度の情報で応答します。

7. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバーに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンス サーバーは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンス サーバーは、共有ライセンス プールに参加することもできます。参加には参加ライセンスもサーバー ライセンスも必要ありません。

1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバーは使用可能な限りのセッション数で応答します。
2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバーが要求に適切に対応できるまで続けます。

9. 参加者の負荷が減少した場合、参加者はサーバーに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバーと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバーの間の通信問題

参加者とサーバー間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔 3 倍の時間が経過した後で、サーバーはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバーに到達できない場合、参加者はサーバーから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンス サーバーと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバーに再接続したが、サーバーが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバーは、参加者に再割り当てできる限りのセッション数で応答します。

共有ライセンス バックアップ サーバーについて

共有ライセンス バックアップ サーバーは、バックアップの役割を実行する前にメインの共有ライセンス サーバーへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバーは共有ライセンス情報に加えてサーバー設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サー

バーとバックアップ サーバーは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバーはリロード後でもバックアップの役割を実行できます。

メイン サーバーがダウンすると、バックアップ サーバーがサーバー動作を引き継ぎます。バックアップ サーバーは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバーは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバーをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバーが復旧した場合、メイン サーバーはバックアップ サーバーと同期してから、サーバー動作を引き継ぎます。

バックアップ サーバーがアクティブでないときは、メインの共有ライセンス サーバーの通常の参加者として動作します。

（注） メインの共有ライセンス サーバーの初回起動時には、バックアップ サーバーは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバーがその後短時間でもダウンした場合、バックアップ サーバーの動作制限は日ごとに減少します。メイン サーバーが復旧した場合、バックアップ サーバーは再び日ごとに増加を開始します。たとえば、メイン サーバーが 20 日間ダウンしていて、その期間中バックアップ サーバーがアクティブであった場合、バックアップ サーバーには、10 日間の制限のみが残っています。バックアップ サーバーは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

フェールオーバーと共有ライセンス

ここでは、共有ライセンスとフェールオーバーの相互作用について説明します。

フェールオーバーと共有ライセンス サーバー

この項では、メイン サーバーおよびバックアップ サーバーと、フェールオーバーとの相互作用について説明します。共有ライセンス サーバーでは、VPN ゲートウェイやファイアウォールなど、ASA としての通常機能も実行されます。このため、メインとバックアップの共有ライセンス サーバーにフェールオーバーを設定して、信頼性を高めることをお勧めします。

（注） バックアップ サーバー メカニズムとフェールオーバーは異なりますが、両者には互換性があります。

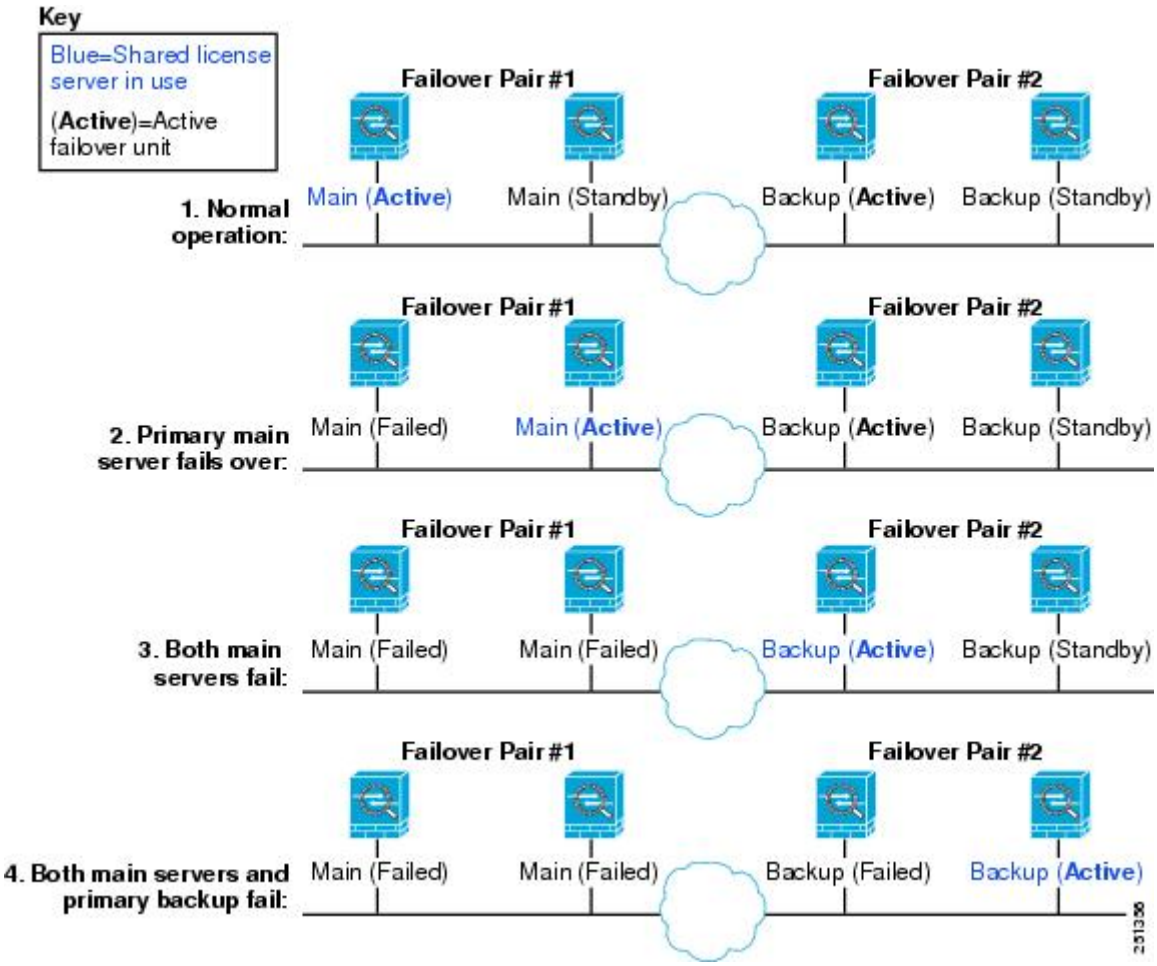
共有ライセンスはシングル コンテキスト モードでだけサポートされるため、アクティブ/アクティブ フェールオーバーはサポートされません。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置が主要な共有ライセンス サーバーとして機能し、スタンバイ装置はフェールオーバー後に主要な共有ライセンス サーバーと

して機能します。スタンバイ装置は、バックアップの共有ライセンス サーバーとしては機能しません。必要に応じて、バックアップ サーバーとして機能する装置のペアを追加します。

たとえば、2 組のフェールオーバー ペアがあるネットワークを使用するとします。ペア #1 にはメインのライセンス サーバーが含まれます。ペア #2 にはバックアップ サーバーが含まれます。ペア #1 のプライマリ装置がダウンすると、ただちに、スタンバイ装置が新しくメイン ライセンス サーバーになります。ペア #2 のバックアップ サーバーが使用されることはありません。ペア #1 の装置が両方ともダウンした場合だけ、ペア #2 のバックアップ サーバーが共有ライセンス サーバーとして使用されるようになります。ペア #1 がダウンしたままで、ペア #2 のプライマリ装置もダウンした場合は、ペア #2 のスタンバイ装置が共有ライセンス サーバーとして使用されるようになります（次の図を参照）。

図 *13 :* フェールオーバーと共有ライセンス サーバー



スタンバイ バックアップ サーバーは、プライマリ バックアップ サーバーと同じ動作制限を共有します。スタンバイ装置がアクティブになると、その時点からプライマリ装置のカウントダウンを引き継ぎます。

関連トピック

共有ライセンス バックアップ サーバーについて （126 ページ）

フェールオーバーと共有ライセンス参加システム

参加システムのペアについては、両方の装置を共有ライセンス サーバーに登録します。登録時には、個別の参加システム ID を使用します。アクティブ装置の参加システム ID は、スタンバイ装置と同期されます。スタンバイ装置は、アクティブに切り替わるときに、この ID を使用して転送要求を生成します。この転送要求によって、以前にアクティブだった装置から新しくアクティブになる装置に共有セッションが移動します。

参加者の最大数

ASA では、共有ライセンスの参加システム数に制限がありません。ただし、共有ネットワークの規模が非常に大きいと、ライセンス サーバーのパフォーマンスに影響する場合があります。この場合は、参加システムのリフレッシュ間隔を長くするか、共有ネットワークを 2 つ作成することをお勧めします。

共有ライセンス サーバーの設定

この項では、ASA を共有ライセンス サーバーとして設定する方法について説明します。

始める前に

サーバーが共有ライセンス サーバー キーを持っている必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licenses]** > **[Shared SSL VPN Licenses]** ペインを選択します。

ステップ 2 [Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。

この秘密を持つすべての参加ユニットがライセンス サーバーを使用できます。

ステップ 3 （オプション）[TCP IP Port] フィールドに、サーバーが参加ユニットからの SSL 接続を受信するポート（1 ～ 65535）を入力します。

デフォルトは、TCP ポート 50554 です。

ステップ 4 （オプション）[Refresh interval] フィールドで、10 ～ 300 秒の更新間隔を入力します。

この値は、サーバーと通信する頻度を設定するために参加ユニットに提供されます。デフォルトは 30 秒です。

ステップ 5 [Interfaces that serve shared licenses] 領域で、[Shares Licenses] チェック ボックスをオンにします。パーティシパントからサーバーへの通信には、このチェックボックスに対応するインターフェイスが使用されます。

ステップ 6 （オプション）バックアップ サーバーを指定するには、[Optional backup shared SSL VPN license server] 領域で次の手順を実行します。

a) [Backup server IP address] フィールドにバックアップ サーバーの IP アドレスを入力します。

b) [Primary backup server serial number] フィールドにバックアップ サーバーのシリアル番号を入力します。
c) バックアップ サーバーがフェールオーバー ペアの一部の場合は、[Secondary backup server serial number] フィールドでスタンバイ ユニットのシリアル番号を指定します。

1 つのバックアップ サーバーとそのオプションのスタンバイ ユニットのみを指定できます。

ステップ 7 [適用（Apply）] をクリックします。

共有ライセンス パーティシパントとオプションのバックアップ サーバーの設定

この項では、共有ライセンス サーバーと通信する共有ライセンス参加システムを設定します。このセクションでは、オプションで参加者をバックアップ サーバーとして設定する方法も説明します。

始める前に

参加システムが共有ライセンス参加キーを持っている必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licenses]** > **[Shared SSL VPN Licenses]** ペインを選択します。
ステップ 2 [Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。
ステップ 3 （任意）[TCP IP Port] フィールドに、SSL を使用してサーバーと通信するポート（1 ～ 65535）を入力します。

デフォルトは、TCP ポート 50554 です。

ステップ 4 （任意）参加ユニットをバックアップ サーバーとして指定するには、[Select backup role of participant] エリアで、次の手順を実行します。
a) [Backup Server] オプション ボタンをクリックします。
b) [Shares Licenses] チェックボックスをオンにします。パーティシパントからバックアップ サーバーへの通信には、このチェックボックスに対応するインターフェイスが使用されます。

ステップ 5 [適用（Apply）] をクリックします。

モデルごとにサポートされている機能のライセンス

この項では、各モデルに使用できるライセンスと、ライセンスに関する特記事項について説明します。

モデルごとのライセンス

この項では、各モデルに使用できる機能のライセンスを示します。

イタリック体で示された項目は、基本ライセンス（または Security Plus など）ライセンス バージョンを置換できる個別のオプション ライセンスです。オプション ライセンスは、混在させることも統一することもできます。

（注） 一部の機能は互換性がありません。互換性情報については、個々の機能の章を参照してください。

ペイロード暗号化機能のないモデルの場合は、次に示す機能の一部がサポートされません。サポートされない機能のリストについては、ペイロード暗号化機能のないモデル（116 ページ）を参照してください。

ライセンスの詳細については、ライセンスに関する注意事項（107 ページ）を参照してください。

ASA 5506-X および ASA 5506W-X のライセンス機能

次の表に、ASA 5506-X および ASA 5506W-X のライセンス機能を示します。

ライセンス	基本ライセンス	Security Plus ライセンス
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし	サポートなし
ファイアウォールの接続、同時	20,000	50,000
キャリア	サポートなし	サポートなし

ライセンス	基本ライセンス		Security Plus ライセンス	
合計 TLS プロキシセッション	160		160	
VPN ライセンス				
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *50*	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *50*
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	50		50	
VPN ロードバランシング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	サポートなし		アクティブ/スタンバイ	
セキュリティコンテキスト	サポートなし		サポートなし	
クラスタ	サポートなし		サポートなし	
VLAN、最大	5		30	

ASA 5506H-X ライセンスの各機能

次の表に、ASA 5506H-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし	
ファイアウォールの接続、同時	50,000	
キャリア	サポートなし	
合計 UC プロキシ セッション	160	
VPN ライセンス		
AnyConnect Plus または Apex ライセンス（個別に購入）、最大プレミアム ピア	50	
合計 VPN ピア。全タイプの合計	50	
その他の VPN ピア	50	
VPN ロード バランシング	イネーブル	
一般ライセンス		
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	Active/Standby または Active/Active	
セキュリティ コンテキスト	サポートなし	
クラスタ	サポートなし	
VLAN、最大	30	

ASA 5508-X ライセンスの各機能

次の表に、ASA 5508-X のライセンス機能を示します。

ライセンス	基本ライセンス		
ファイアウォール ライセンス			
Botnet Traffic Filter	サポートなし		
ファイアウォールの接続、同時	100,000		
キャリア	サポートなし		
合計 TLS プロキシ セッション	320		
VPN ライセンス			
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *100*	
合計 VPN ピア。全タイプの合計	100		
その他の VPN ピア	100		
VPN ロード バランシング	イネーブル		
一般ライセンス			
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	
フェールオーバー	Active/Standby または Active/Active		
セキュリティ コンテキスト	2	オプション ライセンス：	*5*
クラスタ	サポートなし		
VLAN、最大	50		

ASA 5516-X ライセンスの機能

次の表に、ASA 5516-X のライセンス機能を示します。

ライセンス	基本ライセンス		
ファイアウォール ライセンス			
Botnet Traffic Filter	サポートなし		
ファイアウォールの接続、同時	250,000		
キャリア	サポートなし		
合計 TLS プロキシ セッション	1000		
VPN ライセンス			
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *300*	
その他の VPN ピア	300		
合計 VPN ピア。全タイプの合計	300		
VPN ロード バランシング	イネーブル		
一般ライセンス			
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	
フェールオーバー	Active/Standby または Active/Active		
セキュリティ コンテキスト	2	オプション ライセンス：	*5*
クラスタ	2		
VLAN、最大	150		

ASA 5525-X ライセンスの各機能

次の表に、ASA 5525-X のライセンス機能を示します。

ライセンス	基本ライセンス							
ファイアウォール ライセンス								
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能						
ファイアウォールの接続、同時	500,000							
キャリア	ディセーブル	オプション ライセンス：使用可能						
合計 TLS プロキシセッション	2	オプション ライセンス：	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN ライセンス								
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *750*						
その他の VPN ピア	750							
合計 VPN ピア。全タイプの合計	750							
VPN ロードバランシング	イネーブル							
一般ライセンス								

ライセンス	基本ライセンス				
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）			
フェールオーバー	Active/Standby または Active/Active				
セキュリティ コンテキスト	2	オプション ライセンス：	*5*	*10*	*20*
クラスタ	2				
IPS モジュール	ディセーブル	オプション ライセンス：使用可能			
VLAN、最大	200				

ASA 5545-X ライセンスの機能

次の表に、ASA 5545-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能
ファイアウォールの接続、同時	750,000	
キャリア	ディセーブル	オプション ライセンス：使用可能

ライセンス	基本ライセンス									
合計 TLS プロキシセッション	2	オプション ライセンス：	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN ライセンス										
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *2500*								
その他の VPN ピア	2500									
合計 VPN ピア。全タイプの合計	2500									
VPN ロードバランシング	イネーブル									
一般ライセンス										
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）								
フェールオーバー	Active/Standby または Active/Active									
セキュリティコンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*				
クラスタ	2									
IPS モジュール	ディセーブル	オプション ライセンス：使用可能								

ライセンス	基本ライセンス
VLAN、最大	300

ASA 5555-X ライセンスの機能

次の表に、ASA 5555-X のライセンス機能を示します。

ライセンス	基本ライセンス								
ファイアウォール ライセンス									
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能							
ファイアウォールの接続、同時	1,000,000								
キャリア	ディセーブル	オプション ライセンス：使用可能							
合計 TLS プロキシ セッション	2	オプション ライセンス：							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *5000*							
その他の VPN ピア	5000								

ライセンス	基本ライセンス						
合計 VPN ピア。全タイプの合計	5000						
VPN ロードバランシング	イネーブル						
一般ライセンス							
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）					
フェールオーバー	Active/Standby または Active/Active						
セキュリティ コンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*	*100*
クラスタ	2						
IPS モジュール	ディセーブル	オプション ライセンス：使用可能					
VLAN、最大	500						

ISA 3000 ライセンスの各機能

次の表に、ISA 3000 のライセンス機能を示します。

ライセンス	基本ライセンス	Security Plus ライセンス
ファイアウォール ライセンス		

ライセンス	基本ライセンス		Security Plus ライセンス	
Botnet Traffic Filter	サポートなし		サポートなし	
ファイアウォールの接続、同時	20,000		50,000	
キャリア	サポートなし		サポートなし	
合計 TLS プロキシセッション	160		160	
VPN ライセンス				
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *25*	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *25*
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	25		50	
VPN ロードバランシング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	基本（DES）	オプション ライセンス：強化（*3DES/AES*）

ライセンス	基本ライセンス	Security Plus ライセンス
フェールオーバー	サポートなし	アクティブ/スタンバイ
セキュリティコンテキスト	サポートなし	サポートなし
クラスタ	サポートなし	サポートなし
VLAN、最大	5	25

PAK ライセンスのモニターリング

この項では、ライセンス情報の表示方法について説明します。

現在のライセンスの表示

この項では、現在のライセンスと、時間ベース アクティベーション キーの残り時間を表示する方法について説明します。

始める前に

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN および Unified Communications ライセンスは一覧に示されません。詳細については、「ペイロード暗号化機能のないモデル （116 ページ）」を参照してください。

手順

ステップ 1 （永続ライセンスとアクティブな時間ベース ライセンスの組み合わせである）実行ライセンスを表示するには、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Activation Key]** ペインを選択します。

マルチ コンテキスト モードでは、[Configuration] > [Device Management] > [Activation Key] ペインを選択し、システム実行スペースでアクティベーション キーを表示します。

フェールオーバーペアの場合、表示される実行ライセンスは、プライマリ装置とセカンダリ装置からの結合されたライセンスです。詳細については、「フェールオーバーまたは ASA クラ

スタライセンスの結合方法（114ページ）」を参照してください。数値が割り当てられた時間ベース ライセンス（期間は結合されません）の場合、[License Duration] カラムには、プライマリ装置またはセカンダリ装置からの最短の時間ベース ライセンスが表示されます。このライセンスの有効期限が切れると他の装置のライセンスの期間が表示されます。

ステップ 2 （任意）時間ベース ライセンスの詳細（ライセンスに含まれる機能やライセンス期間など）を [Time-Based License Keys Installed] 領域に表示するには、ライセンス キーを選択し、[Show License Details] をクリックします。

ステップ 3 （任意）フェールオーバーユニットで、そのユニットにインストールされている（プライマリ装置とセカンダリ装置からの結合ライセンスではない）ライセンスを [Running Licenses] 領域に表示するには、[Show information of license specifically purchased for this device alone] をクリックします。

共有ライセンスのモニターリング

共有ライセンスをモニターするには、[Monitoring] > [VPN] > [Clientless SSL VPN] > [Shared Licenses] を選択して。

PAK ライセンスの履歴

機能名	プラットフォームリリース	説明
接続数と VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
SSL VPN ライセンス	7.1(1)	SSL VPN ライセンスが導入されました。

機能名	プラットフォームリリース	説明
SSL VPN ライセンスの追加	7.2(1)	5000 ユーザーの SSL VPN ライセンスが ASA 5550 以降に対して導入されました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバーインターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。

機能名	プラットフォームリリース	説明
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、Security Plus ライセンスを使用する Ethernet 0/0 および 0/1 ポート用にギガビットイーサネット（1000 Mbps）をサポートしています。基本ライセンスでは、これらのポートは引き続きファスト イーサネット（100 Mbps）ポートとして使用されます。いずれのライセンスに対しても、Ethernet 0/2、0/3、および 0/4 はファスト イーサネット ポートのままです。 （注） インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
Advanced Endpoint Assessment ライセンス	8.0(2)	Advanced Endpoint Assessment ライセンスが導入されました。Cisco AnyConnect またはクライアントレス SSL VPN 接続の条件としてリモートコンピュータでスキャン対象となる、アンチウイルス アプリケーションやアンチスパイウェア アプリケーション、ファイアウォール、オペレーティング システム、および関連アップデートの種類が、大幅に拡張されました。また、任意のレジストリ エントリ、ファイル名、およびプロセス名を指定してスキャン対象にすることもできます。スキャン結果を ASA に送信します。ASA は、ユーザー ログイン クレデンシャルとコンピュータ スキャン結果の両方を使用して、ダイナミック アクセス ポリシー（DAP）を割り当てます。 Advanced Endpoint Assessment ライセンスを使用すると、バージョン要件を満たすように非準拠コンピュータのアップデートを試行する機能を設定して、Host Scan を拡張できます。 シスコは、Host Scan でサポートされるアプリケーションとバージョンの一覧に、Cisco Secure Desktop とは異なるパッケージで、タイムリーなアップデートを提供できます。

機能名	プラットフォームリリース	説明
ASA 5510 の VPN ロードバランシング	8.0(2)	VPN ロードバランシングが ASA 5510 Security Plus ライセンスでサポートされるようになりました。
AnyConnect for Mobile ライセンス	8.0(3)	AnyConnect for Mobile ライセンスが導入されました。これにより、Windows モバイル デバイスは AnyConnect クライアントを使用して、ASA に接続できます。
時間ベース ライセンス	8.0(4)/8.1(2)	時間ベース ライセンスがサポートされるようになりました。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
Unified Communications Proxy セッション ライセンス	8.0(4)	UC Proxy セッション ライセンスが導入されました。電話プロキシ、Presence Federation Proxy、および Encrypted Voice Inspection アプリケーションでは、それらの接続に TLS プロキシセッションが使用されます。各 TLS プロキシ セッションは、UC ライセンスの制限に対してカウントされます。これらのアプリケーションは、すべて UC Proxy として包括的にライセンスされるので、混在させたり、組み合わせたりできます。 この機能は、バージョン 8.1 では使用できません。
ボットネット トラフィック フィルタ ライセンス	8.2(1)	ボットネット トラフィック フィルタ ライセンスが導入されました。ボットネット トラフィック フィルタでは、既知の不正なドメインや IP アドレスに対する接続を追跡して、マルウェア ネットワーク アクティビティから保護します。

機能名	プラットフォームリリース	説明
AnyConnect Essentials ライセンス	8.2(1)	

機能名	プラットフォームリリース	説明
		AnyConnect Essentials ライセンスが導入されました。このライセンスにより、AnyConnect VPN クライアントは ASA にアクセスできるようになります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。 （注） AnyConnect Essentials ライセンスを所有する VPN ユーザーは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動（WebLaunch）することができます。 このライセンスと AnyConnect Premium ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。 特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。 デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用すると、AnyConnect Essentials ライセ

機能名	プラットフォームリリース	説明
		ンスを無効にして他のライセンスを使用できます。
SSL VPN ライセンスの AnyConnect Premium SSL VPN Edition ライセンスへの変更	8.2(1)	SSL VPN ライセンスの名前が AnyConnect Premium SSL VPN Edition ライセンスに変更されました。
SSL VPN の共有ライセンス	8.2(1)	SSL VPN の共有ライセンスが導入されました。複数の ASA で、SSL VPN セッションのプールを必要に応じて共有できます。
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。
ASA 5585-X（SSP-20）用 10 GE I/O ライセンス	8.2(3)	ASA 5585-X（SSP-20）の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-60 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 （注） ASA 5585-X は 8.3(x) ではサポートされていません。
ASA 5585-X（SSP-10）用 10 GE I/O ライセンス	8.2(4)	ASA 5585-X（SSP-10）の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-40 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 （注） ASA 5585-X は 8.3(x) ではサポートされていません。
同一でないフェールオーバー ライセンス	8.3(1)	フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Activation Key]。

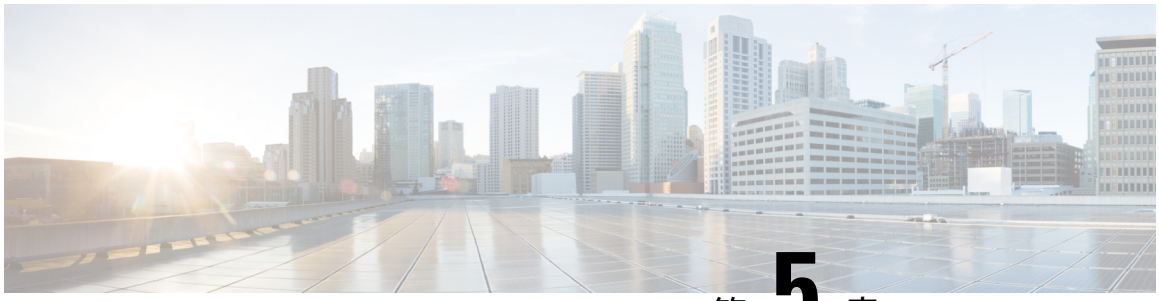
機能名	プラットフォームリリース	説明
スタック可能な時間ベース ライセンス	8.3(1)	時間ベース ライセンスがスタッカブルになりました。多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。
Intercompany Media Engine ライセンス	8.3(1)	IME ライセンスが導入されました。
複数の時間ベース ライセンスの同時アクティブ化	8.3(1)	時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Activation Key]。
時間ベース ライセンスのアクティブ化と非アクティブ化の個別化	8.3(1)	コマンドを使用して、時間ベース ライセンスをアクティブ化または非アクティブ化できるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Activation Key]。
AnyConnect Premium SSL VPN Edition ライセンスの AnyConnect Premium SSL VPN ライセンスへの変更	8.3(1)	AnyConnect Premium SSL VPN Edition ライセンスの名前が AnyConnect Premium SSL VPN ライセンスに変更されました。

機能名	プラットフォームリリース	説明
輸出用のペイロード暗号化なしイメージ	8.3(2)	ASA 5505 ～ 5550 にペイロード暗号化機能のないソフトウェアをインストールした場合、Unified Communications、強力な暗号化VPN、強力な暗号化管理プロトコルをディセーブルにします。 （注） この特殊なイメージは 8.3(x) でのみサポートされます。8.4(1) 以降で暗号化機能のないソフトウェアをサポートするには、ASA の特別なハードウェア バージョンを購入する必要があります。
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。
ASA 5580 および 5585-X での接続数の増加	8.4(1)	ファイアウォール接続の最大数が次のように引き上げられました。 • ASA 5580-20：1,000,000 から 2,000,000 へ。 • ASA 5580-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10：750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20：1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60：2,000,000 から 10,000,000 へ。

機能名	プラットフォームリリース	説明
AnyConnect Premium SSL VPN ライセンスの AnyConnect Premium ライセンスへの変更	8.4(1)	AnyConnect Premium SSL VPN ライセンスの名前が AnyConnect Premium ライセンスに変更されました。ライセンス情報の表示が「SSL VPN ピア」から「AnyConnect Premium ピア」に変更されました。
ASA 5580 での AnyConnect VPN セッション数の増加	8.4(1)	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	8.4(1)	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
IKEv2 を使用した IPsec リモート アクセス	8.4(1)	AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 （注） ASA での IKEv2 のサポートに関して、重複するセキュリティ アソシエーションがサポートされていないという制約が現在あります。 Other VPN ライセンス（以前の IPsec VPN）には IKEv2 サイトツーサイト セッションが追加されました。Other VPN ライセンスは基本ライセンスに含まれています。
輸出用のペイロード暗号化なしハードウェア	8.4(1)	ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、特定の国に ASA を輸出できるよう、ASA ソフトウェアのユニファイド コミュニケーションと VPN 機能を無効にしています。

機能名	プラットフォームリリース	説明
デュアル SSP（SSP-20 および SSP-40）	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバーペアとして使用できます。2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。
ASA 5512-X ～ ASA 5555-X での IPS モジュール ライセンス	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X での IPS SSP ソフトウェア モジュールには IPS モジュール ライセンスが必要です。
ASA 5580 および ASA 5585-X のクラスタリング ライセンス。	9.0(1)	クラスタリング ライセンスが ASA 5580 および ASA 5585-X に対して追加されました。
ASASM での VPN のサポート	9.0(1)	ASASM は、すべての VPN 機能をサポートするようになりました。
ASASM でのユニファイド コミュニケーションのサポート	9.0(1)	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート（SSP-40 および SSP-60 に加えて）、デュアル SSP に対する VPN サポート	9.0(1)	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました（同一シャーシ内で同じレベルの SSP を 2 つ使用できます）。デュアル SSP を使用するときに VPN がサポートされるようになりました。

機能名	プラットフォームリリース	説明
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。
ASAv4 および ASAv30 の標準およびプレミアム モデル ライセンスの導入	9.2(1)	シンプルなライセンス方式で ASAv が導入されました（標準またはプレミアム レベルの ASAv4 および ASAv30 永続ライセンス）。アドオン ライセンスは使用できません。



第 5 章

ライセンス：スマート ソフトウェア ライセンシング

スマート ソフトウェア ライセンシングによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンス キーを管理しなくても、簡単に ASA を導入したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

（注） スマート ソフトウェア ライセンシングは、ASA ハードウェアモデルおよび ISA 3000 ではサポートされていません。PAK ライセンスを使用します。PAK ライセンスについて （103 ページ）を参照してください。

プラットフォーム別のスマートライセンスの機能と動作の詳細については、「Smart Enabled Product Families」を参照してください。

スマート ソフトウェア ライセンスについて

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザがアクセスできるものを制御できます。スマート ライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Firepower 4100/9300 シャーシの ASA のスマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ 上の ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 4100/9300 シャーシ スーパバイザと ASA に分割されています。

- Firepower 4100/9300 シャーシ：License Authority との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャをシャーシで設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。

  注 シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマート ライセンス方式を有効にする必要があります。

- ASA アプリケーション：ASA のすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、オプションで追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社ごとにアカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびデバイスの管理をより簡単に行うことができます。

オフライン管理

デバイスにインターネット アクセスがなく、License Authority に登録できない場合は、オフライン ライセンスを設定できます。

永続ライセンスの予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、License Authority への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様にライセンスを購入し、ASA のライセンス キーをインストールします。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用します。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。

ASAv 永続ライセンスの予約

権限付与固有のライセンスを取得することで、標準層、権限付与に応じた最大スループット、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- 100 Mbps の権限付与
- 1 Gbps の権限付与
- 2 Gbps の権限付与
- 10 Gbps の権限付与
- 20 Gbps の権限付与

ASAv導入時に使用する権限付与レベルを選択する必要があります。その権限付与レベルによって、要求するライセンスが決まります。ユニットの権限付与レベルを後で変更したい場合は、現在のライセンスを返却し、正しい権限付与レベルの新しいライセンスを要求する必要があり

ます。導入済みの ASAv のモデルを変更するには、新しい権限付与の要件に合わせるために、ハイパーバイザから vCPU と DRAM の設定を変更できます。各値については、ASAv のクイックスタートガイドを参照してください。

ライセンスの使用を停止した場合、ASAv で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

永続ライセンスの予約は Azure ハイパーバイザではサポートされません。

Firepower 1000 永続ライセンスの予約

ライセンスを取得することで、標準層、Security Plus（Firepower 1010）、最大のセキュリティコンテキスト（Firepower 1100）、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 2100 永続ライセンスの予約

ライセンスを取得することで、標準層、最大のセキュリティコンテキスト、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 4100/9300 シャーシ 永続ライセンスの予約

ライセンスを取得することで、標準層、最大のセキュリティコンテキスト、キャリアライセンス、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。ライセンスは Firepower 4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、Firepower 4100/9300 シャーシで戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用し

ていないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

サテライトサーバー（Smart Software Manager オンプレミス）

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト（オンプレミス）サーバーをインストールできます。サテライト（衛星）は、Smart Software Manager 機能のサブセットを提供し、これによりすべてのローカル デバイスに重要なライセンス サービスが提供可能になります。ライセンス使用を同期するために、定期的にサテライトだけが License Authority と同期する必要があります。スケジュールに沿って同期するか、または手動で同期できます。

サテライト サーバでは、次の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、Smart Software Manager satellite を参照してください。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのデバイスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシ 上で動作する ASA の場合：シャーシのみがデバイスとして登録される一方で、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3 つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

評価ライセンス

ASAv

ASAv は、評価モードをサポートしていません。Licensing Authority への登録の前に、ASAv は厳しいレート制限状態で動作します。

Firepower 1000

Firepower 1000 は、Licensing Authority に登録する前に 90 日間（合計）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 1000 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、License Authority に登録する必要があります。

Firepower 2100

Licensing Authority への登録の前に、Firepower 210 は評価モードで 90 日間（合計使用時間）動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 2100 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、License Authority に登録する必要があります。

Firepower 4100/9300 シャーシ

Firepower 4100/9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシ レベル評価モード：Firepower 4100/9300 シャーシによる Licensing Authority への登録の前に、評価モードで 90 日間（合計使用期間）動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシが Licensing Authority に登録をした後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、License Authority に登録して永続ライセンスを取得する必要があります。

ライセンスについて（タイプ別）

ここでは、ライセンスに関する追加情報をタイプ別に説明します。

AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス

AnyConnect Plus、AnyConnect Apex、および VPN Only ライセンスは、ライセンスが指定するユーザープールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。スマー

トライセンスを使用するデバイスでは、実際のプラットフォームに AnyConnect ライセンスを物理的に適用する必要はありません。ただし、同じライセンスを購入して、ソフトウェアセンターへのアクセスやテクニカル サポートを使用するために契約番号を Cisco.com ID に関連付ける必要があります。詳細については、以下を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。
- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

暗号化ライセンス

高度暗号化：ASAv

ライセンス認証局またはサテライト サーバーに接続する前に、高度暗号化（3DES/AES）を管理接続に使用できるので、ASDM を起動してライセンス認証局に接続することができます。through-the-box トラフィックの場合、License Authority に接続して高度暗号化ライセンスを取得するまで、スループットは厳しく制限されます。

スマート ソフトウェア ライセンシング アカウントから ASAv の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASAv が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASAv はライセンスを保持し、レート制限状態に戻ることはありません。ASAv を再登録し、エクスポー

トコンプライアンスが無効になっている場合、またはASAvを工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に強力な暗号化なしでASAvを登録し、後で強力な暗号化を追加する場合は、新しいライセンスを有効にするためにASAvをリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

強力な暗号化: アプライアンス モードの Firepower 1000 および Firepower 2100

ASAには、管理アクセスのみを対象にした3DES機能がデフォルトで含まれているので、Smart Software Managerに接続でき、すぐにASDMを使用することもできます。後にASAでSSHアクセスを設定する場合は、SSHおよびSCPを使用することもできます。高度な暗号化を必要とするその他の機能（VPNなど）では、最初にSmart Software Managerに登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理1/1などの管理専用インターフェイスに接続されている場合です。SSHは影響を受けません。HTTPS接続が失われた場合は、コンソール ポートに接続してASAを再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

スマート ソフトウェア ライセンシング アカウントからASAの登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASAが後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASAを工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：プラットフォームモードの Firepower 2100

License Authority またはサテライト サーバーに接続する前に、高度暗号化（3DES/AES）を管理接続に使用できるので、ASDM を起動できます。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用できることに注意してください。高度暗号化ライセンスに接続して取得するまで、through the box トラフィックは許可されません。

スマート ソフトウェア ライセンシング アカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASA を工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：Firepower 4100/9300 シャーシ

ASA を論理デバイスとして展開すると、すぐに ASDM を起動できます。高度暗号化ライセンスに接続して取得するまで、through the box トラフィックは許可されません。

スマート ソフトウェア ライセンシング アカウントから Firepower シャーシの登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。

ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。シャーシを再登録し、エクスポートコンプライアンスが無効になっている場合、またはシャーシを工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度な暗号化なしでシャーシを登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA アプリケーションをリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

DES：すべてのモデル

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

キャリア ライセンス

キャリア ライセンスでは、以下のインスペクション機能が有効になります。

- Diameter
- GTP/GPRS
- SCTP

合計 TLS プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザー数が 250 未満のライセンス）では、TLS プロキシセッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザー数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンス

ASAv のフェールオーバー ライセンス

スタンバイ ユニットにはプライマリ ユニットと同じモデル ライセンスが必要です。

Firepower 1010 のフェールオーバー ライセンス

通常またはサテライト スマート ライセンシング

どちらの Firepower 1010 ユニットも、License Authority またはサテライトサーバに登録されている必要があります。フェールオーバーを設定する前に、両方のユニットで標準ライセンスと Security Plus ライセンスを有効にする必要があります。

通常は、ユニットの登録時に両方のユニットが強力な暗号化トークンを取得する必要があるため、ASA で強力な暗号化（3DES/AES）機能ライセンスを有効にする必要もありません。登録トークンを使用する場合、両方のユニットに同じ暗号化レベルが設定されている必要があります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。この場合、フェールオーバーを有効にした後、アクティブユニットで有効にします。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブユニットのみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となり、高度暗号化トークンを使用する場合は、高度暗号化（3DES/AES）機能ライセンスを必要とする機能の設定変更を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 1100 のフェールオーバー ライセンス

通常またはサテライト スマート ライセンシング

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリ ユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセ

ンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

（注） フェールオーバーペアを形成する場合は、各ASAに同じ暗号化ライセンスが必要です。スマート ライセンシング サーバにASAを登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の2つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマート ライセンシング サーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンシングサーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマート ライセンシング サーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクでAES/3DESを使用するには、両方のユニットをリロードする必要があります。1つのユニットだけをリロードすると、そのユニットはAES/3DES を使用しようとしますが、元のユニットはDES を使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- Standard：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Stardard ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Standard ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - 標準ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1120 ユニットの場合、それらのライセンスで最大4つのコンテキストが追加されます。アクティブ/スタンバイペアのアクティブな装置に 3 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには7つのコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が5なので、結合されたライセンスでは最大 5 つのコンテキストのみ許可されます。この場合、アクティブな Context ライセンスを 1 つのコンテキストとしてのみ設定することになる場合があります。

- 標準ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1140 ユニットの場合、それらのライセンスで最大 4 つのコンテキストが追加されます。アクティブ/アクティブペアのプライマリユニットに 4 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 8 つのコンテキストが含まれています。たとえば、一方のユニットが 5 コンテキストを使用し、他方が 3 コンテキストを使用します（合計 8 の場合）。ユニットごとのプラットフォームの制限が 10 なので、結合されたライセンスでは最大 10 のコンテキストが許可されます。8 コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 2100 のフェールオーバー ライセンス

通常またはサテライト スマート ライセンシング

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリ ユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

（注） フェールオーバーペアを形成する場合は、各ASAに同じ暗号化ライセンスが必要です。スマート ライセンシング サーバに ASA を登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の2つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマート ライセンシング サーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンシング サーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマート ライセンシング サーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクで AES/3DES を使用するには、両方のユニットをリロードする必要があります。1つのユニットだけをリロードすると、そのユニットは AES/3DES を使用しようとしますが、元のユニットは DES を使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- Standard：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Stardard ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Standard ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - Standard ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 2130 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 30 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 34 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 30 であるため、結合されたライセンスでは最大 30 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 25 のコンテキストのみを設定できます。
  - Standard ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 2130 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 14 のコンテキストが含まれています。たとえば、一方のユニットが 9 コンテキストを使用し、他方が 5 コンテキ

ストを使用します（合計 14 の場合）。ユニットごとのプラットフォームの制限が 30 であるため、結合されたライセンスでは最大 30 のコンテキストが許容されます。14 コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300のフェールオーバーライセンス

通常またはサテライト スマート ライセンシング

どちらの Firepower 4100/9300 も、フェールオーバーを設定する前に License Authority またはサテライトサーバに登録される必要があります。セカンダリ ユニットに追加費用はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

アクティブ/スタンバイフェールオーバーの ASA ライセンス設定のフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブな装置のみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライ

センスはスタンバイユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Standard：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Stardard ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Standard ライセンスには 10 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - Standard ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。アクティブ/スタンバイペアのアクティブな装置に 250 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 270 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 230 コンテキストを設定する必要があります。
  - Standard ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 30 のコンテキストが含まれています。たとえば、一方のユニットが 17 コンテキストを使用し、他方が 13 コンテキストを使用します（合計 30 の場合）。ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。30 コンテキストは制限の範囲内です。
- キャリア：アクティブのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300 の ASA クラスタライセンス

通常またはサテライト スマート ライセンシング

クラスタリング機能自体にライセンスは必要ありません。高度暗号化およびその他のオプションライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシが License Authority またはサテライトサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます:

- 標準：制御ユニットのみがサーバから標準ライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトで標準ライセンスは 10 のコンテキストを含み、すべてのクラスタ メンバー上に存在します。各ユニットの標準ライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタに 6 台の Firepower9300 モジュールがある場合を考えます。標準ライセンスは 10 のコンテキストを含みます。6 つユニットの場合、合計で 60 のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 80 のコンテキストを含みます。モジュールごとのプラットフォーム制限は 250 であるため、統合されたライセンスに最大 250 のコンテキストが許容されます。80 のコンテキストは制限範囲内です。したがって、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して 80 コンテキストを持つことになります。
  - クラスタに Firepower4110 が 3 台あるとします。標準ライセンスは 10 のコンテキストを含みます。3 つユニットの場合、合計で 30 のコンテキストが加算されます。制御ユニット上で追加の 250 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 280 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大 250 のコンテキス

トが許容されます。280 コンテキストは制限を超えています。したがって、制御ユニット上で最大 250 のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して 250 のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして 220 のコンテキストのみを設定する必要があります。

- キャリア：分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager サテライト展開用、または管理目的用）—このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

スマート ソフトウェア ライセンスの前提条件

定期およびサテライトのスマートライセンスの前提条件

ASAv、Firepower 1000、Firepower 2100

- デバイスからのインターネットアクセス、HTTP プロキシアクセス、サテライトサーバーへのアクセスを確保します。
- デバイスが License Authority の名前を解決できるように DNS サーバーを設定します。
- デバイスのクロックを設定します。プラットフォームモードの Firepower 2100 では、FXOS でクロックを設定します。

- Cisco Smart Software Manager でマスター アカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

Firepower 4100/9300

ASA ライセンス資格を設定する前に、Firepower 4100/9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

永続ライセンス予約の前提条件

- Cisco Smart Software Manager でマスター アカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。永続ライセンス予約には ASA からスマートライセンスサーバーへのインターネット接続が必要ですが、永続ライセンスの管理には Smart Software Manager が使用されます。

- 永続ライセンス予約のサポートはライセンスチームから受けられます。永続ライセンス予約を使用する理由を示す必要があります。アカウントが承認されていない場合、永続ライセンスを購入して適用することはできません。

- 専用の永続ライセンスを購入します（ライセンス PID （174 ページ）を参照）。アカウントに正しいライセンスがない場合、ASA でライセンスを予約しようとすると、「The licenses cannot be reserved because the Virtual Account does not contain a sufficient surplus of the following perpetual licenses: 1 - Firepower 4100 ASA PERM UNIV(perpetual)」のようなエラーメッセージが表示されます。

- 永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

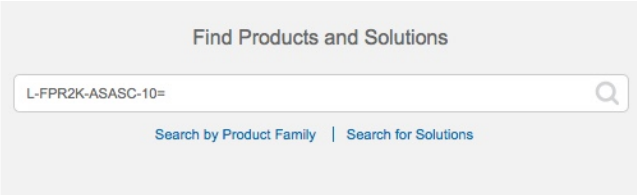
- ASAv：永続ライセンス予約は Azure ハイパーバイザではサポートされません。

ライセンス PID

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要

がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス製品 ID（PID）を検索します。

図 *14 :* ライセンス検索



ASAv PID

ASAv 定期およびサテライト スマート ライセンス PID：

- ASAv5：L-ASAV5S-K9 =
- ASAv10：L-ASAV10S-K9=
- ASAv30：L-ASAV30S-K9=
- ASAv50：L-ASAV50S-K9=
- ASAv100—L-ASAV100S-1Y=
- ASAv100—L-ASAV100S-3Y=
- ASAv100—L-ASAV100S-5Y=

（注） ASAv100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。

ASAv 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- ASAv5—L-ASAV5SR-K9=
- ASAv10—L-ASAV10SR-K9=
- ASAv30—L-ASAV30SR-K9=
- ASAv50—L-ASAV50SR-K9=
- ASAv100—L-ASAV100SR-K9=

Firepower 1010 PID

Firepower 1010 定期およびサテライト スマート ライセンス PID：

- 標準ライセンス：L-FPR1000-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- Security Plus ライセンス：L-FPR1010-SEC-PL=。Security Plus ライセンスによってフェールオーバーが有効になります。
- Strong Encryption（3DES/AES）license—L-FPR1K-ENC-K9=. アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1010 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- L-FPR1K-ASA-BPU=

Firepower 1100 PID

Firepower 1100 定期およびサテライト スマート ライセンス PID：

- 標準ライセンス：L-FPR1000-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 5 コンテキスト ライセンス：L-FPR1K-ASASC-5=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 10 コンテキストライセンス：L-FPR1K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- Strong Encryption（3DES/AES）license—L-FPR1K-ENC-K9=. アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- L-FPR1K-ASA-BPU=

Firepower 2100 PID

Firepower 2100 定期およびサテライト スマート ライセンス PID：

- 標準ライセンス：L-FPR2100-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 5 コンテキスト ライセンス：L-FPR2K-ASASC-5=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。

- 10 コンテキスト ライセンス：L-FPR2K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 強力な暗号化 (3DES/AES) のライセンス：L-FPR2K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 2100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- L-FPR2K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 定期およびサテライト スマート ライセンス PID：

- 標準ライセンス：L-FPR4100-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 10 コンテキスト ライセンス：L-FPR4K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 230 コンテキスト ライセンス：L-FPR4K-ASASC-230=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 250 コンテキスト ライセンス：L-FPR4K-ASASC-250=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、SCTP）：L-FPR4K-ASA-CAR=。
- 高度暗号化（3DES/AES）ライセンス：L-FPR4K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 4100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- L-FPR4K-ASA-BPU=

Firepower 9300 PID

Firepower 9300 定期およびサテライト スマート ライセンス PID：

- 標準ライセンス：L-F9K-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。

- 10 コンテキスト ライセンス：L-F9K-ASA-SC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、SCTP）：L-F9K-ASA-CAR=。
- 高度暗号化（3DES/AES）ライセンス：L-F9K-ASA-ENCR-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 9300 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント機能もプラットフォームの上限まで有効になります（AnyConnect Plus、AnyConnect Apex、VPN Only ライセンス （160 ページ）を参照）。

- L-FPR9K-ASA-BPU=

スマート ソフトウェア ライセンスのガイドライン

- スマート ソフトウェア ライセンスのみがサポートされます。ASAvの古いソフトウェアについては、PAK ライセンスが供与された既存の ASAv をアップグレードする場合、前にインストールしたアクティベーション キーは無視されますが、デバイスに保持されます。ASAv をダウングレードすると、アクティベーション キーが復活します。
- 永続ライセンスの予約については、デバイスを廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しいデバイスに再使用できません。
- Cisco Transport Gateway は非準拠の国番号の証明書を使用するため、ASA をその製品と組み合わせて使用する場合は HTTPS を使用できません。Cisco Transport Gateway で HTTP を使用する必要があります。

スマート ソフトウェア ライセンスのデフォルト

ASAv

- ASAv のデフォルト設定には、認証局の URL を指定する Smart Call Home プロファイルが含まれています。
- ASAv を導入するときに、機能層とスループット レベルを設定します。現時点では、標準レベルのみを使用できます。永続ライセンス予約の場合、これらのパラメータを設定する必要はありません。永続ライセンス予約を有効にすると、これらのコマンドはコンフィギュレーションから削除されます。
- また、導入時に任意で HTTP プロキシを設定できます。

Firepower 1000 および 2100

Firepower 1000 および 2100 のデフォルト設定には、Licensing Authority の URL を指定する「License」という Smart Call Home プロファイルが含まれています。

Firepower 4100/9300 シャーシ 上の ASA

デフォルト設定はありません。標準ライセンス階層、およびその他のオプション ライセンスは手動で有効化する必要があります。

ASAv：スマート ソフトウェア ライセンシングの設定

このセクションでは、ASAv にスマート ソフトウェア ライセンスを設定する方法を説明します。次の方法の中から 1 つを選択してください。

手順

ステップ 1 ASAv：定期スマート ソフトウェア ライセンシングの設定 （179 ページ）。

ステップ 2 ASAv：サテライト スマート ソフトウェア ライセンシングの設定 （182 ページ）。

ステップ 3 ASAv：ユーティリティ モードおよび MSLA スマート ソフトウェア ライセンシングの設定（184 ページ）

ステップ 4 ASAv：永続ライセンス予約の設定 （184 ページ）。

ASAv：定期スマート ソフトウェア ライセンシングの設定

ASAv を展開する場合は、デバイスを事前に設定し、License Authority に登録するために登録トークンを適用して、スマート ソフトウェア ライセンシングを有効にすることができます。HTTP プロキシ サーバー、ライセンス権限付与を変更する必要がある場合、または ASAv を登録する必要がある場合（Day0 コンフィギュレーションに ID トークンを含めなかった場合など）は、このタスクを実行します。

（注） ASAv を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASAv を展開したときに Day0 コンフィギュレーションで登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。

手順

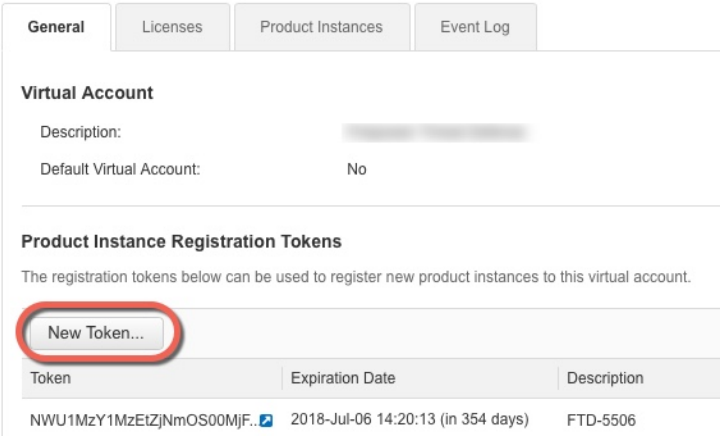
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *15*：インベントリ

b) [General] タブで、[New Token] をクリックします。

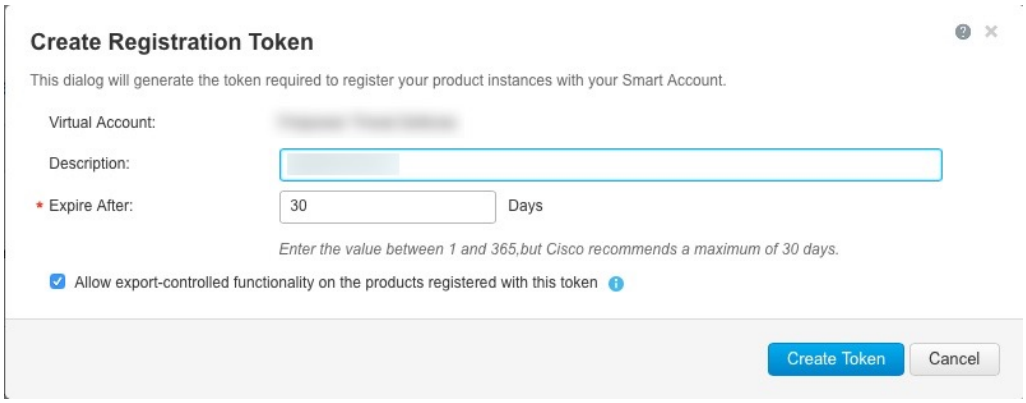
図 *16*：新しいトークン



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

図 *17*：登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *18*：トークンの表示

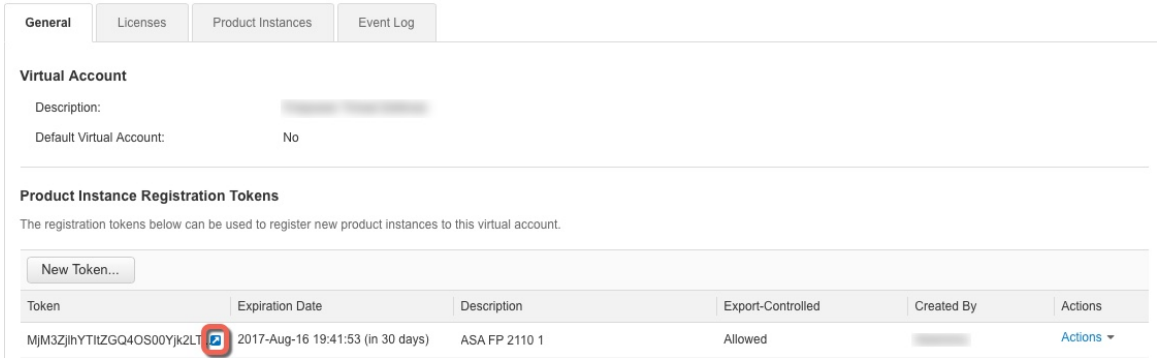
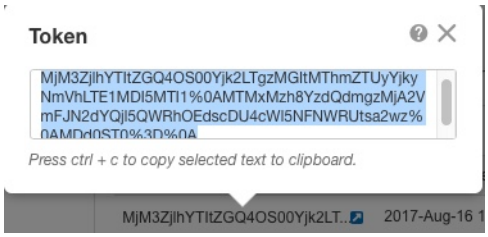


図 *19*：トークンのコピー



ステップ 2 （任意） HTTP プロキシの URL を指定します。

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

a) **[Configuration]** > **[Device Management]** > **[Smart Call-Home]** を選択します。

b) [Enable HTTP Proxy] をオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

ステップ 3 ライセンス権限付与を設定します。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。
b) [Enable Smart license configuration] をオンにします。
c) [Feature Tier] ドロップダウン メニューから [Standard] を選択します。

使用できるのは標準層だけです。

d) [Throughput Level] ドロップダウンメニューから [100M]、[1G]、[2G]、[10G]、[20G] を選択します。

（注） [Enable strong-encryption protocol] チェックボックスはオンにしないでください。この設定は、2.3.0 より前のサテライト サーバー専用です。

e) [Apply] をクリックします。

ステップ 4 ASAv の License Authority への登録。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。
b) [Register] をクリックします。
c) [ID Token] フィールドに登録トークンを入力します。
d) （オプション）[Force registration] チェックボックスをオンにして、License Authority と同期されていない可能性がある登録済みの ASAv を登録します。

たとえば、Smart Software Manager から誤って ASAv を削除した場合に **Force registration** を使用します。

e) [Register] をクリックします。

ASAv は、License Authority への登録を試み、設定されたライセンス資格の認証を要求します。

ASAv：サテライト スマート ソフトウェア ライセンシングの設定

この手順は、サテライト スマート ソフトウェア ライセンシング サーバーを使用する ASAv に適用されます。

始める前に

Smart Software Manager サテライト OVA ファイルを Cisco.com からダウンロードし、VMwareESXi サーバーにインストールおよび設定します。詳細については、Smart Software Manager satellite を参照してください。

手順

ステップ 1 サテライト サーバーで登録トークンを要求します。

ステップ 2 （任意） ASDM で、HTTP プロキシ URL を指定します。

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

a) **[Configuration]** > **[Device Management]** > **[Smart Call-Home]** を選択します。
b) [Enable HTTP Proxy] をオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

ステップ 3 ライセンス サーバーの URL を変更して、サテライト サーバーに移動します。

a) **[Configuration]** > **[Device Management]** > **[Smart Call-Home]** を選択します。
b) [Configure Subscription Profiles] 領域で、[License] プロファイルを編集します。
c) [Deliver Subscriptions Using HTTP transport] 領域で、[Subscribers] URL を選択し、[Edit] をクリックします。
d) [Subscribers] URL を次の値に変更し、[OK] をクリックします。

https://*satellite_ip_address*/**Transportgateway/services/DeviceRequestHandler**

e) [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 4 ASA を License Authority に登録します。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。
b) [Register] をクリックします。
c) [ID Token] フィールドに登録トークンを入力します。
d) （オプション）[Force registration] チェックボックスをオンにして、License Authority と同期されていない可能性がある登録済みの ASA を登録します。

たとえば、Smart Software Manager から誤って ASA を削除した場合に [Force registration] を使用します。

e) [Register] をクリックします。

ASA は、License Authority に登録し、設定されたライセンス権限付与の認証を要求します。License Authority は、ご使用のアカウントが許可すれば強力な暗号化（3DES/AES）ライセ

ンスも適用します。ライセンス ステータスを確認する場合は、[Monitoring] > [Properties] > [Smart License] の順に選択します。

ASAv：ユーティリティ モードおよび MSLA スマート ソフトウェア ライセンシングの設定

この手順は、マネージドサービスライセンス契約（MSLA）プログラムに登録されているスマートライセンシングユーティリティモードの ASAv に適用されます。ユーティリティモードでは、Smart Agent はライセンスの権限付与の使用状況を時間単位で追跡します。Smart Agent は、ライセンスの使用状況レポートを 4 時間ごとにライセンスサテライトまたはサーバーに送信します。使用状況レポートは課金サーバーに転送され、お客様にライセンスの使用に関する月次請求書が送信されます。

始める前に

Smart Software Manager サテライト OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、Smart Software Manager satellite を参照してください。

ASAv：永続ライセンス予約の設定

ASAv に永続ライセンスを割り当てることができます。このセクションでは、ASAv の廃棄やモデル層の変更などにより新しいライセンスが必要となった場合に、ライセンスを返却する方法について説明します。

手順

ステップ 1 ASAv パーマネント ライセンスのインストール （184 ページ）

ステップ 2 （任意） （オプション）ASAv のパーマネント ライセンスの返却 （187 ページ）

ASAv パーマネント ライセンスのインストール

インターネット アクセスを持たない ASAvs の場合は、Smart Software Manager からパーマネント ライセンスを要求できます。

（注） パーマネント ライセンスの予約については、ASAv を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASAv に再使用できません。（オプション）ASAv のパーマネント ライセンスの返却 （187 ページ）を参照してください。

（注） 永久ライセンスをインストールした後に設定をクリアした場合（**write erase** を使用するなど）、ステップ 1 に示すように、引数を指定せずに **license smart reservation** コマンドを使用して永久ライセンスの予約を再度有効にする必要があります。この手順の残りの部分を完了する必要はありません。

始める前に

- パーマネント ライセンスを購入すると、Smart Software Manager でそれらを使用できます。すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。
- ASAv の起動後にパーマネント ライセンスを要求する必要があります。第 0 日コンフィギュレーションの一部としてパーマネント ライセンスをインストールすることはできません。

手順

ステップ 1 ASAv CLI で、パーマネント ライセンスの予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

次のコマンドが削除されます。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

通常のスマート ライセンスを使用するには、このコマンドの **no** 形式を使用し、上記のコマンドを再入力します。その他の Smart Call Home 設定はそのまま維持されますが、使用されないため、それらのコマンドを再入力する必要はありません。

ステップ 2 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

ASAv 導入時に使用するモデルレベル（ASAv5/ASAv10/ASAv30/ASAv50）を選択する必要があります。そのモデル レベルによって、要求するライセンスが決まります。後でモデル レベルを変更したい場合は、現在のライセンスを返却し、変更後のモデル レベルに対応する新規ライセンスを要求する必要があります。既に導入されている ASAv のモデルを変更するには、ハイパーバイザから vCPU と DRAM の設定を新しいモデル要件に合わせて変更できます。 これらの値については、ASAv クイック スタート ガイドを参照してください。現在のモデルを表示するには、**show vm** コマンドを使用します。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネント ライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASAv にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。（オプション）ASAv のパーマネント ライセンスの返却 （187 ページ）を参照してください。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 [License Reservation] をクリックして、ASAv のコードをボックスに入力します。[Reserve License] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネント ライセンスの予約について承認されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 5 ASAv で、承認コードを次のように入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

これで、ASAv ライセンスが完全に適用されました。

（オプション）ASAv のパーマネント ライセンスの返却

パーマネント ライセンスが不要になった場合（ASAv を廃棄する場合や ASAv のモデル レベルの変更によって新しいライセンスが必要になった場合など）、以下の手順に従ってライセンスを正式に Smart Software Manager に戻す必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために容易に解除できなくなります。

手順

ステップ 1 ASAv で返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちに ASAv のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しいパーマネント ライセンスを要求する（**license smart reservation request universal**）か、ASAv のモデル レベルを変更する（電源を切り vCPU/RAM を変更する）と、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

ステップ 2 ASAv ユニバーサル デバイス識別子（UDI）を表示して、Smart Software Manager 内でこの ASAv インスタンスを見つけます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASAv を確認し、**[Actions]** > **[Remove]** を選択して、ASAv の返却コードをボックスに入力します。[Remove Product Instance] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

（オプション）ASAv の登録解除（定期およびサテライト）

ASAv の登録を解除すると、アカウントから ASAv が削除され、ASAv のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい ASAv に利用することもできます。あるいは、Smart Software Manager（SSM）から ASAv を削除できます。

（注） ASAv を登録解除すると、ASAv をリロードした後に、重大なレート制限状態に戻ります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 [登録解除（Unregister）] をクリックします。

ASAv がリロードされます。

（オプション）ASAv ID 証明書またはライセンス権限付与の更新（定期およびサテライト）

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 アイデンティティ証明書を更新するには、[Renew ID Certificate] をクリックします。

ステップ 3 ライセンス資格を更新するには、[Renew Authorization] をクリックします。

Firepower1000、2100：スマート ソフトウェア ライセンシングの設定

この項では、Firepower 1000、 2100 にスマート ソフトウェア ライセンシングを設定する方法を説明します。次の方法の中から 1 つを選択してください。

手順

ステップ 1 Firepower 1000、2100：定期スマート ソフトウェア ライセンシングの設定 （189 ページ）。

（オプション）Firepower 1000、2100 の登録解除（定期およびサテライト） （199 ページ） または （オプション）Firepower 1000、2100 ID 証明書またはライセンス権限付与の更新（定期およびサテライト） （199 ページ） も可能です。

ステップ 2 Firepower 1000、2100：サテライト スマート ソフトウェア ライセンシングの設定 （193 ページ）。

（オプション）Firepower 1000、2100 の登録解除（定期およびサテライト） （199 ページ） または （オプション）Firepower 1000、2100 ID 証明書またはライセンス権限付与の更新（定期およびサテライト） （199 ページ） も可能です。

ステップ 3 Firepower 1000、2100：永続ライセンス予約の設定 （195 ページ）。

Firepower1000、2100：定期スマートソフトウェアライセンシングの設定

この手順は、License Authority を使用した ASA に適用されます。

手順

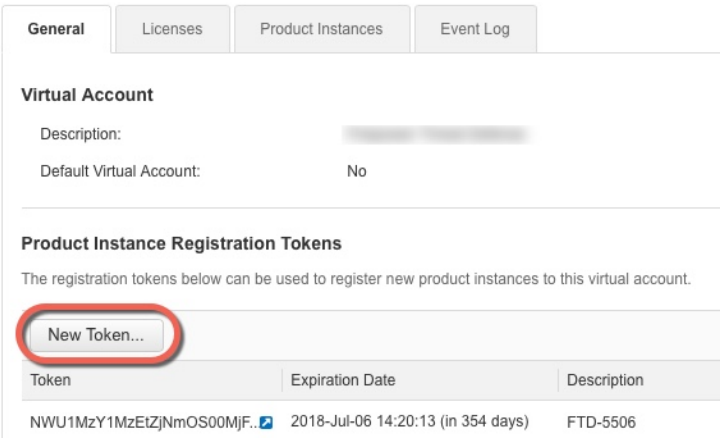
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *20:* インベントリ

b) [General] タブで、[New Token] をクリックします。

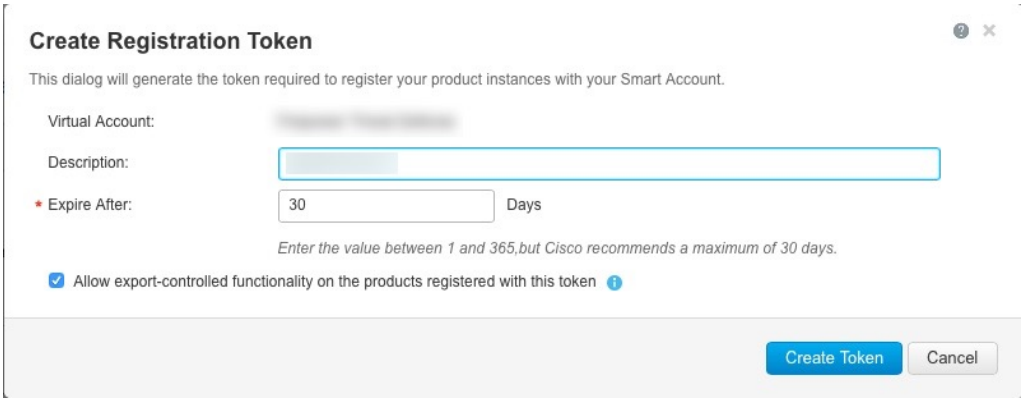
図 *21* : 新しいトークン



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

図 *22* : 登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *23*：トークンの表示

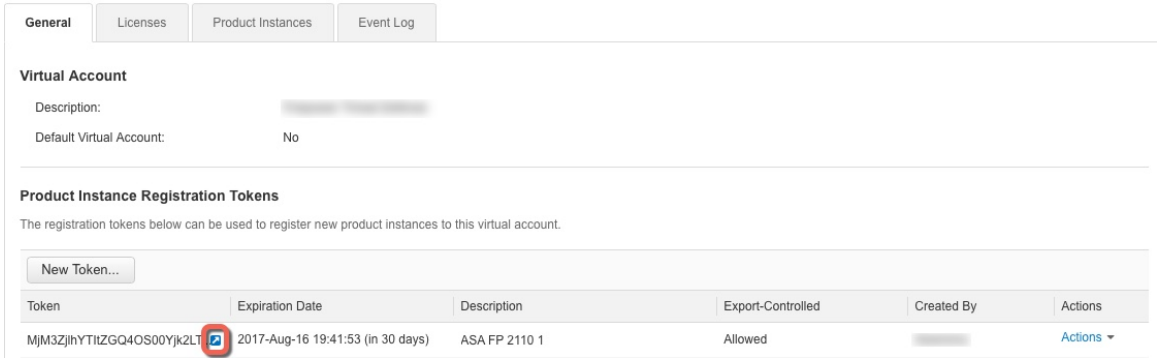
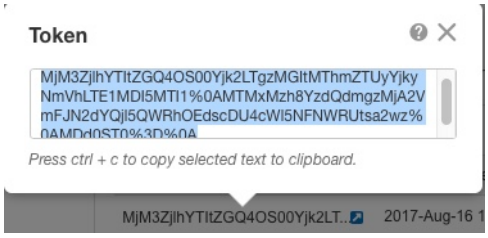


図 *24*：トークンのコピー



ステップ 2 （任意） ASDM で、HTTP プロキシ URL を指定します。

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

a) **[Configuration]** > **[Device Management]** > **[Smart Call-Home]** を選択します。
b) [Enable HTTP Proxy] をオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

ステップ 3 ライセンス権限付与を設定します。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。
b) [Enable Smart license configuration] をオンにします。
c) [Feature Tier] ドロップダウン メニューから [Standard] を選択します。

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

d) （任意） (Firepower 1010）Check **Enable Security Plus**.

Security Plus 層では、アクティブ/スタンバイ フェールオーバーが有効になります。

e) （任意） [Context] ライセンスの場合、コンテキストの数を入力します。

（注） このライセンスは、Firepower 1010 ではサポートされていません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：15 コンテキスト
- Firepower 2110：25 コンテキスト
- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

f) （任意）一般的に、[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] をオンにする必要はありません。たとえば、古いサテライト サーバーのバージョン（2.3.0 より前）を使用する ASA にはこのライセンスが必要ですが、このチェックボックスは、必要な場合、または自分のアカウントでのこのライセンスの使用状況を追跡する場合にはオンにできます。

g) [Apply] をクリックします。

ステップ 4 ASA を License Authority に登録します。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

b) [Register] をクリックします。

c) [ID Token] フィールドに登録トークンを入力します。

d) （オプション）[Force registration] チェックボックスをオンにして、License Authority と同期されていない可能性がある登録済みの ASA を登録します。

たとえば、Smart Software Manager から誤って ASA を削除した場合に [Force registration] を使用します。

e) [Register] をクリックします。

ASA は、License Authority に登録し、設定されたライセンス権限付与の認証を要求します。License Authority は、ご使用のアカウントが許可すれば強力な暗号化（3DES/AES）ライセンスも適用します。ライセンス ステータスを確認する場合は、[Monitoring] > [Properties] > [Smart License] の順に選択します。

Firepower 1000、2100：サテライト スマート ソフトウェア ライセンシングの設定

この手順は、サテライト スマート ソフトウェア ライセンシング サーバーを使用する ASA に適用されます。

始める前に

Smart Software Manager サテライト OVA ファイルを Cisco.com からダウンロードし、VMwareESXi サーバーにインストールおよび設定します。詳細については、Smart Software Manager satellite を参照してください。

手順

ステップ 1 サテライト サーバーで登録トークンを要求します。

ステップ 2 （任意） ASDM で、HTTP プロキシ URL を指定します。

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

a) **[Configuration]** > **[Device Management]** > **[Smart Call-Home]** を選択します。
b) [Enable HTTP Proxy] をオンにします。
c) [Proxy server] および [Proxy port] フィールドにプロキシの IP アドレスとポートを入力します。たとえば、HTTPS サーバーのポート 443 を入力します。
d) [Apply] をクリックします。

ステップ 3 ライセンス サーバーの URL を変更して、サテライト サーバーに移動します。

a) **[Configuration]** > **[Device Management]** > **[Smart Call-Home]** を選択します。
b) [Configure Subscription Profiles] 領域で、[License] プロファイルを編集します。
c) [Deliver Subscriptions Using HTTP transport] 領域で、[Subscribers] URL を選択し、[Edit] をクリックします。
d) [Subscribers] URL を次の値に変更し、[OK] をクリックします。

https://*satellite_ip_address*/**Transportgateway/services/DeviceRequestHandler**

e) [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 4 ライセンス権限付与を設定します。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。
b) [Enable Smart license configuration] をオンにします。
c) [Feature Tier] ドロップダウン メニューから [Standard] を選択します。

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

d) （任意） (Firepower 1010）Check **Enable Security Plus**.

Security Plus 層では、アクティブ/スタンバイ フェールオーバーが有効になります。

e) （任意） [Context] ライセンスの場合、コンテキストの数を入力します。

（注） このライセンスは、Firepower 1010 ではサポートされていません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：15 コンテキスト
- Firepower 2110：25 コンテキスト
- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

f) （任意） 一般的に、[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] をオンにする必要はありません。たとえば、古いサテライト サーバーのバージョン（2.3.0 より前）を使用する ASA にはこのライセンスが必要ですが、このチェックボックスは、必要な場合、または自分のアカウントでのこのライセンスの使用状況を追跡する場合にはオンにできます。

g) [Apply] をクリックします。

ステップ 5 ASA を License Authority に登録します。

a) **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

b) [Register] をクリックします。

c) [ID Token] フィールドに登録トークンを入力します。

d) （オプション）[Force registration] チェックボックスをオンにして、License Authority と同期されていない可能性がある登録済みの ASA を登録します。

たとえば、Smart Software Manager から誤って ASA を削除した場合に [Force registration] を使用します。

e) [Register] をクリックします。

ASA は、License Authority に登録し、設定されたライセンス権限付与の認証を要求します。License Authority は、ご使用のアカウントが許可すれば強力な暗号化（3DES/AES）ライセ

ンスも適用します。ライセンス ステータスを確認する場合は、[Monitoring] > [Properties] > [Smart License] の順に選択します。

Firepower 1000、2100：永続ライセンス予約の設定

Firepower 1000、2100 に永続ライセンスを割り当てることができます。この項では、ASA を廃止する場合にライセンスを返す方法についても説明します。

手順

ステップ 1 Firepower 1000、2100 永続ライセンスのインストール （195 ページ）。

ステップ 2 （任意） （オプション）Firepower 1000、2100永続ライセンスの返却 （198 ページ）。

Firepower 1000、2100 永続ライセンスのインストール

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。永続ライセンスでは、すべての機能が有効になります（セキュリティコンテキストが最大の標準ライセンス）。

（注） 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。（オプション）Firepower 1000、2100永続ライセンスの返却 （198 ページ）を参照してください。

始める前に

パーマネント ライセンスを購入すると、Smart Software Manager でそれらを使用できます。すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

手順

ステップ 1 ASA CLI で、永続ライセンスの予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

ステップ 2 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネント ライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。（オプション）Firepower 1000、2100永続ライセンスの返却 （198 ページ）を参照してください。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 [License Reservation] をクリックして、ASA のコードをボックスに入力します。[Reserve License] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネント ライセンスの予約について承認されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 5 ASA で、承認コードを次のように入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

ステップ 6 ASA でライセンス権限付与を要求します。

ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能階層を設定します。

feature tier standard

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

c) セキュリティコンテキストのライセンスを要求します。

feature context *number*

（注） このライセンスは、Firepower 1010 ではサポートされていません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：15 コンテキスト
- Firepower 2110：25 コンテキスト
- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Firepower 1010）Request the Security Plus license to enable Active/Standby Failover.

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意） 高度暗号化（3DES/AES）ライセンスは、通常は必要ありません。たとえば、古いサテライトサーバーのバージョン（2.3.0 より前）を使用する ASA にはこのライセンスが必要ですが、この機能は、必要とされる場合、または自分のアカウントでのこのライセンスの使用状況を追跡する場合に有効にできます。

feature strong-encryption

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

（オプション）Firepower 1000、2100永続ライセンスの返却

永続ライセンスが不要になった場合（ASA を廃止する場合など）は、この手順を使用して正式に Smart Software Manager にライセンスを返却する必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために容易に解除できなくなります。

手順

ステップ 1 ASA で返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちに ASA のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンス（**license smart reservation request universal**）を要求すると、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。評価期間が終了すると、ASA は期限切れ状態に移行します。コンプライアンス違反状態の詳細については、コンプライアンス逸脱状態 （216 ページ）を参照してください。

ステップ 2 ASA ユニバーサル デバイス識別子（UDI）が表示されるので、Smart Software Manager で ASA インスタンスを見つけることができます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASA を確認し、**[Actions]** > **[Remove]** を選択して、ASA の返却コードをボックスに入力します。[Remove Product Instance] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

（オプション）Firepower1000、2100の登録解除（定期およびサテライト）

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。あるいは、Smart Software Manager（SSM）から ASA を削除できます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 [登録解除（Unregister）] をクリックします。

（オプション）Firepower1000、2100ID証明書またはライセンス権限付与の更新（定期およびサテライト）

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 アイデンティティ証明書を更新するには、[Renew ID Certificate] をクリックします。

ステップ 3 ライセンス資格を更新するには、[Renew Authorization] をクリックします。

Firepower 4100/9300：スマート ソフトウェア ライセンシングの設定

このセクションでは、Firepower 4100/9300 シャーシ にスマート ソフトウェア ライセンスを設定する方法を説明します。

手順

ステップ 1 Firepower 4100/9300：2.3.0 より前のサテライト スマート ソフトウェア ライセンシングの設定（200ページ）。事前2.3.0バージョンのサテライト サーバーを使用して、シャーシを開始する必要があります; CLI で ASA のライセンスの設定事前のライセンスに関する通信を設定する FXOS 構成ガイドを参照してください。

ステップ 2 Firepower 4100/9300：スマート ソフトウェア ライセンシングの設定 （202 ページ）

Firepower 4100/9300：2.3.0 より前のサテライト スマート ソフトウェア ライセンシングの設定

事前2.3.0バージョンのサテライト サーバーを使用して、シャーシを開始する必要があります; CLI で ASA のライセンスの設定事前のライセンスに関する通信を設定する FXOS 構成ガイドを参照してください。

（注） 2.3.0 より前の Smart Software Manager サテライト ユーザーの場合：高度暗号化（3DES/AES）ライセンスはデフォルトで有効になっていないため、ASA CLI を使用して高度暗号化ライセンスをリクエストするまで、ASA の設定に ASDM を使用することはできません。VPN を含む他の強力な暗号化機能も、このリクエストを行うまでは使用できません。

始める前に

ASA クラスタの場合は、設定作業のために制御ユニットにアクセスする必要があります。Firepower Chassis Manager で、制御ユニットを確認します。この手順に示すように、ASA CLI からも確認できます。

手順

ステップ 1 Firepower 4100/9300 シャーシ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* **console connect asa**

例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

次回 ASA コンソールに接続するときは、ASA に直接移動します。**connect asa** を再入力する必要はありません。

ASA クラスタの場合、ライセンス設定などの設定を行う場合にのみ、制御ユニットにアクセスする必要があります。通常、制御ユニットがスロット 1 にあるため、このモジュールにまず接続する必要があります。

ステップ 2 ASA CLI で、グローバル コンフィギュレーション モードを入力します。論理デバイスの展開時に設定しない限り、デフォルトではイネーブルパスワードは空白ですが、**enable** コマンドを最初に入力したときに変更するように求められます。

enable configure terminal

例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa# configure terminal
asa(config)#
```

ステップ 3 ASA クラスタの場合は、必要に応じて、このユニットが制御ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
```

```
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

別のユニットが制御ユニットの場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

ステップ 4 ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

ステップ 5 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。アカウントに十分なティアライセンスが必要です。そうでないと、他の機能ライセンスまたはライセンスを必要とする機能を設定できません。

ステップ 6 次の機能の 1 つ以上をリクエストします。

- キャリア（GTP/GPRS、Diameter、および SCTP インスペクション）

  feature carrier

- セキュリティ コンテキスト

  feature context *<1-248>*

  永続ライセンスの予約では、最大コンテキスト（248）を指定できます。

- 高度暗号化（3DES/AES）

  feature strong-encryption

ステップ 7 ASA コンソールを終了して Telnet アプリケーションに戻るには、プロンプトで「**~**」と入力します。スーパバイザ CLI に戻るには、「**quit**」と入力します。

Firepower 4100/9300：スマート ソフトウェア ライセンシングの設定

この手順は、License Authority を使用するシャーシ、2.3.0 以降のサテライト サーバーのユーザー、または永続ライセンスの予約に適用されます。ライセンス通信を事前設定するにはFXOS

設定ガイドを参照してください。2.3.0 より前のサテライト サーバーでは、最初に CLI でライセンスを設定する必要があります。サテライト サーバー バージョン 2.3.0 以降では、高度暗号化（3DES/AES）エクスポート準拠トークンがサポートされているため、他のライセンス権限付与を要求する前に ASDM を実行できます。

永続ライセンス予約の場合、ライセンスはすべての機能、すなわちセキュリティ コンテキストが最大の標準ティアおよびキャリア ライセンスを有効にします。ただし、ASA がこれらの機能を使用することを「認識する」ためには、ASA でそれらを有効にする必要があります。

（注） 2.3.0 より前のサテライト サーバー ユーザーの場合は、Firepower 4100/9300：2.3.0 より前のサテライト スマート ソフトウェア ライセンシングの設定 （200 ページ） を参照して CLI でライセンスを設定してください。

始める前に

ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 [Feature Tier] ドロップダウン メニューから [Standard] を選択します。

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。アカウントに十分なティアライセンスが必要です。そうでないと、他の機能ライセンスまたはライセンスを必要とする機能を設定できません。

ステップ 3 **2.3.0 より前のサテライト サーバー ユーザーのみ**：[Strong Encryption] ライセンスを無効にしないでください。これは ASDM アクセスに必要です。

ステップ 4 （任意） [Mobile SP] [Carrier] を確認します。

ステップ 5 （任意） [Context] ドロップダウン メニューから、必要なコンテキストの番号を選択します。

永続ライセンスの予約では、最大コンテキスト（248）を指定できます。

ステップ 6 [Apply] をクリックします。

ステップ 7 ASDM を終了し、再起動します。

ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

モデルごとのライセンス

このセクションでは、ASAv および Firepower 4100/9300 シャーシASA セキュリティ モジュールに使用可能なライセンス資格を示します。

ASAv

すべての ASAv ライセンスは、サポートされているすべての ASAv vCPU/メモリ構成で使用できます。これにより、ASAv を使用しているお客様は、さまざまな VM リソースフットプリントでの実行が可能になります。また、サポート対象の AWS および Azure インスタンスタイプの数も増えます。ASAv VM を構成する場合、サポートされる最大 vCPU 数は 8 個です（VMware と KVM 上の ASAv100 では 16 個）。また、サポートされる最大メモリ容量は 64 GB RAM です。

重要 ASAv の最小メモリ要件は 2 GB です。現在の ASAv が 2 GB 未満のメモリで動作している場合、ASAv VM のメモリを増やさずに、以前のバージョンから 9.13(1) 以降のバージョンにアップグレードすることはできません。また、最新バージョンを使用して新しい ASAv VM を再導入することもできます。

1 つ以上の vCPU を使用して ASAv を導入する場合、ASAv の最小メモリ要件は 4 GB です。

柔軟なライセンスのガイドライン

- ライセンスされた機能およびライセンスされていないプラットフォーム機能のセッション制限は、VM メモリの量に基づいて設定されます。
- AnyConnect および TLS プロキシのセッション制限は、ASAv プラットフォームの権限付与によって決定されます。セッション制限は、ASAv モデルタイプ（ASAv5/10/30/50/100）に関連付けられなくなりました。

  セッション制限には最小メモリ要件があります。VM メモリが最小要件を下回っている場合、セッション制限はそのメモリ量でサポートされる最大数に設定されます。
- ファイアウォール接続、同時接続、および VLAN は、ASAv メモリに基づくプラットフォームの制限です。
- 権限付与の制限はありません。すべての権限付与は、vCPU（最大 8 個、VMware と KVM 上の ASAv100 では最大 16 個）とメモリ（最大 64 GB）の任意の組み合わせで実行できます。
- 既存の権限付与に変更はありません。権限付与 SKU と表示名には、引き続きモデル番号（ASAv5/10/30/50/100）が含まれます。
- 権限付与は、レート制限を介して最大スループットを設定します。
- お客様の発注プロセスに変更はありません。

ライセンス	柔軟なライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	イネーブル
通信事業者	イネーブル
Total TLS Proxy Sessions	100 Mbps の権限付与：500 1 Gbps の権限付与：500 2 Gbps の権限付与：1000 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
VPN ライセンス	
AnyConnect ピア	100 Mbps の権限付与：50 1 Gbps の権限付与：250 2 Gbps の権限付与：750 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
その他の VPN ピア	100 Mbps の権限付与：50 1 Gbps の権限付与：250 2 Gbps の権限付与：1000 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
合計 VPN ピア。全タイプの合計	100 Mbps の権限付与：50 1 Gbps の権限付与：250 2 Gbps の権限付与：1000 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
一般ライセンス	

ライセンス	柔軟なライセンス
スループット レベル	ASAv STD 100M：100 Mbps ASAv STD 1G：1 Gbps ASAv STD 2G：2 Gbps ASAv STD 10G：10 Gbps ASAv STD 20G：20 Gbps
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）
フェールオーバー	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし
クラスタ	サポートなし
vCPUs、RAM	サポートされる最大 vCPU 数は 8 個です（VMware と KVM 上の ASAv100 では 16 個）。また、サポートされる最大メモリ容量は 64 GB RAM です。vCPU とメモリの任意の組み合わせを使用して、任意の ASAv 権限付与レベルを展開できます。 • ASAv の最小メモリ要件は 2 GB です。 • 1 つ以上の vCPU を使用して ASAv を導入する場合、ASAv の最小メモリ要件は 4 GB です。 • プラットフォームの制限は、必要なメモリの量によって適用されます。 • セッション制限は、展開されている権限付与のタイプによって異なり、最小メモリ要件によって適用されます。 • 100 Mbps の権限付与：2 ～ 7.9 GB • 1 Gbps の権限付与：2 ～ 7.9 GB • 2 Gbps の権限付与：8 ～ 15.9 GB • 10 Gbps の権限付与：16 ～ 31.9 GB • 20 Gbps の権限付与：32 ～ 64 GB

プラットフォームの制限

ファイアウォール接続、同時接続、および VLAN は、ASAv メモリに基づくプラットフォームの制限です。

（注） ASAv がライセンスされていない状態にある場合、ファイアウォール接続は 100 に制限されます。権限付与によってライセンスが付与されると、接続はプラットフォームの制限に移行します。ASAv の最小メモリ要件は 2 GB です。

表 *9:* プラットフォームの制限

ASAv メモリ	ファイアウォールの接続、同時	VLANs
2 GB ～ 7.9 GB	100,000	50
8 GB ～ 15.9 GB	500,000	200
16 ～ 31.9 GB	2,000,000	1024
32 GB ～ 64 GB	4,000,000	1024

Firepower 1010

次の表に、Firepower 1010 のライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	100,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシセッション	4,000	
VPN ライセンス		
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus* または *Apex* ライセンス、最大：*75*
その他の VPN ピア	75	
合計 VPN ピア。全タイプの合計	75	

ライセンス	Standard ライセンス	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
Security Plus（フェールオーバー)	ディセーブル	オプション
セキュリティ コンテキスト	サポートしない	
クラスタ	サポートしない	
VLAN、最大	60	

Firepower 1100 シリーズ

次の表に、Firepower 1100 シリーズのライセンス機能を示します。

ライセンス	Standard ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。
ファイアウォールの接続、同時	Firepower 1120：200,000 Firepower 1140：400,000 Firepower 1150：600,000
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。
合計 TLS プロキシ セッション	Firepower 1120：4,000 Firepower 1140：8,000 Firepower 1150：8,000
VPN ライセンス	

ライセンス	Standard ライセンス	
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus* または *Apex* ライセンス、最大： *Firepower 1120*：*150* *Firepower 1140*：*400* *Firepower 1150*：*800*
その他の VPN ピア	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
合計 VPN ピア。全タイプの合計	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大値： *Firepower 1120*：*5* *Firepower 1140*：*5* *Firepower 1150*：*25*
クラスタ	サポートしない	
VLAN、最大	1024	

Firepower 2100 シリーズ

次の表に、Firepower 2100 シリーズのライセンス機能を示します。

ライセンス	Standard ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。

ライセンス	Standard ライセンス	
ファイアウォールの接続、同時	Firepower 2110：1,000,000 Firepower 2120：1,500,000 Firepower 2130：2,000,000 Firepower 2140：3,000,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシ セッション	Firepower 2110：4,000 Firepower 2120：8,000 Firepower 2130：8,000 Firepower 2140：10,000	
VPN ライセンス		
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus* または *Apex* ライセンス、最大： *Firepower 2110：1,500* *Firepower 2120：3,500* *Firepower 2130：7,500* *Firepower 2140：10,000*
その他の VPN ピア	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
合計VPN ピア。全タイプの合計	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	

ライセンス	Standard ライセンス	
セキュリティ コンテキスト	2	オプション ライセンス、最大 *5* または *10* の増分： *Firepower 2110*：*25* *Firepower 2120*：*25* *Firepower 2130*：*30* *Firepower 2140*：*40*
クラスタ	サポートしない	
VLAN、最大	1024	

Firepower 4100 シリーズ ASA アプリケーション

次の表に、Firepower 4100 シリーズ ASA アプリケーションのライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 4110：10,000,000 Firepower 4112：10,000,000 Firepower 4115：15,000,000 Firepower 4120：15,000,000 Firepower 4125：25,000,000 Firepower 4140：25,000,000 Firepower 4145：40,000,000 Firepower 4150：35,000,000	
通信事業者	ディセーブル	オプション ライセンス：通信事業者
合計 TLS プロキシセッション	Firepower 4110：10,000 その他すべて：15,000	
VPN ライセンス		

ライセンス	Standard ライセンス	
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus* または *Apex* ライセンス： *Firepower 4110*：*10,000* その他すべて：*20,000*
その他の VPN ピア	Firepower 4110：10,000 その他すべて：20,000	
合計 VPN ピア。全タイプの合計	Firepower 4110：10,000 その他すべて：20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプション ライセンス：最大 *250*、*10* 単位
クラスタ	イネーブル	
VLAN、最大	1024	

Firepower 9300 ASA アプリケーション

次の表に、Firepower 9300 ASA アプリケーションのライセンス機能を示します。

ライセンス	Standard ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。

ライセンス	Standard ライセンス	
ファイアウォールの接続、同時	Firepower 9300 SM-56：60,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ） Firepower 9300 SM-48：60,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ） Firepower 9300 SM-44：60,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ） Firepower 9300 SM-40：60,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ） Firepower 9300 SM-36：60,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ） Firepower 9300 SM-24：55,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ）	
キャリア	無効	オプション ライセンス：通信事業者
合計 TLS プロキシ セッション	15,000	
VPN ライセンス		
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *20,000*
その他の VPN ピア	20,000	
合計 VPN ピア。全タイプの合計	20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプション ライセンス：最大 *250*、*10* 単位
クラスタ	イネーブル	
VLAN、最大	1024	

スマート ソフトウェア ライセンシングのモニタリング

デバッグ メッセージをイネーブルにするだけでなく、ライセンスの機能、ステータス、および証明書をモニターすることもできます。

現在のライセンスの表示

ライセンスを表示するには、次の 画面を参照してください。

- [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ペインで、[Effective Running Licenses] 領域を表示します。

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- ：**[Monitoring] > [Properties] > [Smart License]**

  スマート ソフトウェア ライセンシング、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、資格ステータス、使用許可証明書情報および予定のスマート エージェント タスクを表示します。

UDI の表示

ユニバーサル製品識別子（UDI）を表示するには、次のコマンドを参照してください。

show license udi

次に、ASAv の UDI の例を示します。

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Smart Software Manager 通信

このセクションでは、デバイスが Smart Software Manager と通信する方法について説明します。

デバイス登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各デバイスを導入するとき、または既存のデバイスを登録するときにこのトー

クン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

（注） Firepower 4100/9300 シャーシ：デバイス登録は、ASA 論理デバイス上ではなく、シャーシで設定されます。

展開後の起動時、または既存のデバイスでこれらのパラメータを手動で設定した後、デバイスは Cisco License Authority に登録されます。デバイスをトークンに登録すると、ライセンス認証局はデバイスとそのライセンス認証局との間での通信を行うために ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

ライセンス認証局との定期通信

デバイスはライセンス認証局と 30 日おきに通信します。Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、すぐに変更されるようにすることができます。または、スケジュールどおりにデバイスが通信するのを待ちます。

必要に応じて、HTTP プロキシを設定できます。

ASAv

ASAv は直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネット アクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間遵守が維持されます。猶予期間終了後は、Licensing Authority に連絡する必要があり、そうしないと ASAv がコンプライアンス違反の状態になります。

Firepower 1000

Firepower 1000 では、直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネット アクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

Firepower 2100

Firepower 2100 では、直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネット アクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

Firepower 4100/9300

Firepower 4100/9300では、少なくとも 90 日おきに、直接接続またはHTTP プロキシを介したインターネットアクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

コンプライアンス逸脱状態

次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 使用超過：デバイスが利用できないライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、デバイスで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反状態では、モデルによってはデバイスが制限されている可能性があります。

- ASAv：ASAv は影響を受けません。
- Firepower 1000：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分な標準ライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。
- Firepower 2100：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分な標準ライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。
- Firepower 4100/9300：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分な標準ライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。

Smart Call Home インフラストラクチャ

デフォルトでは、Smart Call Home のプロファイルは、ライセンス認証局の URL を指定する設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの設定可能な

オプションは、ライセンス機関の宛先アドレスURLのみであることに注意してください。Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

（注） Firepower 4100/9300 シャーシ の場合、ライセンスの Smart Call Home は ASA ではなく Firepower 4100/9300 シャーシ スーパバイザで設定されます。

スマート ソフトウェア ライセンスの Smart Call Home をディセーブルにすることはできません。たとえば、**no service call-home** コマンドを使用して Smart Call Home を無効化しても、スマート ソフトウェア ライセンシングは無効化されません。

他の Smart Call Home の機能は、特に設定しない限り、有効になりません。

スマート ライセンス証明書の管理

ASA は Smart Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。サーバー証明書を発行する階層が変更される場合、サービスの中断を防ぐため、定期的な trustpool バンドルの自動更新が有効になるように、 **[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** > **[Edit Trusted Certificate Pool Policy]** 画面の **[Automatic Import]** 領域を設定します。

スマート ライセンス サーバーから受信したサーバー証明書は、[Extended Key Usage] フィールドに「ServAuth」が含まれていなければなりません。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

スマート ソフトウェア ライセンスの履歴

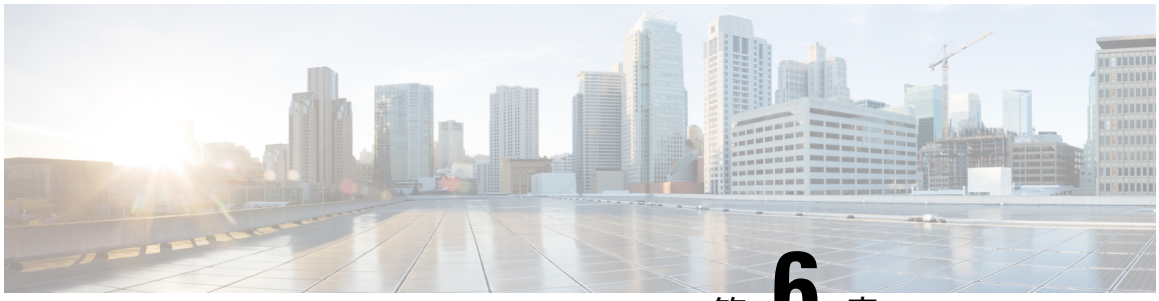
機能名	プラットフォームリリース	説明
ASAv100 永続ライセンス予約	9.14(1.30)	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。**注**：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。

機能名	プラットフォームリリース	説明
ASAv MSLA サポート	9.13(1)	ASAvは、シスコのマネージドサービス ライセンス契約（MSLA）プログラムをサポートしています。このプログラムは、マネージド ソフトウェア サービスをサードパーティに提供するシスコのお客様およびパートナー向けに設計された、ソフトウェアのライセンスおよび消費のフレームワークです。 MSLA はスマートライセンスの新しい形式で、ライセンス スマート エージェントは時間単位でライセンス権限付与の使用状況を追跡します。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]**。
ASAv の柔軟なライセンス	9.13(1)	すべての ASAv ライセンスは、サポートされているすべての ASAv vCPU/メモリ構成で使用できるようになりました。AnyConnect および TLS プロキシのセッション制限は、モデルタイプに関連付けられたプラットフォーム制限ではなく、インストールされた ASAv プラットフォームの権限付与によって決まります。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]**。
Firepower 4100/9300 シャーシのフェールオーバー ペアのライセンスの変更	9.7(1)	アクティブなユニットのみがライセンス権限を要求します。以前は、両方のユニットがライセンスの権限付与を要求していました。FXOS 2.1.1 でサポートされます。
ASAv の短かい文字列の拡張機能向けの永続ライセンス予約	9.6(2)	スマート エージェント（1.6.4 への）の更新により、要求と認証コードには短い文字列が使用されます。 変更された画面はありません。
ASAv のサテライト サーバーのサポート	9.6(2)	デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト サーバーをインストールできます。 変更された画面はありません。

機能名	プラットフォームリリース	説明
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。
ASAv の永続ライセンス予約	9.5(2.200) 9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASAv 用に永続ライセンスを要求できます。 9.6(2) では、Amazon Web サービスの ASAv 向けに、この機能のサポートが追加されました。この機能は Microsoft Azure ではサポートされません。 次のコマンドが導入されました。**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return** ASDM サポートはありません。
スマート エージェントの v1.6 へのアップグレード	9.5(2.200) 9.6(2)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5（2.200）からダウングレードした場合、ASAv はライセンス登録状態を保持しません。[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを指定して再登録する必要があります。Smart Software Manager から ID トークンを取得します。 変更された画面はありません。

機能名	プラットフォームリリース	説明
FirePOWER 9300 の ASA に高度暗号化（3DES）ライセンスを自動的に適用	9.5(2.1)	通常の Cisco Smart Software Manager（SSM）ユーザーの場合、FirePOWER 9300 で登録トークンを適用すると、対象となるお客様には強力な暗号化ライセンスが自動的に有効になります。 （注） スマート ソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、ASA の展開後に ASA CLI を使用して、高度暗号化ライセンスを有効にする必要があります。 この機能には、FXOS 1.1.3 が必要です。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**
サーバー証明書の発行階層が変更された場合の Smart Call Home/スマート ライセンス証明書の検証	9.5(2)	スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを最初に設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA はサーバー証明書の発行階層が変更された場合の証明書の検証をサポートします。トラストプール バンドルの定期的な自動更新を有効にできます。 次の画面が変更されました。**[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Trusted Certificate Pool]** > **[Edit Trusted Certificate Pool Policy]**
新しいキャリア ライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 上の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**
FirePOWER 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	9.4(1.150)	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**

機能名	プラットフォームリリース	説明
ASAv のシスコ スマート ソフトウェア ライセンシング	9.3(2)	Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAK ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンス キーを管理しなくても、簡単に ASAv を導入したり導入を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。 次の画面が導入または変更されました。 **[Configuration] > [Device Management] > [Licensing] > [Smart License] [Configuration] > [Device Management] > [Smart Call-Home] [Monitoring] > [Properties] > [Smart License]**



第 6 章

論理デバイス Firepower 4100/9300

Firepower 4100/9300は柔軟なセキュリティ プラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。この章では、基本的なインターフェイスの設定、および Firepower Chassis Manager を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、Firepower 4100/9300 の ASA クラスタ （511 ページ）を参照してください。FXOS CLI を使用するには、FXOS CLI コンフィギュレーション ガイドを参照してください。高度な FXOS の手順とトラブルシューティングについては、『FXOS 構成ガイド』を参照してください。

Firepower インターフェイスについて

Firepower 4100/9300 シャーシ は、物理インターフェイスおよび EtherChannel（ポート チャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバ インターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で、FXOS シャーシの管理に使用されます。このインターフェイスはMGMTとして、[Interfaces] タブの上部に表示されます。[Interfaces] タブでは、このインターフェイスの有効化または無効化のみを実行できます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLIから設定にする必要があります。このインターフェイスについての情報をFXOS CLIで表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたはSFPモジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

各インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは1つまたは複数の論理デバイス/コンテナインスタンス（FTD-using-FMC 専用）で共有できます。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。ASAの場合：後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス（223ページ）を参照してください。

  （注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Firepower-eventing：FTD-using-FMCデバイスのセカンダリ管理インターフェイスとして使用します。

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。

スタンドアロン展開とクラスタ展開での FTD および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 *10*：インターフェイスタイプのサポート

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	Firepower イベント	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
FTD	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	対応	—	—
	スタンドアロン コンテナ インスタンス	対応	対応	対応	対応	対応	対応	—	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	—
	クラスタ コンテナ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	対応

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	Firepower イベント	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
ASA	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	—	対応	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	—	対応	—

FXOS インターフェイスとアプリケーション インターフェイス

Firepower 4100/9300 は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーション間の連携について説明します。

VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるため、シャーシとアプリケーションの間で不一致が発生することがあります。

論理デバイスについて

論理デバイスでは、1 つのアプリケーション インスタンス（ASA または Firepower Threat Defense のいずれか）および 1 つのオプション デコレータ アプリケーション（Radware DefensePro）を実行し、サービスチェーンを形成できます。

論理デバイスを追加する場合は、アプリケーション インスタンス タイプとバージョンを定義し、インターフェイスを割り当て、アプリケーション設定に送信されるブートストラップ設定を構成することもできます。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および FTD）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3 つすべてのモジュールがネイティブインスタンスとコンテナインスタンスの両方のクラスタに参加する必要があります。

ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

Firepower 9300 の要件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- セキュリティモジュール タイプ：Firepower 9300 に異なるタイプのモジュールをインストールできます。たとえば、SM-36 をモジュール 1、SM-40 をモジュール 2 、SM-44 をモジュール 3 としてインストールできます。
- ネイティブインスタンスとコンテナインスタンス：セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを 1 つのみインストールできます。一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。たとえば、モジュール 1 とモジュール 2 にネイティブインスタンスをインストールできますが、モジュール 3 にはコンテナインスタンスをインストールできます。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2 つの SM-36 を、シャーシ 2 に 3 つの SM-36 をインストールできます。 同じシャーシに 1 つの SM-24 および 2 つの SM-36 をインストールする場合、クラスタリングは使用できません。
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。 ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- ASA および FTD のアプリケーションタイプ：異なるアプリケーション タイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール 1 とモジュール 2 に ASA をインストールし、モジュール 3 に FTD をインストールすることができます。
- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーション インスタンス タイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

Firepower 4100 の要件

Firepower 4100 は複数のモデルに搭載されています。次の要件を参照してください。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100 にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブインスタンスを 1 つのみインストールできます。
- クラスタリング ：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。

- ASA および FTD のアプリケーションタイプ：Firepower 4100 は、1 つのアプリケーションタイプのみを実行できます。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

Firepower インターフェイスに関する注意事項と制約事項

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

一般的なガイドラインと制限事項

ファイアウォール モード

FTDと ASA のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。

ハイ アベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。 データ共有インターフェイスはサポートされていません。

コンテキストモード

- 展開後に、ASA のマルチ コンテキスト モードを有効にします。

ハイアベイラビリティの要件と前提条件

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 個別のシャーシ上にあること。Firepower 9300 のシャーシ内ハイアベイラビリティはサポートされません。
  - 同じモデルであること。
  - 高可用性論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイ アベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシに SM-36、SM-40、および SM-44 を配置できます。SM-36 モジュール間、SM-40 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。
- 他のハイ アベイラビリティ システム要件については、フェールオーバー のシステム要件（326 ページ）を参照してください。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、EtherChannels、、インターフェイス プロパティを編集して。

（注） FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

インターフェイスの有効化または無効化

各インターフェイスの **[Admin State]** を有効または無効に切り替えることができます。デフォルトでは、物理インターフェイスはディセーブルになっています。

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

[インターフェイス（Interface）] ページには、現在インストールされているインターフェイスの視覚的表現がページの上部に表示され、下の表にはインストールされているインターフェイスのリストが示されます。

ステップ 2 インターフェイスを有効にするには、[disabled **無効なスライダ**（  ）] をクリックします。これで、[enabled **有効なスライダ**（  ）] に変わります。

[はい（Yes）] をクリックして、変更を確定します。視覚的に表示された対応するインターフェイスがグレーからグリーンに変化します。

ステップ 3 インターフェイスを無効にするには、有効な **有効なスライダ**（  ） をクリックして、無効な **無効なスライダ**（  ） に変更します。

[はい（Yes）] をクリックして、変更を確定します。視覚的に表示された対応するインターフェイスがグリーンからグレーに変わります。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

[**All Interfaces**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの行で [編集（Edit）] をクリックし、[インターフェイスを編集（Edit Interface）] ダイアログボックスを開きます。

ステップ 3 インターフェイスを有効にするには、[有効化（Enable）] チェックボックスをオンにします。インターフェイスをディセーブルにするには、[Enable] チェックボックスをオフにします。

ステップ 4 インターフェイスの [タイプ（Type）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （224 ページ）を参照してください。

- データ
- 管理
- [クラスタ（Cluster）] : [クラスタ（Cluster）] タイプは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャネル 48 に自動的に作成されます。

ステップ 5 （任意） [速度（Speed）] ドロップダウンリストからインターフェイスの速度を選択します。

ステップ 6 （任意） インターフェイスで [自動ネゴシエーション（Auto Negotiation）] がサポートされている場合は、[はい（Yes）] または [いいえ（No）] オプション ボタンをクリックします。

ステップ 7 （任意） [Duplex] ドロップダウンリストからインターフェイスのデュプレックスを選択します。

ステップ 8 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大16個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45またはSFPのいずれかです。異なるタイプ（銅と光ファイバ）のSFPを混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1GBインターフェイスと10GBインターフェイスなど）を混在させることはできません。リンク集約制御プロトコル（LACP）では、2つのネットワークデバイス間でリンク集約制御プロトコルデータユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データインターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannelは常にオンであり、LACPは使用されません。「オン」のEtherChannelは、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データ インターフェイスのみがアクティブ モードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。 「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止（Suspended）] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータ インターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止（Suspended）] または [ダウン（Down）] 状態に戻ります。

手順

ステップ 1 [Interfaces] を選択して、[Interfaces] ページを開きます。

[**All Interfaces**] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 インターフェイス テーブルの上にある [ポート チャネルの追加（Add Port Channel）] をクリックし、[ポート チャネルの追加（Add Port Channel）] ダイアログボックスを開きます。

ステップ 3 [ポート チャネル ID（Port Channel ID）] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

クラスタ化した論理デバイスを導入すると、ポートチャネル 48 はクラスタ制御リンク用に予約されます。クラスタ制御リンクにポートチャネル 48 を使用しない場合は、ポートチャネル 48 を削除し、別の ID を使用してクラスタタイプの EtherChannel を設定できます。複数のクラスタタイプの EtherChannel を追加し、マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスを追加できます。シャーシ内クラスタリングでは、クラスタ EtherChannel にインターフェイスを割り当てないでください。

ステップ 4 ポート チャネルを有効にするには、[有効化（Enable）] チェックボックスをオンにします。ポート チャネルをディセーブルにするには、**[Enable]**チェックボックスをオフにします。

ステップ 5 インターフェイスの [タイプ（Type）] を選択します。

インターフェイスタイプの使用方法の詳細については、インターフェイス タイプ （224 ページ）を参照してください。

- **データ**
- **管理**
- **クラスタ**

ステップ 6 ドロップダウン リストでメンバーインターフェイスに適した [管理速度（Admin Speed）] を設定します。

指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。

ステップ 7 データインターフェイスに対して、LACP ポート チャネル [Mode]、[Active] または [On] を選択します。

インターフェイスの場合、モードは常にアクティブです。

ステップ 8 メンバーインターフェイスに適した [管理デュプレックス（Admin Duplex）] を設定します（[全二重（Full Duplex）] または [半二重（Half Duplex）]）。

指定したデュプックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。

ステップ 9 ポート チャネルにインターフェイスを追加するには、**[Available Interface]** リストでインターフェイスを選択し、**[Add Interface]** をクリックしてそのインターフェイスを [Member ID] リストに移動します。

同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があり、このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

ヒント 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、Ctrl キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、Shift キーを押しながら最後のインターフェイスをクリックして選択します。

ステップ 10 ポート チャネルからインターフェイスを削除するには、[Member ID] リストでそのインターフェイスの右側にある **[Delete]** ボタンをクリックします。

ステップ 11 **[OK]** をクリックします。

論理デバイスの設定

Firepower 4100/9300 シャーシに、スタンドアロン論理デバイスまたはハイ アベイラビリティ ペアを追加します。

クラスタ リングについては、#unique_283を参照してください。

スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュールクラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

Firepower 4100/9300 シャーシからルーテッドまたはトランスペアレント ファイアウォール モード ASA を展開できます。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。

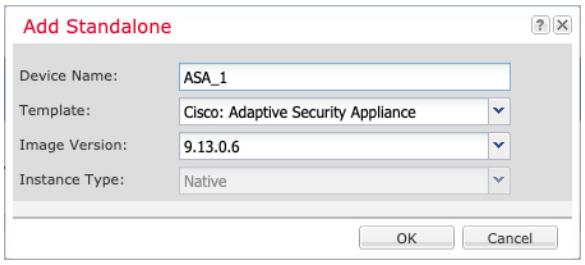
  注 Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および FTD）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（また、[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示されます）。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）] > [スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。
c) [Image Version] を選択します。
d) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [データ ポート（Data Ports）] 領域を展開し、デバイスに割り当てる各ポートをクリックします。

以前に [Interfaces] ページで有効にしたデータインターフェイスのみを割り当てることができます。後で、ASA でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。

a) （Firepower 9300 の場合）[セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。
b) [Management Interface] を選択します。

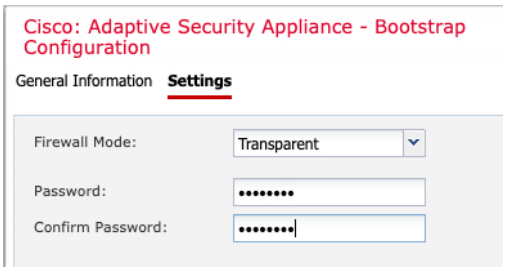
このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。
f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブをクリックします。



ステップ 7 [Firewall Mode] を [Routed] または [Transparent] に指定します。

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

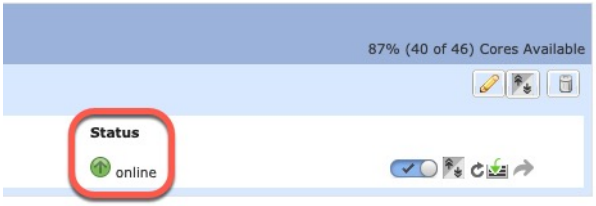
ステップ 8 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザ/パスワードおよびイネーブル パスワードは、パスワードの回復に役立ちます。FXOS アクセスが可能な場合、管理者ユーザ パスワード/イネーブル パスワードを忘れたときにリセットできます。

ステップ 9 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 10 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ステップ 11 セキュリティ ポリシーの設定を開始するには、『ASA 設定ガイド』を参照してください。

ハイ アベイラビリティ ペアの追加

ASA ハイ アベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイ アベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

フェールオーバー のシステム要件 （326 ページ）を参照してください。

手順

ステップ 1 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 2 フェールオーバー リンクとステート リンクに 1 つまたは 2 つのデータ インターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシの間でハイ アベイラビリティ トラフィックをやり取りします。統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。使用可能なインターフェイスがある場合、別のフェールオーバー リンクとステート リンクを使用できます。ステート リンクが帯域幅の大半を必要とします。フェールオーバー リンクまたはステート リンクに管理タイプのインターフェイスを使用することはできません。同じネットワーク セグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

ステップ 3 論理デバイスでハイ アベイラビリテを有効にします。 ハイ アベイラビリティのためのフェールオーバー （325 ページ）を参照してください。

ステップ 4 ハイ アベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

（注） ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、ASA の設定に与える影響は最小限です。ただし、FXOS で割り当てられたインターフェイスを削除する場合（ネットワーク モジュールの削除、EtherChannel の削除、割り当てられたインター

フェイスの EtherChannel への再割り当てなど）、そのインターフェイスがセキュリティポリシーで使用されると、削除は ASA の設定に影響を与えます。この場合、ASA 設定では元のコマンドが保持されるため、必要な調整を行うことができます。ASA OS の古いインターフェイス設定は手動で削除できます。

（注） 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。

始める前に

- 物理インターフェイスの設定 （231 ページ）および EtherChannel（ポート チャネル）の追加 （232 ページ）に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトですべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でデバイスに EtherChannel を割り当てることができます。
- 管理インターフェイスを管理 EtherChannel に置き換えるには、未割り当てのデータ メンバー インターフェイスが少なくとも 1 つある EtherChannel を作成し、現在の管理インターフェイスをその EtherChannel に置き換える必要があります。ASA がリロードし（管理インターフェイスを変更するとリロードします）、（現在未割り当ての）管理インターフェイスも EtherChannel に追加できます。
- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にデータ/スタンバイユニットでインターフェイスを変更してから、制御/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイス モニタリングに影響を及ぼしません。

手順

ステップ 1 Firepower Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 右上にある [編集（Edit）] アイコンをクリックして、その論理デバイスを編集します。

ステップ 3 データ インターフェイスの割り当てを解除するには、[データ ポート（Data Ports）] 領域でそのインターフェイスの選択を解除します。

ステップ 4 [データ ポート（Data Ports）] 領域で新しいデータ インターフェイスを選択して、そのインターフェイスを割り当てます。

ステップ 5 次のように、管理インターフェイスを置き換えます。

このタイプのインターフェイスでは、変更を保存するとデバイスがリロードします。

a) ページ中央のデバイス アイコンをクリックします。

b) [一般/クラスタ情報（General/Cluster Information）] タブで、ドロップダウン リストから新しい [管理インターフェイス（Management Interface）] を選択します。
c) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

アプリケーションのコンソールへの接続

アプリケーションのコンソールに接続するには、次の手順を使用します。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect asa *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA：**Ctrl-a, d** と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

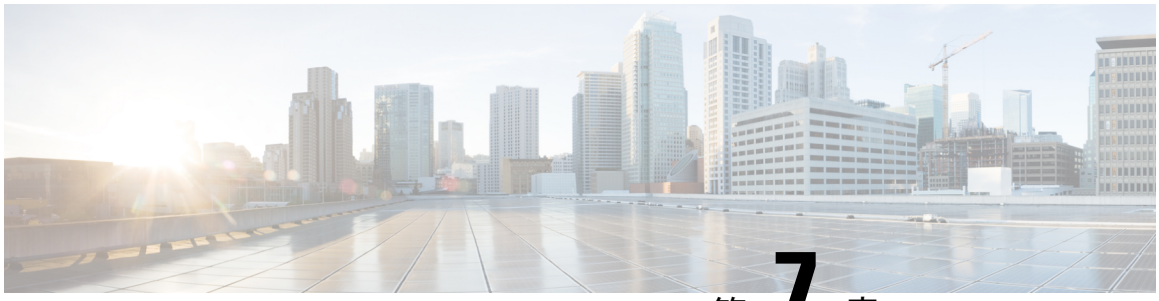
論理デバイスの履歴

機能	バージョン	詳細
Firepower 4112 用の ASA	9.14(1)	Firepower 4112 を導入しました。 （注） FXOS 2.8.1 が必要です。
Firepower 9300 SM-56 のサポート	9.12.2	SM-56 セキュリティ モジュールが導入されました。 （注） FXOS 2.6.1.157 が必要です。

機能	バージョン	詳細
Firepower 4115、4125、および 4145 向け ASA	9.12(1)	Firepower 4115、4125、および 4145 が導入されました。 （注） FXOS 2.6.1 が必要です。
Firepower 9300 SM-40 および SM-48 のサポート	9.12.1	セキュリティ モジュールの SM-40 と SM-48 が導入されました。 （注） FXOS 2.6.1 が必要です。
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	9.12.1	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	9.10.1	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 （注） FXOS 2.4.1 が必要です。 新規/変更された [Firepower Chassis Manager] 画面： **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** > **[クラスタ情報（Cluster Information）]** > [CCL Subnet IP] フィールド

機能	バージョン	詳細
オン モードでのデータ EtherChannel のサポート	9.10.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオンモードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 （注） FXOS 2.4.1 が必要です。 新規/変更された [Firepower Chassis Manager] 画面： **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [ポート チャネルの編集（Edit Port Channel）] > [モード（Mode）]**
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次の画面が変更されました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]**
Firepower 4100 シリーズ のサポート	9.6(1)	FXOS 1.1.4 では、ASA クラスタリングは、Firepower 4100 シリーズ のシャーシ間クラスタリングをサポートします。 変更された画面はありません。

機能	バージョン	詳細
6 つのモジュールのシャーシ間クラスタリング、および FirePOWER 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 変更された画面はありません。
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4（1.150）	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次の画面を導入しました。 **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]**



第 7 章

トランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード

この章では、ファイアウォール モードをルーテッドまたはトランスペアレントに設定する方法と、各ファイアウォール モードでファイアウォールがどのように機能するかについて説明します。

マルチコンテキスト モードでは、コンテキストごとに別個にファイアウォール モードを設定できます。

ファイアウォール モードについて

Secure Firewall ASA は、でルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの 2 つのファイアウォール モードをサポートします。

ルーテッド ファイアウォール モードについて

ルーテッドモードでは、Secure Firewall ASA はネットワーク内のルータホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。コンテキスト間でレイヤ 3 インターフェイスを共有することもできます。

統合ルーティングおよびブリッジングにより、ネットワーク上の複数のインターフェイスをまとめた「ブリッジグループ」を使用できます。そして、Secure Firewall ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループ

には、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。Secure Firewall ASA は BVI と通常のルーテッドインターフェイス間でルーティングを行います。マルチコンテキストモード、クラスタリング、EtherChannel、または Visual Networking Index（VNI）メンバーインターフェイスが必要ない場合は、トランスペアレントモードではなくルーテッドモードの使用を検討してください。ルーテッドモードでは、トランスペアレントモードと同様に 1 つ以上の分離されたブリッジグループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッドインターフェイスも含めることができます。

トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

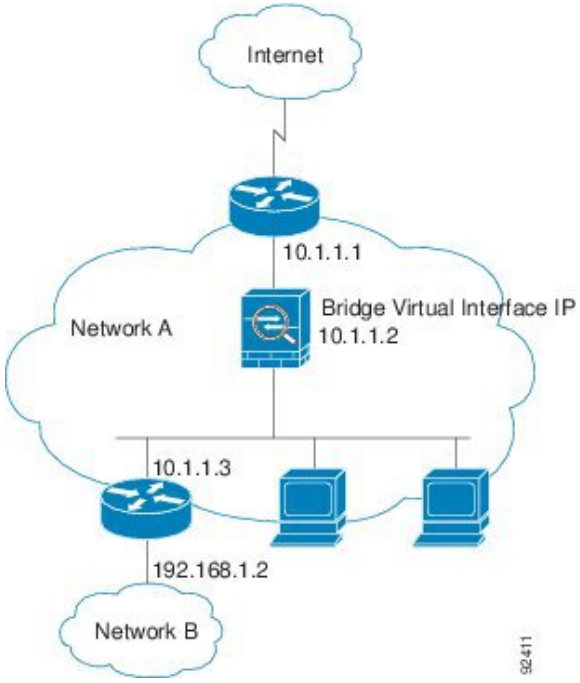
レイヤ2の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して確立されます。また、Secure Firewall ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

ネットワークでのトランスペアレント ファイアウォールの使用

Secure Firewall ASA は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレントファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータと各ホストは、外部ルータに直接接続されているように見えます。

図 *25 :* トランスペアレント ファイアウォール ネットワーク



Management [インターフェイス（Interface）]

各ブリッジ仮想インターフェイス（BVI）IPアドレスのほかに、別のManagementスロット/ポート インターフェイスを追加できます。このインターフェイスはどのブリッジ グループにも属さず、Secure Firewall ASA への管理トラフィックのみを許可します。詳細については、管理インターフェイス （610 ページ）を参照してください。

ルーテッド モード機能のためのトラフィックの通過

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセス ルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV で作成されるようなマルチキャスト トラフィックを許可したりできます。また、トランスペアレント ファイアウォールを通過するルーティング プロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセス ルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは Secure Firewall ASA を通過できます。

ブリッジグループについて

ブリッジ グループは、Secure Firewall ASA がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。他のファイアウォール イン

ターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のチェックがすべて実施されます。

ブリッジ仮想インターフェイス（BVI）

各ブリッジグループには、ブリッジ仮想インターフェイス（BVI）が含まれます。Secure Firewall ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスはブリッジグループ メンバー インターフェイスと同じサブネット上になければなりません。BVI では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

トランスペアレントモード：インターフェイスベースの各機能はブリッジグループのメンバーインターフェイスだけを指定でき、これらについてのみ使用できます。

ルーテッド モード：BVI はブリッジグループと他のルーテッド インターフェイス間のゲートウェイとして機能します。ブリッジグループ/ルーテッド インターフェイス間でルーティングするには、BVI を指定する必要があります。一部のインターフェイスベース機能に代わり、BVI 自体が利用できます。

- アクセス ルール：ブリッジグループのメンバー インターフェイスと BVI 両方のアクセス ルールを設定できます。インバウンドのルールでは、メンバーインターフェイスが先にチェックされます。アウトバウンドのルールでは BVI が最初にチェックされます。
- DHCPv4 サーバ：BVI のみが DHCPv4 サーバの構成をサポートします。
- スタティック ルート：BVI のスタティック ルートを設定できます。メンバーインターフェイスのスタティック ルートは設定できません。
- Syslog サーバーと Secure Firewall ASA 由来の他のトラフィック：syslog サーバー（または SNMP サーバー、Secure Firewall ASA からトラフィックが送信される他のサービス）を指定する際、BVI またはメンバー インターフェイスのいずれかも指定できます。

ルーテッド モードで BVI を指定しない場合、Secure Firewall ASA はブリッジ グループのトラフィックをルーティングしません。この設定は、ブリッジグループのトランスペアレント ファイアウォール モードを複製します。マルチコンテキストモード、クラスタリング、または EtherChannel または VNI メンバーインターフェイスが不要であれば、ルーテッドモードの使用を検討すべきです。ルーテッド モードでは、トランスペアレント モードと同様に 1 つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

トランスペアレント ファイアウォール モードのブリッジグループ

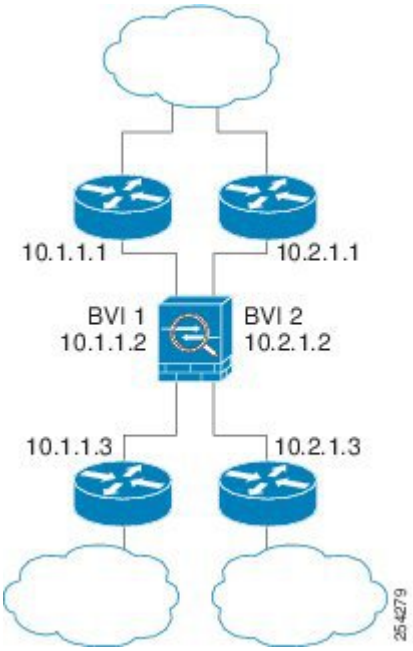
ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは Secure Firewall ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから Secure Firewall ASA 内の他のブリッジ グループにルーティングされる前に、Secure Firewall ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバーまたは AAA サーバーの設定は、すべてのブリッジ グループで共有さ

れます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に1つのブリッジグループにして、セキュリティ コンテキストを使用します。

1 つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、ファイアウォール モードのガイドライン（256ページ）を参照してください。ブリッジグループごとに2つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが3つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2 つのブリッジ グループを持つ、Secure Firewall ASA に接続されている 2 つのネットワークを示します。

図 *26 : 2* つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク



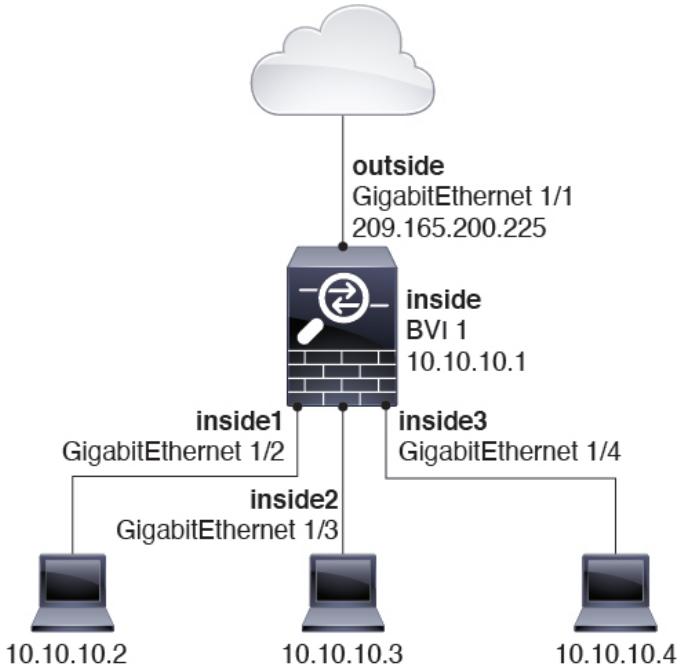
ルーテッド ファイアウォール モードのブリッジグループ

ブリッジグループ トラフィックは他のブリッジ グループまたはルーテッド インターフェイスにルーティングできます。ブリッジグループのBVIインターフェイスに名前を割り当てないことで、ブリッジグループのトラフィックを分離することもできます。BVIに名前を付けると、その BVI はその他の通常のインターフェイスと同様にルーティングに参加します。

ルーテッド モードでブリッジ グループを使用する方法として、外部スイッチの代わりに ASA 追加のインターフェイスを使用する方法があります。たとえば、デバイスの中には、通常のインターフェイスとして外部インターフェイスを持ち、その他すべてのインターフェイスが内部ブリッジグループに割り当てられているというデフォルト設定のものがあります。このブリッジグループは外部スイッチを置き換えることを目的としているので、すべてのブリッジグルー

プインターフェイスが自由に通信できるようにアクセス ポリシーを設定する必要があります。たとえば、デフォルト設定と同様に、すべてのインターフェイスを同じセキュリティ レベルに設定し、同じセキュリティ レベルのインターフェイス間の通信を有効にします。この通信ではアクセス ルールは不要です。

図 *27*:内部ブリッジグループと外部ルーテッド インターフェイスからなるルーテッド ファイアウオール ネットワーク



ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、アクセス ルールで許可しても、いくつかのタイプのトラフィックは Secure Firewall ASA を通過できません。ただし、ブリッジグループは、アクセス ルール（IP トラフィックの場合）または EtherType ルール（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

- IP トラフィック：ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。ブリッジ グループ内では、このトラフィックをアクセス ルールで許可できます。
- 非 IP トラフィック：AppleTalk、IPX、BPDU や MPLS などは、EtherType ルールを使用することで、通過するように設定できます。

（注） ブリッジ グループは、CDP パケットおよび 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。サポートされる例外は、BPDU および IS-IS です。

レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスに移動する場合、アクセス ルールなしで自動的にブリッジグループを通過できます。
- セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに移動するレイヤ 3 トラフィックの場合、セキュリティの低いインターフェイスでアクセル ルールが必要です。
- ARP は、アクセス ルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセス ルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャスト トラフィックは、アクセス ルールを使用して通過させることができます。

許可される MAC アドレス

アクセス ポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます（レイヤ 3 トラフィックの許可 （251 ページ）を参照）。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

BPDU 処理

スパニングツリープロトコルを使用するときのループを防止するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、BPDU を拒否するように EtherType ルールを設定する必要があります。外部スイッチで BPDU をブロックすることもできます。たとえば、同じブリッジグループのメンバーが異なる VLAN のスイッチポートに接続されている場合、スイッチで BPDU をブロックできます。この場合、一方の VLAN からの BPDU がもう一方の VLAN で認識されるため、スパニング ツリー ルート ブリッジの選定プロセスで問題が発生する可能性があります。

フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチ ポートがブロッキング ステートに移行することを回避できます。詳細については、フェールオーバーのブリッジ グループ要件 （338 ページ）を参照してください。

MAC アドレスとルート ルックアップ

ブリッジ グループ内のトラフィックでは、パケットの発信インターフェイスは、ルート ルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

- トラフィックの発信元が Secure Firewall ASA：syslog サーバーなどがあるリモート ネットワーク宛てのトラフィック用に、Secure Firewall ASA にデフォルト/スタティック ルートを追加します。
- インスペクションが有効になっている Voice over IP（VoIP）および TFTP トラフィック、エンドポイントが 1 ホップ以上離れている：セカンダリ接続が成功するように、リモート エンドポイント宛てのトラフィック用に、Secure Firewall ASA にスタティック ルートを追加します。Secure Firewall ASA は、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、Secure Firewall ASA は正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

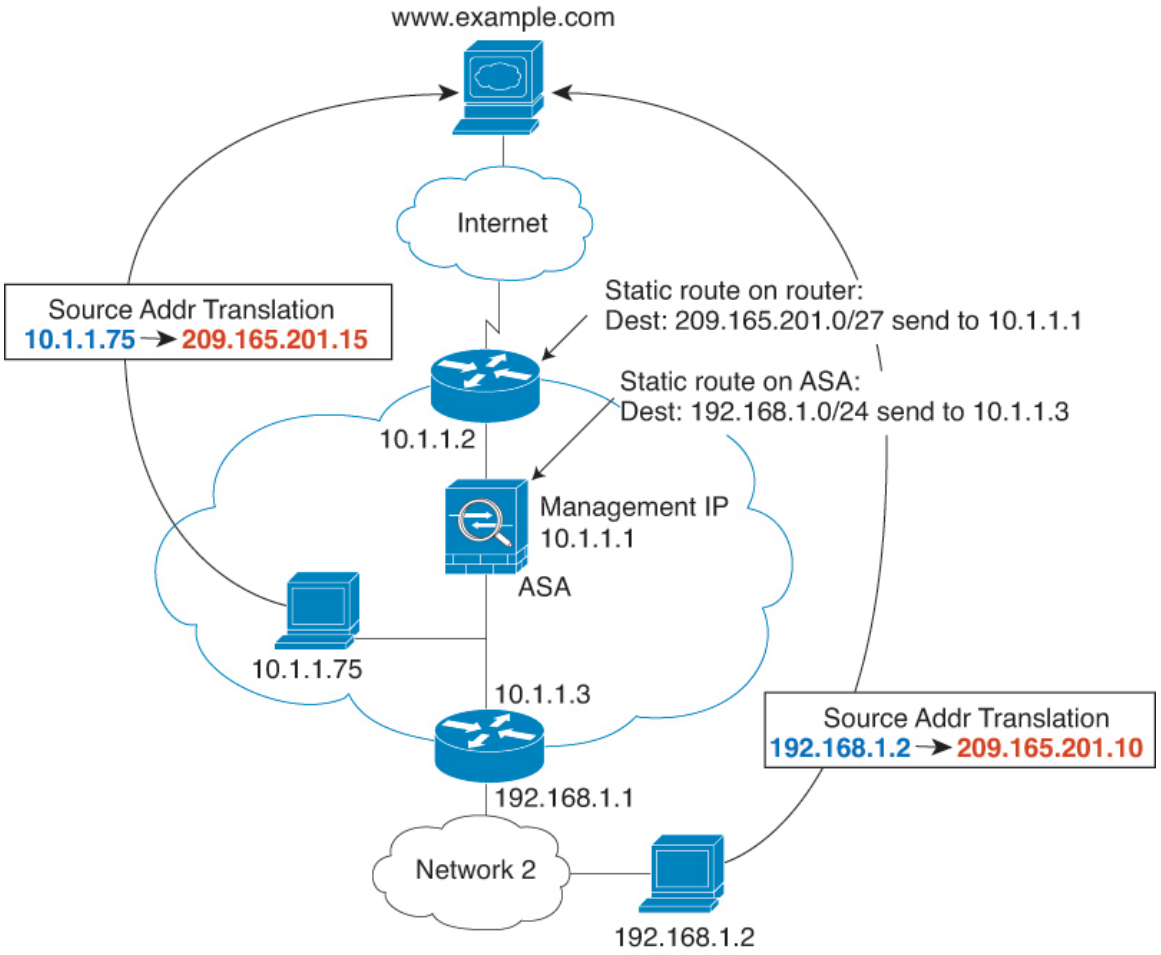
  影響を受けるアプリケーションは次のとおりです。

  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny（SCCP）
  - SQL*Net
  - SunRPC
  - TFTP

- Secure Firewall ASA が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛てのトラフィック用に、Secure Firewall ASA にスタティック ルートを設定します。また、Secure Firewall ASA に送信されるマッピング アドレス宛てのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

  このルーティング要件は、インスペクションと NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。Secure Firewall ASA は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 *28 : NAT* の例：ブリッジ グループ内の *NAT*



トランスペアレント モードのブリッジ グループのサポートされていない機能

次の表に、トランスペアレント モードのブリッジ グループでサポートされない機能を示します。

表 *11 :* トランスペアレント モードでサポートされない機能

機能	説明
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	ブリッジグループ メンバー インターフェイスでは、DHCPv4 サーバのみがサポートされます。

機能	説明
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバーとして機能することができますが、DHCP リレーはサポートしません。2 つのアクセス ルール（1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバーからの応答を逆方向に許可します。）を使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループ メンバー インターフェイスの場合、Secure Firewall ASA で発信されたトラフィックにスタティック ルートを追加できます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが Secure Firewall ASA を通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが Secure Firewall ASA を通過できるようにすることができます。
QoS	-
通過トラフィック用の VPN 終端	トランスペアレント ファイアウォールは、ブリッジ グループ メンバー インターフェイスでのみ、管理接続用のサイト間 VPN トンネルをサポートします。これは、Secure Firewall ASA を通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。
Unified Communications	—

ルーテッド モードのブリッジ グループのサポートされていない機能

次の表に、ルーテッド モードのブリッジ グループでサポートされない機能を示します。

表 *12* : ルーテッド モードでサポートされない機能

機能	説明
EtherChannel または VNI メンバー インターフェイス	物理インターフェイス、冗長インターフェイス、およびサブインターフェイスのみがブリッジ グループ メンバー インターフェイスとしてサポートされます。 Management インターフェイスもサポートされていません。
クラスタリング	ブリッジ グループはクラスタリングでサポートされません。
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	DHCPv4 サーバーのみが BVI でサポートされます。
DHCP リレー	ルーテッド ファイアウォールは DHCPv4 サーバーとして機能することができますが、DHCP リレーを BVI またはブリッジ グループ メンバー インターフェイスでサポートしません。
ダイナミック ルーティング プロトコル	ただし、BVI のスタティック ルートを追加することはできます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが Secure Firewall ASA を通過できるようにすることもできます。非ブリッジ グループ インターフェイスはダイナミック ルーティングをサポートします。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが Secure Firewall ASA を通過できるようにすることができます。非ブリッジ グループ インターフェイスはマルチキャスト ルーティングをサポートします。
マルチ コンテキスト モード	ブリッジ グループは、マルチ コンテキスト モードではサポートされません。
QoS	非ブリッジ グループ インターフェイスは、QoS をサポートします。

機能	説明
通過トラフィック用の VPN 終端	VPN 接続を BVI で終端することはできません。非ブリッジ グループ インターフェイスは、VPN をサポートします。 ブリッジグループ メンバーインターフェイスは、管理接続専用のサイト間 VPN トンネルをサポートします。これは、Secure Firewall ASA を通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックにブリッジグループを通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。
Unified Communications	非ブリッジ グループ インターフェイスは、Unified Communications をサポートします。

デフォルト設定

デフォルト モード（Default Mode）

デフォルト モードはルーテッド モードです。

ブリッジ グループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジ グループ内で渡されます。

ファイアウォール モードのガイドライン

コンテキスト モードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

ブリッジグループのガイドライン（トランスペアレントおよびルーテッドモード）

- 64 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Secure Firewall ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

- デバイスとデバイス間の管理トラフィック、および Secure Firewall ASA を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- ASAv50 の場合、ブリッジグループは透過的モードまたはルーテッドモードのいずれでもサポートされません。
- FirePOWER 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower 1010 では、同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Secure Firewall ASA の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1 つのブリッジグループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジグループのインターフェイスとブリッジグループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジグループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。
- トランスペアレント モードでは、PPPoE は Management インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、ASA 定義の EtherChannel および VNI インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

その他のガイドラインと制限事項

- ファイアウォールモードを変更すると、多くのコマンドが両方のモードでサポートされていないため、ASA は実行コンフィギュレーションをクリアします。スタートアップ コンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップ コンフィギュレーションがロードされて、モードは元の設定に戻ります。 コンフィギュレーション ファイルのバックアップについては、ファイアウォールモード（シングルモード）の設定 （258 ページ）を参照してください。
- **firewall transparent** コマンドでモードを使用して変更するテキスト コンフィギュレーションを ASA にダウンロードする場合、コマンドをコンフィギュレーションの先頭に配置してください。このコマンドが読み込まれるとすぐに ASA がモードを変更し、その後ダウンロードされたコンフィギュレーションを引き続き読み込みます。コマンドがコンフィギュレーションの後ろの方にあると、ASA はそのコマンドよりも前の位置に記述されているすべての行をクリアします。

ファイアウォール モード（シングル モード）の設定

この項では、CLI を使用してファイアウォール モードを変更する方法を説明します。 シングルモードの場合およびマルチモードで現在接続されているコンテキスト（通常は管理コンテキスト）の場合は、ASDM でモードを変更できません。他のマルチ モードのコンテキストでは、コンテキストごとに ASDM でモードを設定できます。セキュリティ コンテキストの設定 （308 ページ）を参照してください。

（注） ファイアウォール モードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォール モードを設定することをお勧めします。

始める前に

モードを変更すると、ASA は実行コンフィギュレーションをクリアします（詳細については、ファイアウォール モードのガイドライン （256 ページ）を参照してください）。

- 設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。このバックアップは、新しいコンフィギュレーション作成時の参照として使用できます。
- モードを変更するには、コンソール ポートで CLI を使用します。ASDM コマンドライン インターフェイス ツールや SSH などの他のタイプのセッションを使用する場合、コンフィギュレーションがクリアされるときにそれが切断されるので、いずれの場合もコンソール ポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。

（注） 設定が削除された後にファイアウォール モードをトランスペアレントに設定し、ASDM への管理アクセスを設定するには、ASDM アクセスの設定 （25 ページ）を参照してください。

手順

ファイアウォール モードをトランスペアレントに設定します。

firewall transparent

例：

```
ciscoasa(config)# firewall transparent
```

モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

（注） ファイアウォールモードの変更では確認は求められず、ただちに変更が行われます。

ファイアウォール モードの例

このセクションには、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードで、Secure Firewall ASA を介してどのようにトラフィックが転送されるかを説明する例が含まれます。

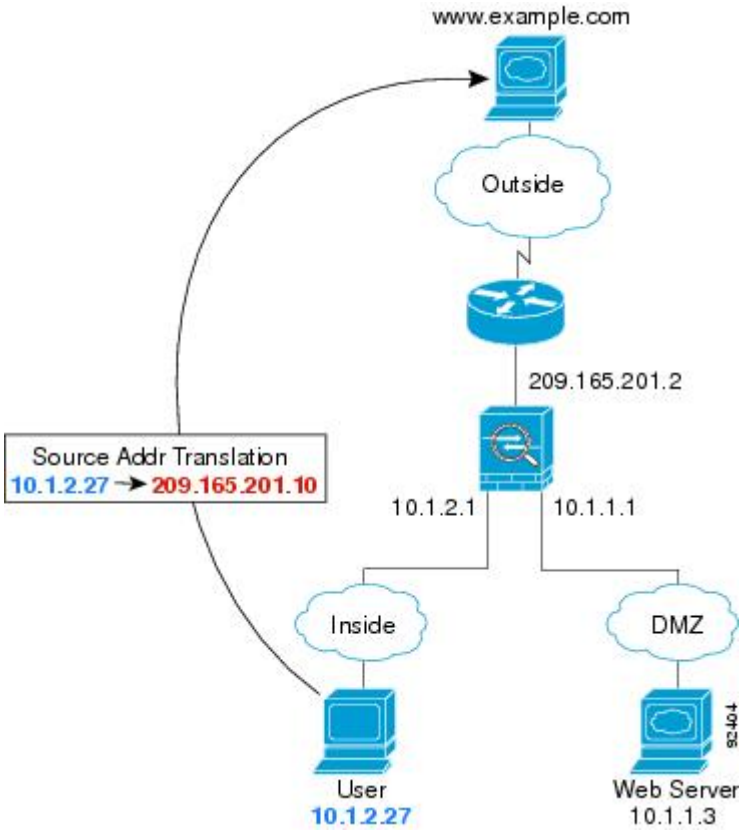
ルーテッド ファイアウォール モードで Secure Firewall ASA を通過するデータ

次のセクションでは、複数のシナリオのルーテッド ファイアウォール モードで、データが Secure Firewall ASA をどのように通過するかを示します。

内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバーにアクセスしていることを示しています。

図 *29 :* 内部から外部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザーは、www.example.com から Web ページを要求します。
2. Secure Firewall ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシーの条件に従って、パケットが許可されているか確認します。

   マルチ コンテキスト モードの場合、Secure Firewall ASA はパケットをまずコンテキストに分類します。
3. Secure Firewall ASA は、実アドレス（10.1.2.27）をマップ アドレス 209.165.201.10 に変換します。このマップ アドレスは外部インターフェイスのサブネット上にあります。

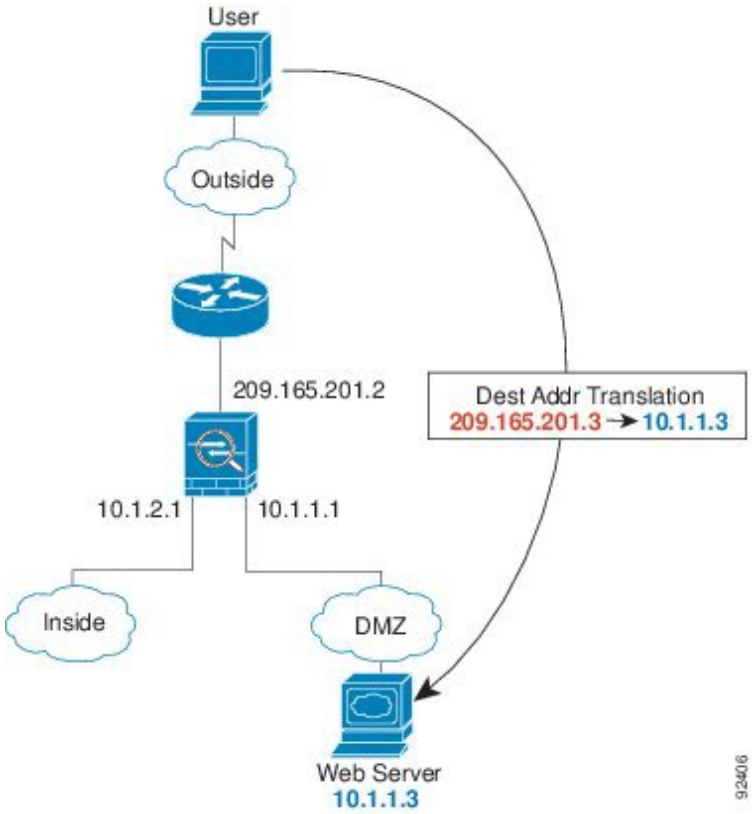
   マップ アドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. 次に、Secure Firewall ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、パケットはSecure Firewall ASAを通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。Secure Firewall ASA は、グローバル宛先アドレスをローカル ユーザー アドレス 10.1.2.27 に変換せずに、NAT を実行します。

6. Secure Firewall ASAは、パケットを内部ユーザーに転送します。

外部ユーザーが DMZ 上の Web サーバーにアクセスする

次の図は、外部ユーザーが DMZ の Web サーバーにアクセスしていることを示しています。

図 *30 :* 外部から *DMZ* へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーがマップ アドレス 209.165.201.3 を使用して、DMZ 上の Web サーバーに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
2. Secure Firewall ASA はパケットを受信し、マッピング アドレスは実アドレス 10.1.1.3 に変換しません。
3. Secure Firewall ASA は新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

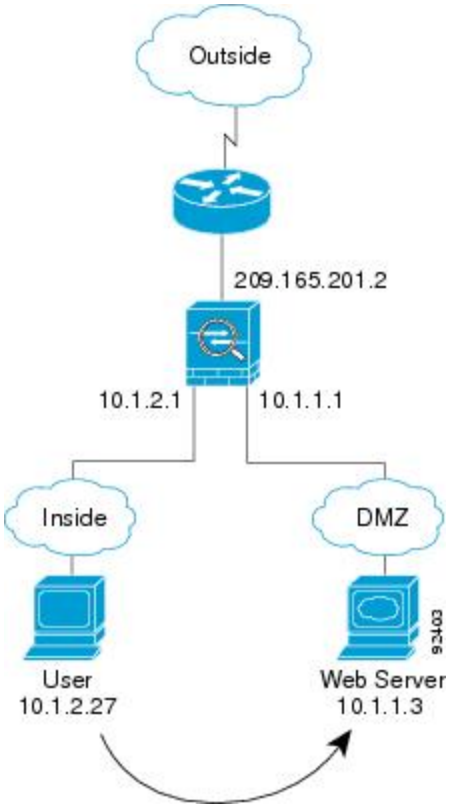
   マルチ コンテキスト モードの場合、Secure Firewall ASA はパケットをまずコンテキストに分類します。
4. 次に、Secure Firewall ASAはセッション エントリを高速パスに追加し、DMZ インターフェイスからパケットを転送します。

5. DMZ Web サーバーが要求に応答すると、パケットはSecure Firewall ASAを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。Secure Firewall ASA は、実アドレスを 209.165.201.3 に変換することで NAT を実行します。
6. Secure Firewall ASAは、パケットを外部ユーザーに転送します。

内部ユーザーが DMZ 上の Web サーバーにアクセスする

次の図は、内部ユーザーが DMZ の Web サーバーにアクセスしていることを示しています。

図 *31* : 内部から *DMZ* へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 内部ネットワーク上のユーザーは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバーから Web ページを要求します。
2. Secure Firewall ASA はパケットを受信します。これは新しいセッションであるため、Secure Firewall ASA はセキュリティ ポリシーの条件に従ってパケットが許可されているか確認します。

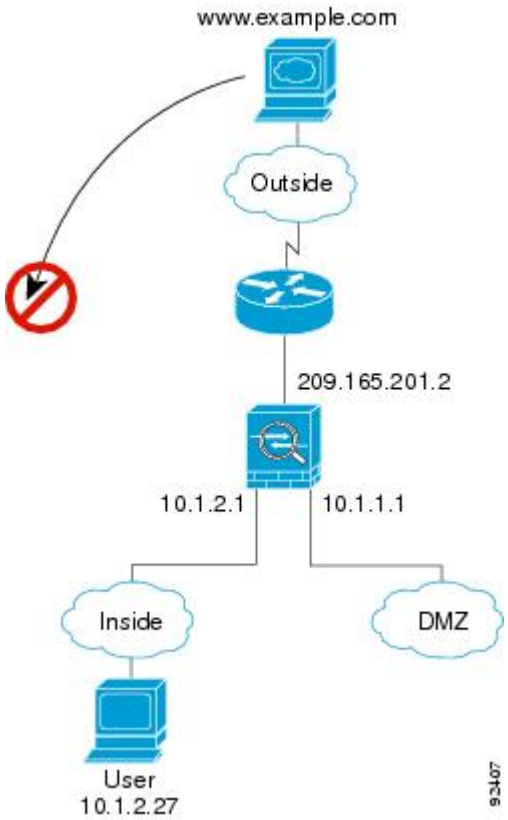
   マルチ コンテキスト モードの場合、Secure Firewall ASA はパケットをまずコンテキストに分類します。

3. 次に、Secure Firewall ASAはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。
4. DMZ Web サーバーが要求に応答すると、パケットは高速パスを通過します。これのため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. Secure Firewall ASAは、パケットを内部ユーザーに転送します。

外部ユーザーが内部ホストにアクセスしようとする

次の図は、外部ユーザーが内部ネットワークにアクセスしようとしていることを示しています。

図 *32 :* 外部から内部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーが、内部ホストに到達しようとします（ホストにルーティング可能な IP アドレスがあると想定します）。

   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザーが NAT なしで内部ネットワークに到達することはできません。外部ユーザーは既存の NAT セッションを使用して内部ユーザーに到達しようとすることが考えられます。

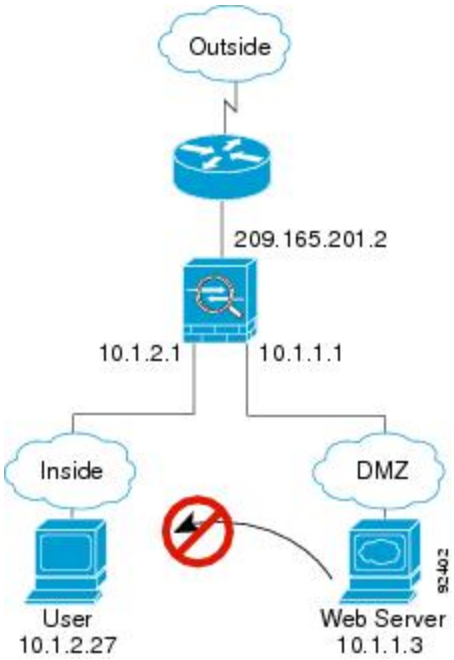
2. Secure Firewall ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、Secure Firewall ASAはパケットをドロップし、接続試行をログに記録します。

   外部ユーザーが内部ネットワークを攻撃しようとした場合、Secure Firewall ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザーによる内部ホストへのアクセスの試み

次の図は、DMZ 内のユーザーが内部ネットワークにアクセスしようとしていることを示しています。

図 *33 : DMZ* から内部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

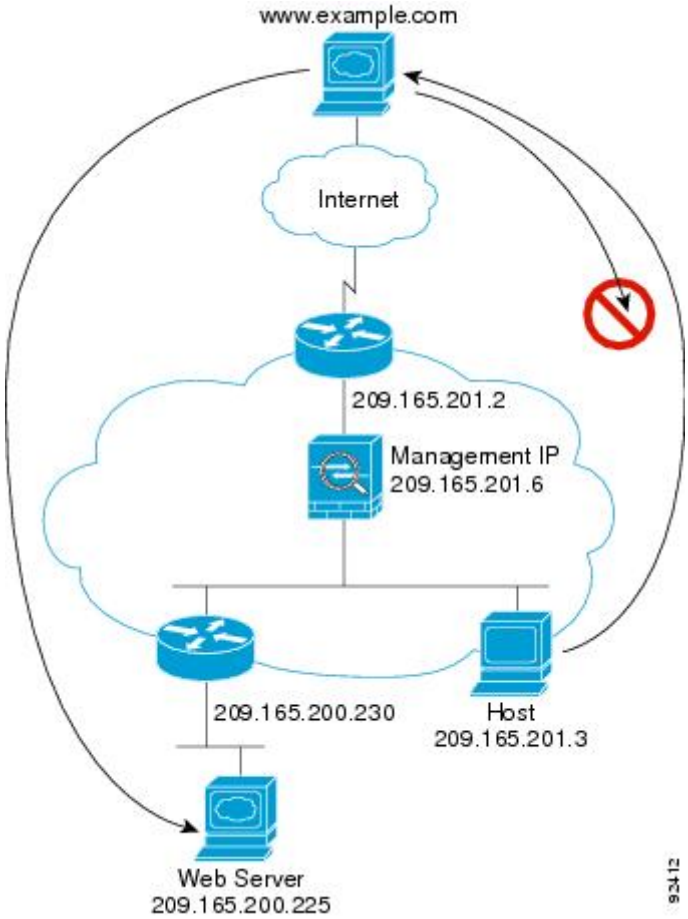
1. DMZ ネットワーク上のユーザーが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. Secure Firewall ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシーに従って、パケットが許可されているか確認します。

   パケットが拒否され、Secure Firewall ASAはパケットをドロップし、接続試行をログに記録します。

トランスペアレント ファイアウォールを通過するデータの動き

次の図に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザーがインターネット リソースにアクセスできるよう、Secure Firewall ASA にはアクセス ルールがあります。別のアクセス ルールによって、外部ユーザーは内部ネットワーク上の Web サーバーだけにアクセスできます。

図 *34 :* 一般的なトランスペアレント ファイアウォールのデータ パス

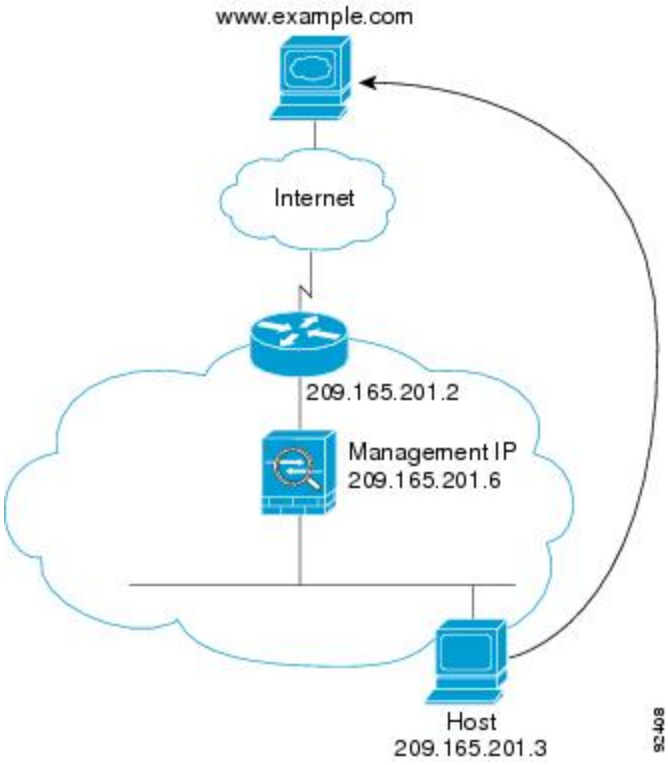


次のセクションでは、データが Secure Firewall ASA をどのように通過するかを示します。

内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバーにアクセスしていることを示しています。

図 *35 :* 内部から外部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザーは、www.example.com から Web ページを要求します。
2. Secure Firewall ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレステーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。

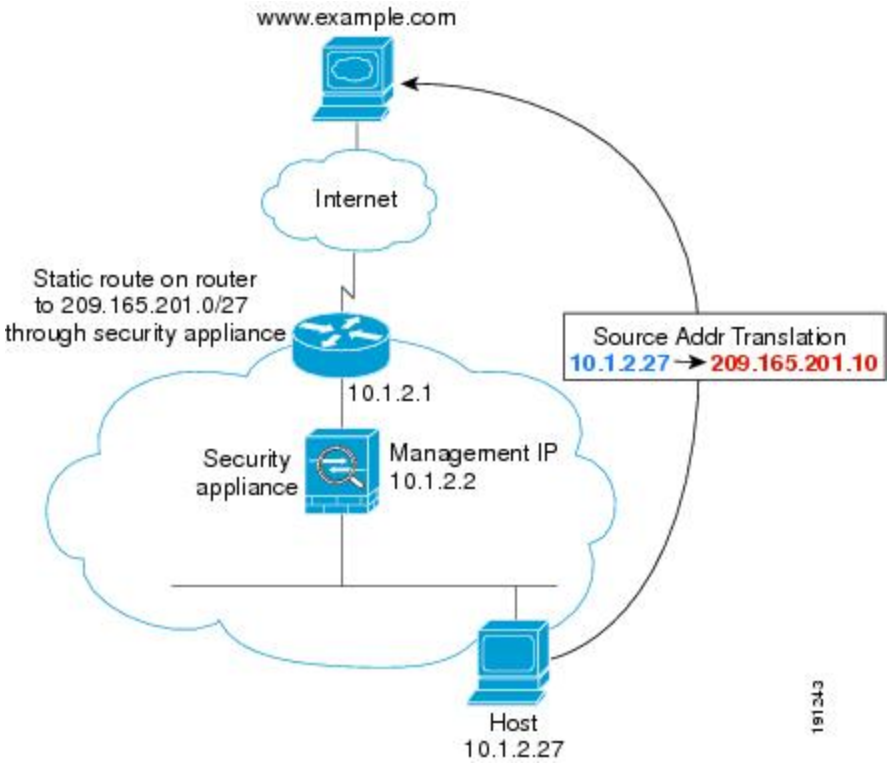
   マルチ コンテキスト モードの場合、Secure Firewall ASA はパケットをまずコンテキストに分類します。
3. Secure Firewall ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、Secure Firewall ASAは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

   宛先 MAC アドレスが Secure Firewall ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。
5. Web サーバーが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. Secure Firewall ASAは、パケットを内部ユーザーに転送します。

NAT を使用して内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバーにアクセスしていることを示しています。

図 *36 : NAT* を使用して内部から外部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザーは、www.example.com から Web ページを要求します。
2. Secure Firewall ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレステーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、Secure Firewall ASAは、固有なインターフェイスに従ってパケットを分類します。
3. Secure Firewall ASAは実際のアドレス（10.1.2.27）をマッピング アドレス 209.165.201.10 に変換します。

   マッピング アドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータにSecure Firewall ASAをポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、Secure Firewall ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。

5. 宛先 MAC アドレスがテーブル内にある場合、Secure Firewall ASAは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 10.1.2.1 です。

   宛先 MAC アドレスが Secure Firewall ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

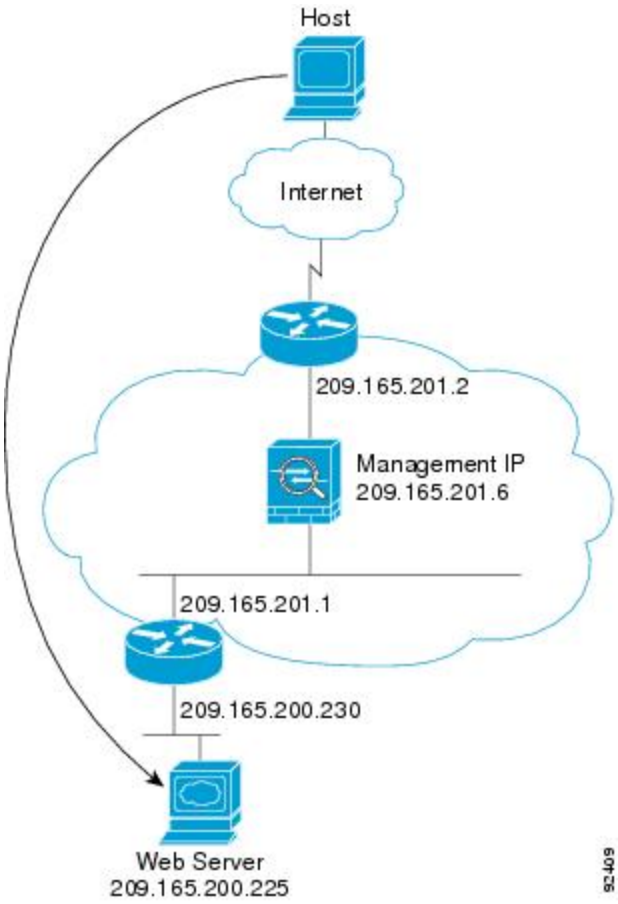
6. Web サーバーが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。

7. Secure Firewall ASA は、マッピング アドレスを実際のアドレス 10.1.2.27 にせずに、NAT を実行します。

外部ユーザーが内部ネットワーク上の Web サーバーにアクセスする

次の図は、外部ユーザーが内部の Web サーバーにアクセスしていることを示しています。

図 *37*: 外部から内部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーは、内部 Web サーバーから Web ページを要求します。

2. Secure Firewall ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレステーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、Secure Firewall ASA はパケットをまずコンテキストに分類します。

3. Secure Firewall ASAは、セッションが確立されたことを記録します。

4. 宛先MACアドレスがテーブル内にある場合、Secure Firewall ASAは内部インターフェイスからパケットを転送します。宛先MACアドレスは、ダウンストリームルータ209.165.201.1のアドレスです。

   宛先 MAC アドレスが Secure Firewall ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

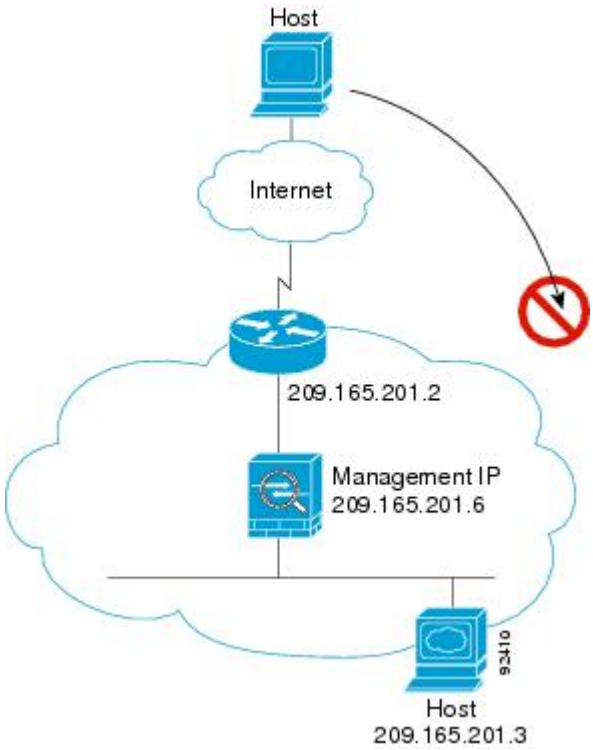
5. Web サーバーが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。

6. Secure Firewall ASAは、パケットを外部ユーザーに転送します。

外部ユーザーが内部ホストにアクセスしようとする

次の図は、外部ユーザーが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 *38* : 外部から内部へ



次の手順では、データが Secure Firewall ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーが、内部ホストに到達しようとします。
2. Secure Firewall ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレステーブルに追加します。これは新しいセッションであるため、セキュリティポリシーの条件に従って、パケットが許可されているか確認します。

   マルチ コンテキスト モードの場合、Secure Firewall ASA はパケットをまずコンテキストに分類します。
3. 外部ホストを許可するアクセス ルールは存在しないため、パケットは拒否され、Secure Firewall ASA によってドロップされます。
4. 外部ユーザーが内部ネットワークを攻撃しようとした場合、Secure Firewall ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

ファイアウォール モードの履歴

表 *13 :* ファイアウォール モードの各機能履歴

機能名	プラットフォームリリース	機能情報
トランスペアレント ファイアウォール モード	7.0(1)	トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。 **firewall transparent**、および **show firewall** コマンドが導入されました。 ASDM ではファイアウォール モードを設定できません。コマンドライン インターフェイスを使用する必要があります。

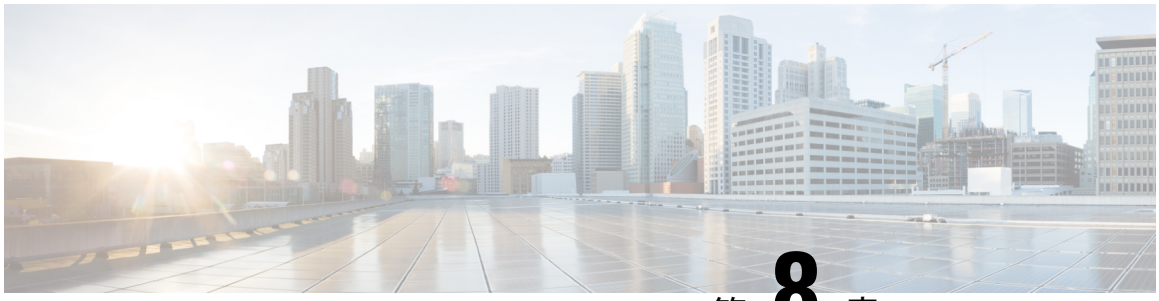
機能名	プラットフォームリリース	機能情報
トランスペアレント ファイアウォール ブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードでは最大 8 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 （注） ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]

機能名	プラットフォームリリース	機能情報
マルチ コンテキスト モードのファイアウォールモードの混合がサポートされます。	8.5(1)/9.0(1)	セキュリティ コンテキスごとに個別のファイアウォールモードを設定できます。したがってその一部をトランスペアレント モードで実行し、その他をルーテッドモードで実行することができます。 **firewall transparent** コマンドが変更されました。 シングルモードでは、ASDM でファイアウォールモードを設定することはできません。コマンドライン インターフェイスを使用する必要があります。 マルチモードでは、次の画面が変更になりました。[Configuration] > [Context Management] > [Security Contexts]。
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	ブリッジグループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジグループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 次の画面が変更されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]
トランスペアレントモードで、ブリッジグループごとのインターフェイス数が最大で 64 に増加	9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更された画面はありません。

機能名	プラットフォームリリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	

機能名	プラットフォームリリース	機能情報
		Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジグループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定するASA上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVIは名前付きインターフェイスとなり、アクセスルールやDHCPサーバーなどの一部の機能に、メンバーインターフェイスとは個別に参加できます。 トランスペアレントモードでサポートされるマルチ コンテキスト モードやASAクラスタリングの各機能は、ルーテッド モードではサポートされません。マルチキャストルーティングとダイナミック ルーティングの機能も、

機能名	プラットフォームリリース	機能情報
		BVI ではサポートされません。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Server]** **[Configuration]** > **[Firewall]** > **[Access Rules]** **[Configuration]** > **[Firewall]** > **[EtherType Rules]**
Firepower 4100/9300 ASA 論理デバイスのトランスペアレントモード展開のサポート	9.10(1)	Firepower 4100/9300 に ASA を展開するときに、トランスペアレントまたはルーテッドモードを指定できるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： **[Logical Devices]** > **[Add Device]** > **[Settings]** 新規/変更されたオプション：[Firewall Mode] ドロップダウン リスト



第 8 章

Startup Wizard

この章では、ASDM Startup Wizard について説明します。このウィザードでは、手順に従って Cisco ASA の初期設定を行い、基本設定を定義できます。

Startup Wizard へのアクセス

Startup Wizard にアクセスするには、以下のいずれかのオプションを選択します。

- [Wizards] > [Startup Wizard] を選択する。
- [Configuration] > [Device Setup] > [Startup Wizard] を選択して、[Launch Startup Wizard] をクリックする。

Startup Wizard のガイドライン

コンテキスト モードのガイドライン

Startup Wizard はシステム コンテキストではサポートされません。

Startup Wizard の画面

画面の実際の順序は、設定時の選択によって決まります。特に明記していない限り、各画面はすべてのモードまたはモデルで使用できます。

開始点またはウェルカム

- 既存の設定を変更するには、[Modify existing configuration] オプション ボタンをクリックします。
- 設定を工場出荷時のデフォルト値に設定するには、[Reset configuration to factory defaults] オプション ボタンをクリックします。
  - Management 0/0 インターフェイスの IP アドレスとサブネット マスクをデフォルト値（192.168.1.1）と異なる値に設定するには、[Configure the IP address of the management interface] チェックボックスをオンにします。

注 設定を工場出荷時のデフォルト値にリセットすると、[Cancel] をクリックしたり、この画面を閉じたりしても、変更を元に戻せません。

マルチ コンテキスト モードでは、この画面にパラメータは含まれていません。

基本設定

この画面では、ホスト名、ドメイン名、およびイネーブル パスワードを設定します。

インターフェイスの画面

インターフェイスの画面は、選択したモードとモデルによって異なります。

外部インターフェイスの設定（ルーテッド モード）

- Outside インターフェイス（セキュリティ レベルが最も低いインターフェイス）の IP アドレスを設定します。
- IPv6 アドレスを設定します。

外部インターフェイスの設定 - PPPoE（ルーテッド モード、シングル モード）

外部インターフェイスの PPPoE 設定を設定します。

Management IP Address Configuration（トランスペアレント モード）

IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジ グループに対し、管理 IP アドレスが必要です。この画面では、BVI 1 の IP アドレスを設定します。

その他のインターフェイスの設定

その他のインターフェイスのパラメータを設定します。

スタティック ルート

スタティック ルートを設定します。

DHCP サーバー

DHCP サーバーを設定します。

アドレス変換（NAT/PAT）

外部（セキュリティ レベルが最も低いインターフェイス）にアクセスするときの内部アドレス（セキュリティ レベルが最も高いインターフェイス）の NAT または PAT を設定します。詳細については、ファイアウォールの設定ガイドを参照してください。

管理アクセス

- ASDM、Telnet、または SSH アクセスを設定します。
- ASDM にアクセスするための HTTP サーバーへのセキュアな接続をイネーブルにするには、[Enable HTTP server for HTTPS/ASDM access] チェックボックスをオンにします。
- [Enable ASDM history metrics] チェックボックスをオンにします。

IPS の基本設定

シングル コンテキスト モードでは、ASDM で Startup Wizard を使用して、基本的な IPS ネットワーク設定を行います。これらの設定は、コンフィギュレーションではなく ASA コンフィギュレーションに保存されます。詳細については、IPS のクイック スタート ガイドを参照してください。

ASA CX の基本設定（ASA 5585-X）

ASDM の Startup Wizard を使用して、ASA CX の管理アドレスおよび Auth Proxy Port を設定できます。これらの設定は、ASA コンフィギュレーションではなく、ASA CX コンフィギュレーションに保存されます。ASA CX CLI での追加のネットワーク設定も必要です。この画面に関する詳細については、『ASA CX クイック スタート ガイド』を参照してください。

ASA FirePOWER の基本設定

ASDM の Startup Wizard を使用して、ASA FirePOWER の管理アドレス情報を設定し、エンドユーザー ライセンス契約（EULA）を承認することができます。これらの設定は、ASA コンフィギュレーションではなく、ASA FirePOWER コンフィギュレーションに保存されます。ASA FirePOWER CLI でも、いくつかの設定を行う必要があります。詳細については、ファイアウォールの設定ガイドの ASA FirePOWER モジュールに関する章を参照してください。

タイム ゾーンおよびクロック コンフィギュレーション

時計のパラメータを設定します。

Auto Update サーバー（シングル モード）

これらのガイドラインに従って Auto Update サーバーを設定します。

- [Enable Auto Update Server for ASA] チェックボックスをオンにして、Auto Update サーバーを設定します。
- IPS モジュールがある場合は、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。次の追加パラメータを設定します。
  - Cisco.com のユーザー名とパスワードを入力し、確認のためにパスワードを再入力します。
  - 24 時間制を使用して、hh:mm:ss 形式で開始時間を入力します。

スタートアップ ウィザードの概要

この画面には、ASA に対して行ったすべての設定の概要が表示されます。

- 前の画面での設定を変更するには、[Back] をクリックします。
- 次のいずれかを選択します。
  - スタートアップ ウィザードをブラウザから直接起動した場合は、[Finish] をクリックすると、ウィザードで作成された構成時の設定が ASA に自動的に送信され、フラッシュ メモリに保存されます。
  - ASDM 内でスタートアップ ウィザードを実行した場合は、[File] > [Save Running Configuration to Flash] を選択し、その設定を明示的にフラッシュ メモリに保存する必要があります。

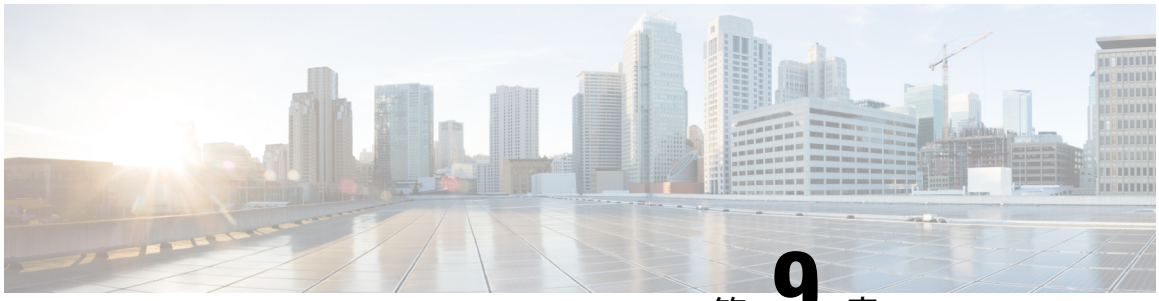
Startup Wizard の履歴

表 *14 : Startup Wizard* の履歴

機能名	プラットフォームリリース	説明
スタートアップ ウィザード	7.0(1)	このウィザードが導入されました。 [Wizards] > [Startup Wizard] 画面が導入されました。
ASA IPS の設定	8.4(1)	ASA IPS モジュールでは、[IPS Basic Configuration] 画面が Startup Wizard に追加されました。IPS モジュールに対するシグニチャアップデートが、[Auto Update] 画面に追加されました。ASA でクロックが設定されるように、[Time Zone and Clock Configuration] 画面が追加されました。IPS モジュールはそのクロックを ASA から取得します。 次の画面が導入または変更されました。 **[Wizards] > [Startup Wizard] > [IPS Basic Configuration]** **[Wizards] > [Startup Wizard] > [Auto Update]** **[Wizards] > [Startup Wizard] > [Time Zone and Clock Configuration]**
ASA CX の設定	9.1(1)	ASA CX モジュールでは、[ASA CX Basic Configuration] 画面が Startup Wizard に追加されました。 次の画面が導入されました。 **[Wizards] > [Startup Wizard] > [ASA CX Basic Configuration]**
ASA FirePOWER の設定	9.2(2.4)	ASA FirePOWER モジュールでは、[ASA FirePOWER Basic Configuration] 画面が Startup Wizard に追加されました。 次の画面が導入されました。 **[Wizards] > [Startup Wizard] > [ASA FirePOWER Basic Configuration]**

第 II 部

ハイ アベイラビリティとスケーラビリティ



第 9 章

マルチ コンテキスト モード

この章では、Cisco ASA でマルチセキュリティ コンテキストの設定方法について説明します。

セキュリティ コンテキストについて

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、マルチ コンテキスト モードのガイドライン （299 ページ）を参照してください。

この項では、セキュリティ コンテキストの概要について説明します。

セキュリティ コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービスプロバイダとして、多数のカスタマーにセキュリティ サービスを販売する。ASA 上でマルチ セキュリティ コンテキストを有効にすることによって、費用対効果の高い、省スペース ソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。

- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数の ASA が必要なネットワークを使用する場合。

コンテキスト コンフィギュレーション ファイル

この項では、ASA がマルチ コンテキスト モードのコンフィギュレーションを実装する方法について説明します。

コンテキスト コンフィギュレーション

コンテキストごとに、ASA の中に 1 つのコンフィギュレーションがあり、この中ではセキュリティ ポリシーやインターフェイスに加えて、スタンドアロン デバイスで設定できるすべてのオプションが指定されています。コンテキスト コンフィギュレーションはフラッシュ メモリ内に保存することも、TFTP、FTP、または HTTP（S）サーバーからダウンロードすることもできます。

システム設定（System Configuration）

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。

管理コンテキストの設定

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

システムがすでにマルチ コンテキスト モードになっている場合、またはシングル モードから変換された場合、管理コンテキストが admin.cfg と呼ばれるファイルとして内部フラッシュ メモリに自動的に作成されます。このコンテキストの名前は "admin" です。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

ASA がパケットを分類する方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。

（注） 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子基準

この項では、分類子で使用される基準について説明します。

（注） インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが1つだけの場合、ASAはパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

複数のコンテキストが同じインターフェイスを共有している場合は、各コンテキストでそのインターフェイスに割り当てられた一意のMACアドレスが分類子で使用されます。固有のMACアドレスがないと、アップストリームルータはコンテキストに直接ルーティングできません。MAC アドレスの自動生成を有効にできます。各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

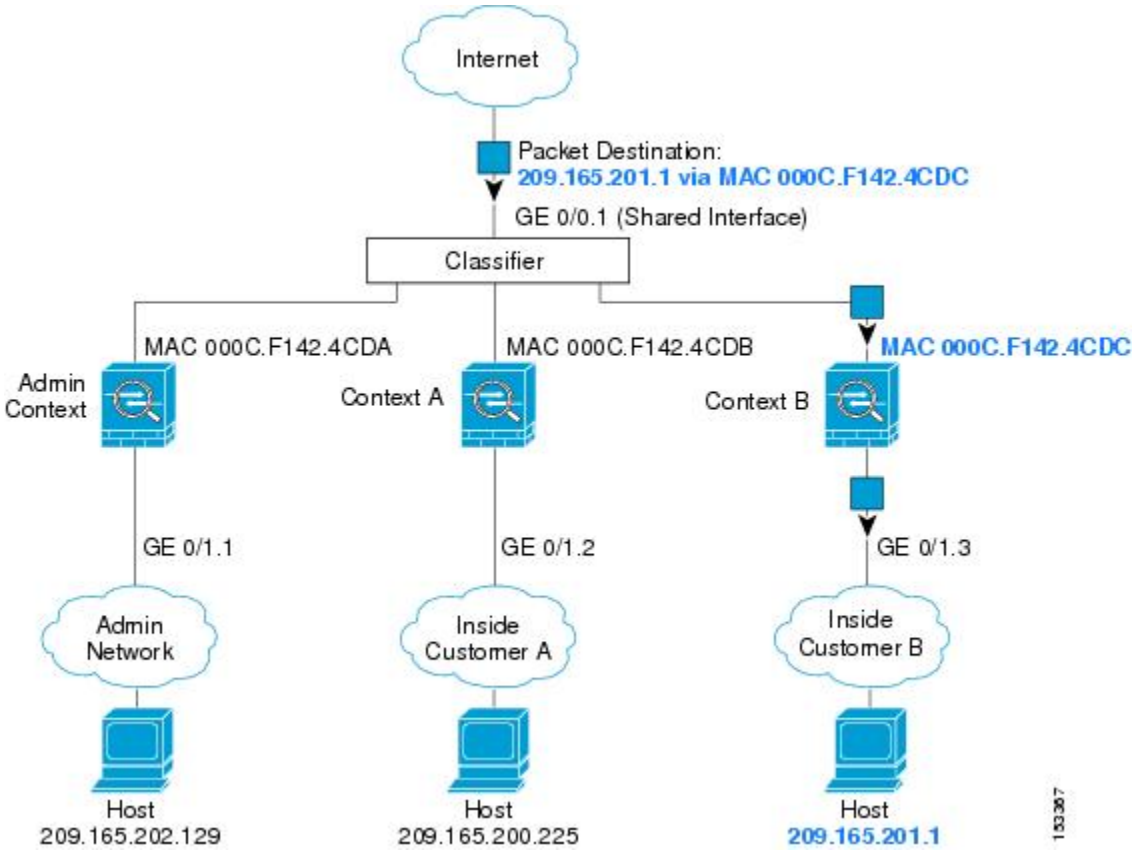
NAT の設定

固有の MAC アドレスの使用を有効にしなければ、ASA は、NAT コンフィギュレーション内のマッピングされたアドレスを使用してパケットを分類します。NAT コンフィギュレーションの完全性に関係なくトラフィック分類を行うことができるように、NAT ではなく MAC アドレスを使用することをお勧めします。

分類例

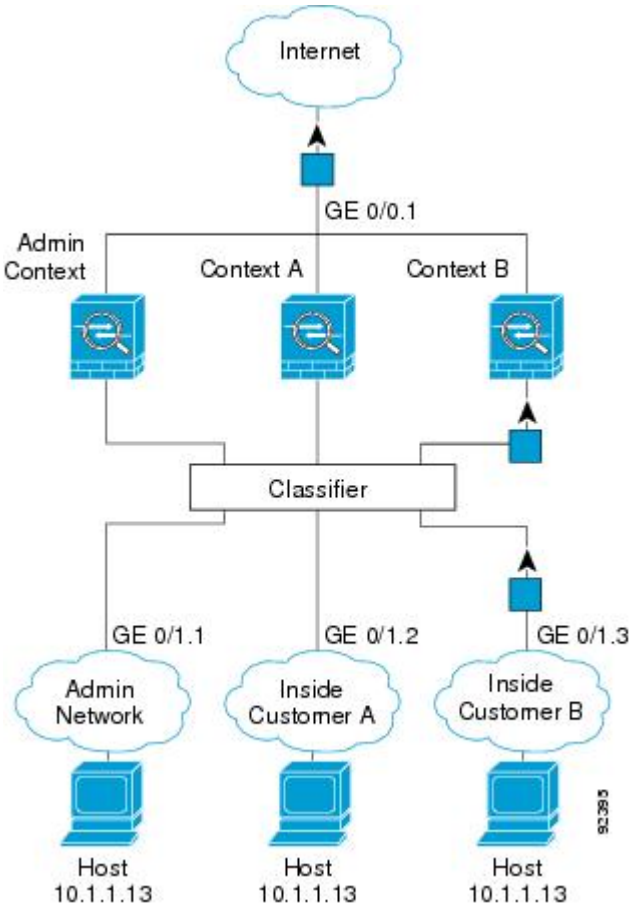
次の図に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 *39 : MAC* アドレスを使用した共有インターフェイスのパケット分類



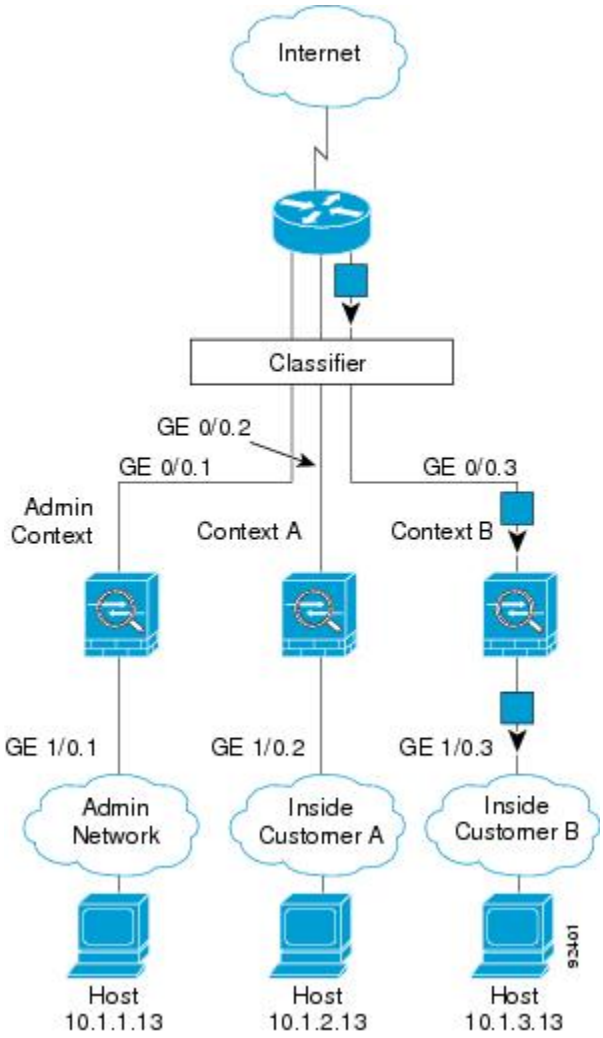
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のコンテキストBのホストを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *40 :* 内部ネットワークからの着信トラフィック



トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のコンテキストBのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *41 :* トランスペアレント ファイアウォール コンテキスト



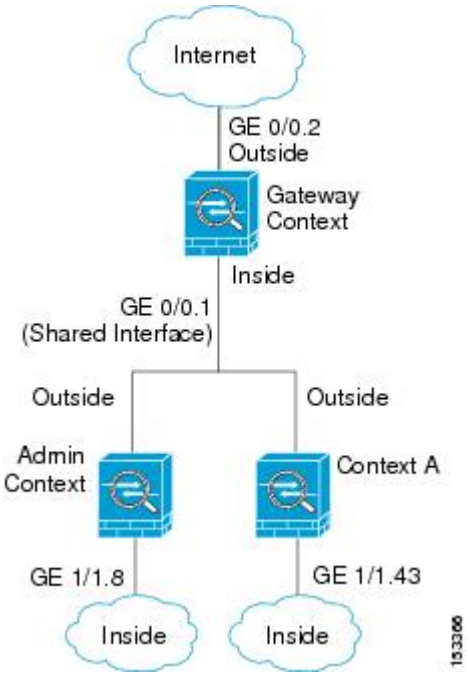
セキュリティ コンテキストのカスケード接続

コンテキストを別のコンテキストのすぐ前に置くことを、コンテキストをカスケード接続するといいます。一方のコンテキストの外部インターフェイスは、他方のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。

（注） コンテキストをカスケード接続するには、各コンテキスト インターフェイスに固有の MAC アドレスが必要です。MAC アドレスのない共有インターフェイスのパケットを分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

次の図に、ゲートウェイの背後に2つのコンテキストがあるゲートウェイ コンテキストを示します。

図 *42*：コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

ASA では、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。

システム管理者のアクセス

2 つの方法で、システム管理者として ASA をアクセスできます。

- ASA コンソールにアクセスする。

  コンソールからシステム実行スペースにアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行（run-time コマンド）だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

システム管理者として、すべてのコンテキストにアクセスできます。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザー名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、またはASDMを使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。

インターフェイス使用率の管理

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

ルーテッド ファイアウォール モードでは、管理インターフェイスをすべてのコンテキストで共有できます。

トランスペアレント ファイアウォール モードの管理インターフェイスは特殊です。許可される最大通過トラフィックインターフェイスに加えて、この管理インターフェイスを個別の管理専用インターフェイスとして使用できます。ただし、マルチコンテキストモードでは、どのインターフェイスもトランスペアレントコンテキスト間で共有させることはできません。代わりに、管理インターフェイスのサブインターフェイスを使用して、各コンテキストにインターフェイスを1つ割り当てることができます。ただし、サブインターフェイスを使用できるのは、Firepowerモデルの管理インターフェイスに限られます。のASAモデルの場合は、データインターフェイスまたはデータインターフェイスのサブインターフェイスを使用して、コンテキスト内のブリッジグループに追加する必要があります。

Firepower4100/9300シャーシトランスペアレントコンテキストでは、管理インターフェイスとサブインターフェイスのいずれも、特別なステータスを保持しません。この場合は、コンテキストをデータインターフェイスとして扱い、ブリッジグループに追加する必要があります(シングルコンテキストモードでは、管理インターフェイスで特別なステータスが保持されるので注意してください)。

トランスペアレントモードに関するもう1つの考慮事項：マルチコンテキストモードを有効にすると、設定されているすべてのインターフェイスが自動的に管理コンテキストに割り当てられます。たとえば、デフォルト設定に管理インターフェイスが含まれている場合、そのインターフェイスは管理コンテキストに割り当てられます。メインインターフェイスを管理コンテキストに割り当てたままで、ネイティブVLANを使用してメインインターフェイスを管理し、サブインターフェイスを使用して各コンテキストを管理するという選択肢もあります。管理コンテキストを透過的にすると、そのIPアドレスは削除されることに注意してください。管理コンテキストをブリッジグループに割り当て、BVIにIPアドレスを割り当てる必要があります。

リソース管理の概要

デフォルトでは、すべてのセキュリティ コンテキストはASAのリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPNのリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管

理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

リソース クラス

ASAは、リソースクラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルトクラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは1つのリソースクラスにだけ割り当てることができます。このルールの例外は、メンバ クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース制限値

個々のリソースの制限値は、パーセンテージ（ハードシステム制限がある場合）または絶対値として設定できます。

ほとんどのリソースについては、ASAはクラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASAはコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます割り当てられた量を超える、VPNセッションの一時的なバーストに対応できるように、ASAは「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バーストセッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルトクラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルトクラスの設定を何も使用しません。

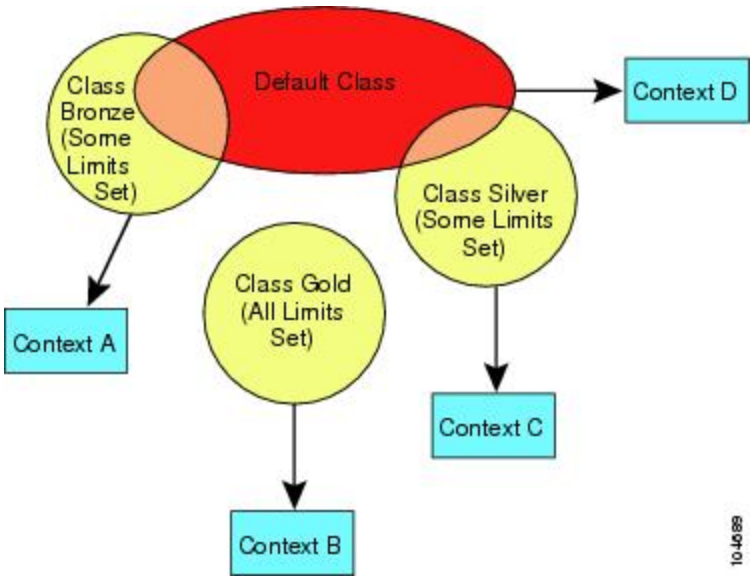
ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。

- ASDM セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（システムの最大値）。
- AnyConnect ピア：0 セッション（AnyConnect ピアを許可するようにクラスを手動で設定する必要があります）。
- VPN サイトツーサイトトンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。
- HTTPS セッション：6 セッション。（コンテキストあたりの最大値）。

次の図に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルト クラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルト クラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

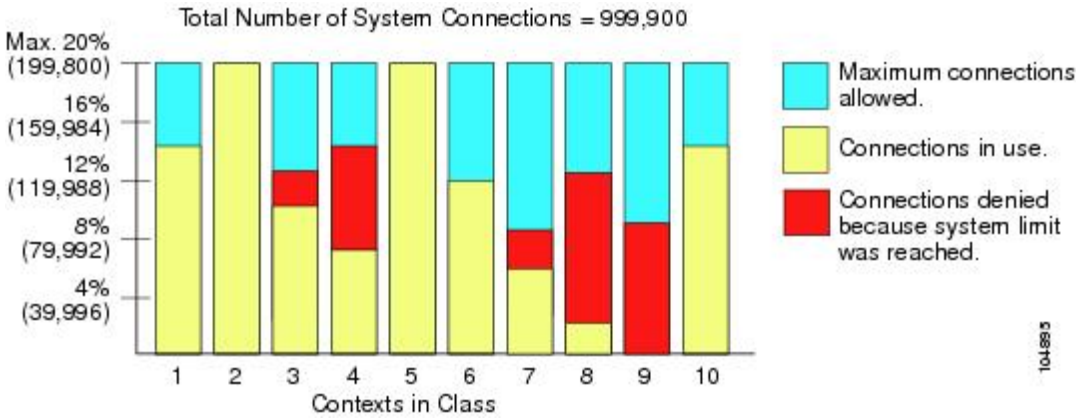
図 *43 :* リソース クラス



オーバーサブスクライブ リソースの使用

ASA をオーバーサブスクライブするには、割り当て率の合計が 100% を超えるようにあるリソースをすべてのコンテキストに割り当てます（非バーストの VPN リソースを除く）。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。

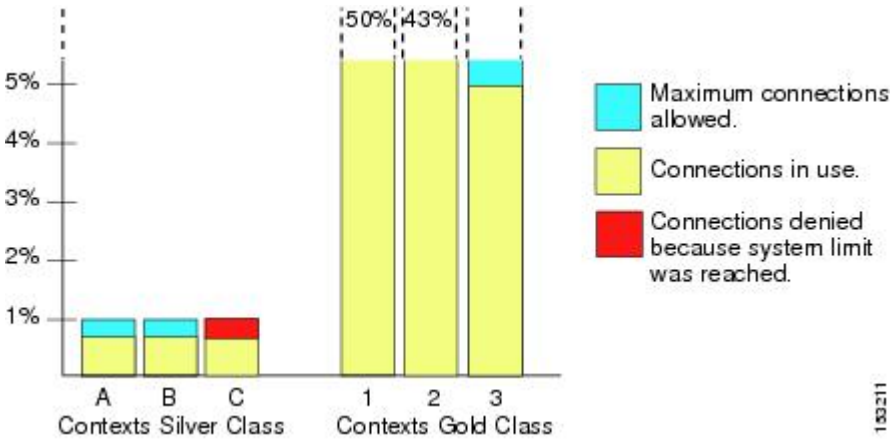
図 *44 :* リソース オーバーサブスクリプション



無限リソースの使用

ASA は、パーセンテージや絶対値ではなく、クラス内の 1 つ以上のリソースに無制限アクセスを割り当てることができます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、これらの制限の合計である 3% に達することは不可能になります無制限アクセスの設定は、ASA のオーバーサブスクライブと同様ですが、システムをどの程度オーバーサブスクライブできるかを詳細には制御できません。

図 *45 :* 無限リソース



MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。。

（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

マルチコンテキスト モードでの MAC アドレス

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。

コンテキスト間でのインターフェイス共有を許可するには、共有されるコンテキストインターフェイスそれぞれで仮想 MAC アドレスの自動生成を有効にしてください。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成が有効になっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効な場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

VPN サポート

VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

マルチ コンテキスト モードでサイト間 VPN を使用できます。

リモート アクセス VPN の場合は、SSL VPN および IKEv2 プロトコルに AnyConnect 3.x 以降を使用する必要があります。 AnyConnect のイメージとカスタマイズ、およびすべてのコンテキストで共有フラッシュ メモリを使用するために、コンテキストごとにフラッシュ ストレージをカスタマイズできます。サポートされていない機能については、マルチ コンテキスト モードのガイドライン （299 ページ） を参照してください。ASA リリースごとにサポートされる VPN 機能の詳細なリストについては、マルチ コンテキスト モードの履歴 （319 ページ） を参照してください。

（注） マルチ コンテキスト モードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードのライセンス

モデル	ライセンス要件
ASA 5506-X	サポートしない
ASA 5508-X	Security Plus ライセンス：2 コンテキスト オプション ライセンス：5 コンテキスト
ASA 5516-X	Security Plus ライセンス：2 コンテキスト オプション ライセンス：5 コンテキスト

モデル	ライセンス要件
ASA 5525-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、または *20* コンテキスト
ASA 5545-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、*20*、または *50* コンテキスト
ASA 5555-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、*20*、*50*、または *100* コンテキスト。
Firepower 1010	サポートしない
Firepower 1100	基本ライセンス：2 コンテキスト オプションライセンス、最大値： *Firepower 1120*：*5* *Firepower 1140*：*5* *Firepower 1150*：*25*
Firepower 2100	基本ライセンス：2 コンテキスト オプション ライセンス、最大 *5* または *10* の増分： *Firepower 2110*：*25* *Firepower 2120*：*25* *Firepower 2130*：*30* *Firepower 2140*：*40*
Firepower 4100	基本ライセンス：10 コンテキスト オプションのライセンス：*10* コンテキストずつの追加で、*250* コンテキストまで。
Firepower 9300	基本ライセンス：10 コンテキスト オプションのライセンス：*10* コンテキストずつの追加で、*250* コンテキストまで。
ISA 3000	サポートしない
ASAv	サポートしない

（注） 管理コンテキストに管理専用インターフェイスのみが含まれていて、通過トラフィックのデータインターフェイスが含まれていない場合は、制限に対してカウントされません。

（注） マルチ コンテキスト モードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードの前提条件

マルチ コンテキスト モードに切り替えた後で、システム コンフィギュレーションにアクセスするために管理コンテキストに接続します。管理以外のコンテキストからシステムを設定することはできません。デフォルトでは、マルチ コンテキスト モードをイネーブルにした後はデフォルトの管理 IP アドレスを使用して管理コンテキストに接続できます。

マルチ コンテキスト モードのガイドライン

フェールオーバー

アクティブ/アクティブ モードフェールオーバーは、マルチコンテキストモードでのみサポートされます。

IPv6

クロス コンテキスト IPv6 ルーティングはサポートされません。

サポートされない機能

マルチコンテキスト モードでは、次の機能をサポートしません。

- RIP
- OSPFv3 （OSPFv2 がサポートされます）。
- マルチキャスト ルーティング
- 脅威の検出
- ユニファイド コミュニケーション
- QoS
- 仮想トンネルインターフェイス（VTI）
- スタティック ルート トラッキング

マルチ コンテキスト モードでは、次のリモート アクセス VPN の機能を現在サポートしません。

- クライアントレス SSL VPN
- AnyConnect 2.x 以前
- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN ロード バランシング
- カスタマイゼーション
- L2TP

その他のガイドライン

- コンテキストモード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを match に設定します。
- フラッシュ メモリのルート ディレクトリにコンテキスト コンフィギュレーションを保存する場合、一部のモデルでは、メモリに空き容量があっても、そのディレクトリに保存する余地がなくなることがあります。この場合は、コンフィギュレーション ファイルのサブディレクトリを作成します。Background: some models use the FAT 16 file system for internal flash memory, and if you do not use 8.3-compliant short names, or use uppercase characters, then fewer than 512 files and folders can be stored because the file system uses up slots to store long file names（see http://support.microsoft.com/kb/120138/en-us).

マルチ コンテキスト モードのデフォルト

- デフォルトで、ASA はシングル コンテキスト モードになります。
- デフォルト クラス （293 ページ） を参照してください。

マルチ コンテキストの設定

手順

ステップ 1 マルチ コンテキスト モードの有効化または無効化 （301 ページ）。

ステップ 2 （任意）リソース管理用のクラスの設定 （303 ページ）。

（注） VPN のサポートのために、リソース クラスの VPN リソースを設定する必要があります。デフォルト クラスは VPN を許可しません。

ステップ 3 システム実行スペースでインターフェイスを設定します。

- ASA 5500-X、Firepower 1100、アプライアンスモードの Firepower 2100：基本的なインターフェイス設定 （609 ページ）。
- プラットフォームモードの Firepower 2100：スタートアップ ガイドを参照してください。
- Firepower 4100/9300—論理デバイス Firepower 4100/9300 （223 ページ）

ステップ 4 セキュリティ コンテキストの設定 （308 ページ）。

ステップ 5 （任意）コンテキスト インターフェイスへの MAC アドレスの自動割り当て （311 ページ）。

ステップ 6 コンテキストのインターフェイス コンフィギュレーションを完成させます。ルーテッド モードおよびトランスペアレント モードのインターフェイス （675 ページ） を参照してください。

マルチ コンテキスト モードの有効化または無効化

シスコへの発注方法によっては、ASA がすでにマルチセキュリティ コンテキスト用に設定されている場合があります。シングル モードからマルチ モードに変換する必要がある場合は、この項の手順に従ってください。

ASDM では、[ハイ アベイラビリティおよび拡張性（High Availability and Scalability）] ウィザードを使用し、アクティブ/アクティブ フェールオーバーを有効にした場合、シングル モードからマルチ モードへの変更をサポートします。詳細については、ハイ アベイラビリティのためのフェールオーバー （325 ページ） を参照してください。アクティブ/アクティブ フェールオーバーを使用するか、またはシングル モードに戻す場合は、CLI を使用してモードを変更する必要があります。モードの変更には確認を必要とするため、コマンドライン インターフェイス ツールは使用できません。この項では、CLI でのモード変更について説明します。

マルチ コンテキスト モードの有効化

シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。これらはシステム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管

理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルート ディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

始める前に

スタートアップ コンフィギュレーションが実行コンフィギュレーションと異なっている場合はバックアップします。シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを2つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されません。ファイルの管理 （1198 ページ）を参照してください。

手順

マルチコンテキストモードに変更します。

mode multiple

例：

モードを変更して設定を変換し、システムをリロードするように求められます。

（注） SSH 接続を再確立する前に、管理コンテキストで RSA キーペアを再生成する必要があります。コンソールから、**crypto key generate rsa modulus** コマンドを入力します。詳細については、SSH アクセスの設定 （1142 ページ） を参照してください。

例：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system
```

```
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

シングルコンテキスト モードの復元

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングル モードに変更するには、次の手順を実行します。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 元の実行コンフィギュレーションのバックアップバージョンを現在のスタートアップ コンフィギュレーションにコピーします。

copy disk0:old_running.cfg startup-config

例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

ステップ 2 モードをシングル モードに設定します。

mode single

例：

```
ciscoasa(config)# mode single
```

ASA をリブートするよう求められます。

リソース管理用のクラスの設定

システム コンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

始める前に

- この手順はシステム実行スペースで実行します。
- 以下の表に、リソース タイプおよび制限を記載します。

注　「システム制限」に「該当なし」と記述されている場合、そのリソースにはハード システム制限がないため、リソースのパーセンテージを設定できません。

表 *15*：リソース名および制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
ASDM Sessions	同時接続数	最小 1 最大 5	200	ASDM 管理セッション。 ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 200 の場合、HTTPS セッション数は 400 に制限されます。
Connections Conns/Sec	同時またはレート	該当なし	同時接続数：モデルごとの接続制限については、モデルごとにサポートされている機能のライセンス（131 ページ）を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。 （注）　syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
ホスト	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。
Inspects/sec	利率	該当なし	該当なし	アプリケーション インスペクション数/秒。
MAC Entries	同時接続数	該当なし	65,535	トランスペアレントファイアウォールモードでは、MACアドレステーブルで許可される MAC アドレス数。
ルート	同時接続数	該当なし	該当なし	ダイナミック ルート。
AnyConnect Burst	同時接続数	該当なし	モデルに応じた AnyConnect Premium ピア数から、AnyConnect 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	AnyConnect でコンテキストに割り当てられた数を超えて許可される AnyConnect セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、AnyConnect で割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが AnyConnect Burst に使用可能です。AnyConnect ではセッション数がコンテキストに対して保証されますが、対照的に AnyConnect Burst ではオーバーサブスクライブが可能です。バースト プールをすべてのコンテキストが、先着順に使用できます。
AnyConnect	同時接続数	該当なし	ご使用のモデルに使用できる AnyConnect Premium ピアについては、モデルごとにサポートされている機能のライセンス （131 ページ）を参照してください。	AnyConnect ピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
Other VPN Burst	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、Other VPN 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	Other VPN でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえばモデルが 5000 セッションをサポートしており、Other VPN のすべてのコンテキスト全体で 4000 セッションを割り当てると、残りの 1000 セッションは Other VPN Burst に使用できます。Other VPN ではセッション数がコンテキストに対して保証されますが、対照的に Other VPN Burst ではオーバーサブスクライブが可能です。すべてのコンテキストでバースト プールを先着順に使用できます。
その他の VPN	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、モデルごとにサポートされている機能のライセンス（131 ページ）を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
IKEv1 SAs In Negotiation	同時（パーセンテージのみ）	該当なし	このコンテキストに割り当てられている Other VPN セッションのパーセンテージ。セッションをコンテキストに割り当てるには、Other VPN リソースを参照してください。	コンテキストでの Other VPN パーセンテージ制限として表される、着信 IKEv1 SA ネゴシエーション。
SSH	同時接続数	最小 1 最大 5	100	SSH セッション。
ストレージ	MB	最大値は、指定するフラッシュ メモリのドライブによって異なります。	最大値は、指定するフラッシュ メモリのドライブによって異なります。	コンテキストでのディレクトリのストレージ制限（MB 単位）。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
Syslogs/sec	利率	該当なし	該当なし	Syslog メッセージ数/秒。
Telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
Xlates	同時接続数	該当なし	該当なし	ネットワーク アドレス変換。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 **[設定（Configuration）] > [コンテキスト管理（Context Management）] > [リソース クラス（Resource Class）]** の順に選択し、[追加（Add）] をクリックします。

[Add Resource Class] ダイアログボックスが表示されます。

ステップ 3 [Resource Class] フィールドに、最大 20 文字のクラス名を入力します。

ステップ 4 [Count Limited Resources] 領域で、リソースの同時接続制限を設定します。

各リソース タイプの説明については、上記の表を参照してください。

システム制限のないリソースは、パーセント（%）で設定できません。設定できるのは絶対値だけです。制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、リソースは無制限またはシステム制限値（使用できる場合）に設定されます。ほとんどのリソースについて、0 を指定すると無制限と設定されます。VPN タイプについて、0 を指定すると制限なしと設定されます。

（注） また、コンテキスト内で **[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]** も設定して、最大管理セッション（SSH など）を設定した場合は、小さい方の値が使用されます。

ステップ 5 [Rate Limited Resources] 領域で、リソースのレート制限を設定します。

各リソース タイプの説明については、上記の表を参照してください。

制限を設定しない場合、デフォルト クラスの制限値が継承されます。制限値がデフォルト クラスにない場合は、デフォルトでは無制限になります。0 は制限を無制限に設定します。

ステップ 6 [OK] をクリックします。

セキュリティ コンテキストの設定

システム コンフィギュレーションのセキュリティ コンテキスト定義では、コンテキスト名、コンフィギュレーション ファイルの URL、コンテキストが使用できるインターフェイス、およびその他の設定値を指定します。

始める前に

- この手順はシステム実行スペースで実行します。
- インターフェイスを設定します。トランスペアレントモードのコンテキストでは、コンテキスト間でインターフェイスを共有できないため、サブインターフェイスの使用が必要になる場合があります。管理インターフェイスの使用計画については、「インターフェイス使用率の管理 （292 ページ）」を参照してください。
  - ASA 5500-X、Firepower 1100、アプライアンスモードの Firepower 2100：基本的なインターフェイス設定 （609 ページ）。
  - プラットフォームモードの Firepower 2100：スタートアップ ガイドを参照してください。
  - Firepower 4100/9300—論理デバイス Firepower 4100/9300 （223 ページ）

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[デバイス リスト（Device List）] ペインで、アクティブなデバイスの IP アドレスの下にある [システム（System）] をダブルクリックします。

ステップ 2 **[構成（Configuration）] > [コンテキスト管理（Context Management）] > [セキュリティ コンテキスト（Security Contexts）]** の順に選択し、[追加（Add）] をクリックします。

[コンテキストの追加（Add Context）] ダイアログボックスが表示されます。

ステップ 3 [セキュリティ コンテキスト（Security Context）] フィールドに、コンテキストの名前を 32 文字以内の文字列で入力します。

この名前は大文字と小文字が区別されるため、たとえば「customerA」と「CustomerA」という 2 つのコンテキストを設定できます。「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

ステップ 4 [インターフェイス割り当て（Interface Allocation）] 領域で、[追加（Add）] ボタンをクリックし、コンテキストにインターフェイスを割り当てます。

a) **[Interfaces] > [Physical Interface]** ドロップダウン リストからインターフェイスを選択します。

メイン インターフェイスを割り当てる場合、サブインターフェイス ID を空白にします。サブインターフェイスまたはその範囲を指定すると、このインターフェイスに設定されます。トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てら

れていないインターフェイスだけが表示されます。メインインターフェイスが他のコンテキストに割り当てられている場合、サブインターフェイスを選択する必要があります。

b) （オプション）**[インターフェイス（Interfaces）]**>**[サブインターフェイス範囲（Subinterface Range）]** ドロップダウン リストからサブインターフェイス ID を選択します。

サブインターフェイス ID の範囲を指定する場合、2 つ目のドロップダウン リストが有効であれば、そこから最後の ID を選択します。

トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます。

c) （オプション）[エイリアス名（Aliased Names）] 領域で、[コンテキストでエイリアス名を使用する（Use Aliased Name in Context）] をオンにして、このインターフェイスに対して、コンテキスト コンフィギュレーションでインターフェイス ID の代わりに使用するエイリアス名を設定します。

- [名前（Name）] フィールドに、エイリアス名を設定します。

  エイリアス名の先頭および最後は英字にします。間の文字として使用できるのは、英字、数字、下線だけです。このフィールドで名前の最後を英字または下線にした場合、その名前の後に追加する数字を [範囲（Range）] フィールドで設定できます。

- （オプション）[範囲（Range）] フィールドで、エイリアス名のサフィックスを数字で設定します。

  サブインターフェイスに範囲がある場合、範囲の数字を入力して名前の後に追加できます。

d) （オプション）エイリアス名を設定した場合でも、コンテキストのユーザーが物理インターフェイスのプロパティを表示できるようにするには、[コンテキストでハードウェア プロパティを表示する（Show Hardware Properties in Context）] をオンにします。

e) [OK] をクリックして、[コンテキストの追加（Add Context）] ダイアログボックスに戻ります。

ステップ 5 （任意）[リソース割り当て（Resource Assignment）] 領域で、[リソース クラス（Resource Class）] ドロップダウン リストから、このコンテキストをリソース クラスに割り当てるクラス名を選択します。

この領域から直接リソース クラスを追加または編集できます。

ステップ 6 [構成 URL（Config URL）] ドロップダウン リストから、ファイル システム タイプを選択します。フィールドに、コンテキスト コンフィギュレーションの場所の URL を指定します。

FTP の場合、URL は次の形式になります。

ftp://server.example.com/configs/admin.cfg

ステップ 7 （任意）[ログイン（Login）] をクリックし、外部ファイル システムのユーザー名とパスワードを設定します。

ステップ 8 （任意）[フェールオーバーグループ（Failover Group）] ドロップダウン リストからグループ名を選択し、アクティブ/アクティブ フェールオーバーのフェールオーバー グループを設定します。

ステップ 9 （任意）[クラウド Web セキュリティ（Cloud Web Security）] の [有効化（Enable）] をクリックして、このコンテキストで Web セキュリティ インスペクションを有効にします。システム コンフィギュレーションに設定されたライセンスを上書きする場合は、[ライセンス（License）] フィールドにライセンスを入力します。

ステップ 10 （任意）[説明（Description）] フィールドに、説明を追加します。

ステップ 11 （任意）[ストレージ URL 割り当て（Storage URL Assignment）] 領域では、各コンテキストでフラッシュ メモリを使用して AnyConnect などの VPN パッケージを保存できるだけでなく、AnyConnect およびクライアントレス SSL VPN ポータルのカスタマイズ設定のストレージも提供できるようにすることができます。たとえば、マルチ コンテキスト モードを使用してダイナミック アクセス ポリシーを含む AnyConnect プロファイルを設定する場合は、コンテキスト固有のプライベート ストレージおよび共有ストレージを計画する必要があります。読み取り専用の共有記憶域だけでなく、コンテキストごとに専用の記憶域も使用できます。**注：[ツール（Tools）] > [ファイル管理（File Management）]** を使用して、指定するディスク上にターゲット ディレクトリがすでに存在することを確認してください。

a) [プライベート ストレージ割り当ての構成（Configure private storage assignment）] チェックボックスをオンにして、[選択（Select）] ドロップダウン リストから専用ストレージ ディレクトリを選択します。private で指定できる専用記憶域は、コンテキストごとに 1 つに限られます。コンテキスト内から（およびシステム実行スペースから）、このディレクトリの読み取り/書き込み/削除操作を実行できます。ASA は指定されたパスにサブディレクトリを作成し、コンテキストに基づく名前を付けます。たとえば、contextA の場合、**disk1:/private-storage** をパスとして指定すると、ASA はこのコンテキストのサブディレクトリを **disk1:/private-storage/contextA/** に作成します。オプションで、ファイル システムがコンテキスト管理者に公開されないよう、このパスにコンテキスト内での名前を指定することもできます。それには、[マッピング先（is mapped to）] フィールドに名前を入力します。たとえば、**context** をマップされる名前として指定すると、コンテキスト内からは、このディレクトリは **context:** と呼ばれます。コンテキストごとに許容するディスク容量を制御する方法については、リソース管理用のクラスの設定 （303 ページ）を参照してください。

b) [共有ストレージ割り当ての構成（Configure shared storage assignment）] チェックボックスをオンにして、[選択（Select）] ドロップダウン リストから共有ストレージ ディレクトリを選択します。指定できる読み取り専用の **shared** 記憶域はコンテキストごとに 1 つですが、共有ディレクトリは複数作成できます。AnyConnect パッケージなど、すべてのコンテキストに共通の大きなファイルを共有記憶域で共有することで、大きなファイルの重複を抑えることができます。この記憶域は複数のコンテキストで共有されるため、ASA は記憶域にはコンテキストのサブディレクトリを作成しません。共有ディレクトリの書き込みおよび削除操作は、システム実行スペースでのみ実行できます。

ステップ 12 [OK] をクリックして、[セキュリティ コンテキスト（Security Contexts）] ペインに戻ります。

ステップ 13 （任意） コンテキストを選択してから [ファイアウォール モードの変更（Change Firewall Mode）] をクリックし、ファイアウォール モードをトランスペアレントに設定します。

新しいコンテキストの場合は、消去するための設定はありません。[モードの変更（Change Mode）] をクリックして、トランスペアレント ファイアウォール モードに変更します。

既存のコンテキストの場合は、モードを変更する前に設定をバックアップするのを忘れないでください。

（注） ASDM の現在接続されているコンテキストのモード（通常は管理コンテキスト）は変更できません。コマンド ラインでモードを設定するには、ファイアウォール モード（シングル モード）の設定 （258 ページ）を参照してください。

ステップ 14 （任意） MAC アドレスの自動生成をカスタマイズするには、コンテキスト インターフェイスへの MAC アドレスの自動割り当て （311 ページ）を参照してください。

ステップ 15 （任意） デバイスの最大 TLS プロキシ セッション数を指定するには、[ASA でサポートされる必要がある TLS プロキシ セッションの最大数の指定（Specify the maximum number of TLS Proxy sessions that the ASA needs to support）] チェックボックスをオンにします。TLS プロキシの詳細については、ファイアウォールの設定ガイドを参照してください。

コンテキスト インターフェイスへの MAC アドレスの自動割り当て

この項では、MACアドレスの自動生成の設定方法について説明します。MACアドレスは、コンテキスト内でパケットを分類するために使用されます。

始める前に

- コンテキストでインターフェイスの名前を設定すると、ただちに新規 MAC アドレスが生成されます。コンテキストインターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[デバイスリスト（Device List）] ペインで、アクティブなデバイスの IP アドレスの下にある [システム（System）] をダブルクリックします。

ステップ 2 **[設定（Configuration）] > [コンテキスト管理（Context Management）] > [セキュリティ コンテキスト（Security Contexts）]** の順に選択し、[自動 MAC アドレス（Mac-Address auto）] をオンにします。プレフィックスを入力しない場合は、ASA によって、インターフェイスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 3 （オプション）[プレフィックス（Prefix）] チェックボックスをオンにしてから、フィールドに 0 ～ 65535 の範囲内の 10 進数値を入力します。

このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

コンテキストとシステム実行スペースの切り替え

システム実行スペース（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニターリングを実行することができます。コンフィギュレーションモードで編集される実行コンフィギュレーション実行コンフィギュレーションは、ユーザーのログイン先によって決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。

手順

ステップ 1 [Device List] ペインでシステムを設定するには、アクティブなデバイスの IP アドレスの下にある [System] をダブル クリックします。

ステップ 2 コンテキストを設定するには、[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

セキュリティ コンテキストの管理

この項では、セキュリティ コンテキストを管理する方法について説明します。

セキュリティ コンテキストの削除

現在の管理コンテキストは削除できません。

（注） フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 **[Configuration]** > **[Context Management]** > **[Security Contexts]** の順に選択します。

ステップ 3 削除するユーザーを選択し、[Delete] をクリックします。

[Delete Context] ダイアログボックスが表示されます。

ステップ 4 このコンテキストを再追加するかもしれず、再使用できるようにコンフィギュレーション ファイルを保持する場合は、[Also delete config URL file from the disk] チェックボックスをオフにします。

コンフィギュレーション ファイルを削除するには、チェックボックスをオンにしたままにします。

ステップ 5 [Yes] をクリックします。

管理コンテキストの変更

システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。

（注） ASDM の場合、ASDM セッションが切断されるため、ASDM 内の管理コンテキストを変更できません。新しい管理コンテキストに再割り当てなければならないことに注意するコマンドライン インターフェイス ツールを使用してこの手順を実行できます。

始める前に

- コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。
- この手順はシステム実行スペースで実行します。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 **[Tools]** > **[Command Line Interface]** を選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 3 次のコマンドを入力します。

admin-context *context_name*

ステップ 4 [Send] をクリックします。

Telnet、SSH、HTTPS（ASDM）など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。

（注） いくつかのシステム コンフィギュレーション コマンド、たとえば **ntp server** では、管理コンテキストに所属するインターフェイス名が指定されます。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

セキュリティ コンテキスト URL の変更

この項では、コンテキスト URL を変更する方法について説明します。

始める前に

- セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。
- 同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。
- マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。
  - コンフィギュレーションが同じ場合、変更は発生しません。
  - コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバーが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。

- コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。
- この手順はシステム実行スペースで実行します。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 **[Configuration]** > **[Context Management]** > **[Security Contexts]** の順に選択します。

ステップ 3 編集するコンテキストを選択して、[Edit] をクリックします。

[Edit Context] ダイアログボックスが表示されます。

ステップ 4 [Config URL] フィールドに新しい URL を入力して、[OK] をクリックします。

システムは、動作中になるように、ただちにコンテキストをロードします。

セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の 2 つの方法でリロードできます。

- 実行コンフィギュレーションをクリアしてからスタートアップ コンフィギュレーションをインポートする。

  このアクションでは、セキュリティ コンテキストに関連付けられている接続や NAT テーブルなどの属性の大部分がクリアされます。

- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。

  このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的な属性がクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

コンフィギュレーションのクリアによるリロード

手順

ステップ 1 [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

ステップ 2 **[Tools]** > **[Command Line Interface]** を選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 3 次のコマンドを入力します。

clear configure all

ステップ 4 [Send] をクリックします。

コンテキストの設定が削除されます。

ステップ 5 **[Tools]** > **[Command Line Interface]** を再度選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 6 次のコマンドを入力します。

copy startup-config running-config

ステップ 7 [Send] をクリックします。

ASA が設定をリロードします。ASA は、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の手順を実行してください。

手順

ステップ 1 セキュリティ コンテキストの削除 （312 ページ）。[Also delete config URL file from the disk] チェックボックスがオフになっていることを確認します。

ステップ 2 セキュリティ コンテキストの設定 （308 ページ）

セキュリティ コンテキストのモニターリング

この項では、コンテキスト情報を表示およびモニターリングする方法について説明します。

コンテキスト リソースの使用状況のモニターリング

手順

ステップ 1 まだシステム モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 ツールバーの [Monitoring] ボタンをクリックします。

ステップ 3 [Context Resource Usage] をクリックします。

すべてのコンテキストのリソース使用状況を表示するには、次の各リソースタイプをクリックします。

- [ASDM/Telnet/SSH]：ASDM、Telnet、SSH 接続状況を表示します。
  - [Context]：各コンテキストの名前を表示します。

    各アクセス方式に対して、次の使用状況統計が表示されます。
  - [Existing Connections (#)]：既存の接続の数を表示します。
  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [Routes]：ダイナミック ルートの使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Existing Connections (#)]：既存の接続の数を表示します。
  - [Existing Connections (%)]：このコンテキストで使用されている接続数を、すべてのコンテキストで使用されている接続の総数のパーセントとして表示します。
  - [Peak Connections (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク接続数を表示します。
- [Xlates]：ネットワーク アドレス変換の使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Xlates (#)]：現在の xlate の数を表示します。
  - [Xlates (%)]：このコンテキストで使用されている xlate 数を、すべてのコンテキストで使用されている xlate の総数のパーセントとして表示します。
  - [Peak (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク xlate 数を表示します。
- [NATs]：NAT ルールの数を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [NATs (#)]：現在の NAT ルールの数を表示します。
  - [NATs (%)]：このコンテキストで使用されている NAT ルール数を、すべてのコンテキストで使用されている NAT ルールの総数のパーセントとして表示します。

- [Peak NATs (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク NAT ルール数を表示します。

- **[Syslogs]**：システム ログ メッセージのレートを表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [Syslog Rate (#/sec)]：システム ログ メッセージの現在のレートを表示します。
  - [Syslog Rate (%)]：このコンテキストで生成されたシステム ログ メッセージ数を、すべてのコンテキストで生成されたシステム ログ メッセージの総数のパーセントとして表示します。
  - [Peak Syslog Rate (#/sec)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のシステム ログ メッセージのピーク レートを表示します。

- [VPN]：VPN サイトツーサイト トンネルの使用状況を表示します。
  - [Context]：各コンテキストの名前を表示します。
  - [VPN Connections]：保証された VPN セッションの使用状況を表示します。
  - [VPN Burst Connections]：バースト VPN セッションの使用状況を表示します。
    - [Existing (#)]：既存トンネルの数を表示します。
    - [Peak (#)]：**clear resource usage** コマンドの使用またはデバイスのリブートにより統計情報が最後にクリアされて以降のピーク トンネル数を表示します。

ステップ 4 表示をリフレッシュするには、**[Refresh]** をクリックします。

割り当てられた MAC アドレスの表示

システム コンフィギュレーション内またはコンテキスト内の自動生成された MAC アドレスを表示できます。

システム設定での MAC アドレスの表示

この項では、システム コンフィギュレーション内の MAC アドレスを表示する方法について説明します。

始める前に

MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 **[Configuration]** > **[Context Management]** > **[Security Contexts]** を選択し、[Primary MAC] カラムと [Secondary MAC] カラムを表示します。

コンテキスト内の MAC アドレスの表示

この項では、コンテキスト内で MAC アドレスを表示する方法について説明します。

手順

ステップ 1 まだシステム コンフィギュレーション モードに入っていない場合、[Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

ステップ 2 **[Configuration]** > **[Interfaces]** を選択し、[MAC Address] アドレス カラムを表示します。

このテーブルには、使用中の MAC アドレスが表示されます。MAC アドレスを手動で割り当てており、自動生成もイネーブルになっている場合は、システム コンフィギュレーションからは未使用の自動済み生成アドレスのみを表示できます。

マルチ コンテキスト モードの履歴

表 *16 :* マルチ コンテキスト モードの履歴

機能名	プラットフォームリリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 次の画面が導入されました。[Configuration] > [Context Management]。

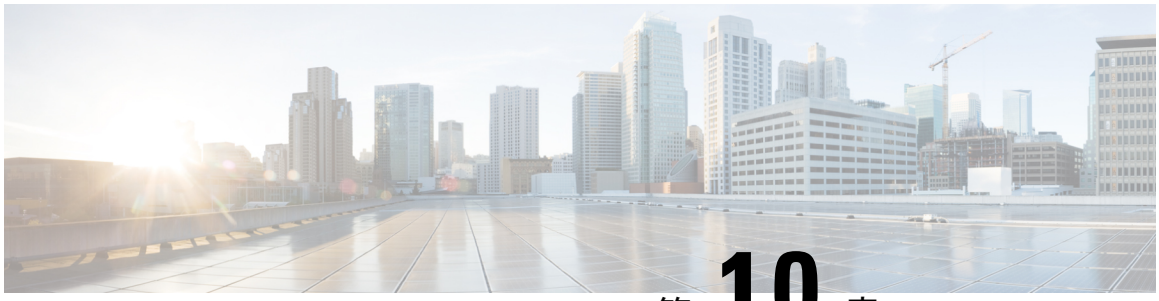
機能名	プラットフォームリリース	機能情報
MAC アドレス自動割り当て	7.2(1)	コンテキスト インターフェイスへの MAC アドレス自動割り当てが導入されました。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
リソース管理	7.2(1)	リソース管理が導入されました。 次の画面が導入されました。[Configuration] > [Context Management] > [Resource Management]。
IPS 仮想センサー	8.0(2)	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に複数のセキュリティ ポリシーを設定することができます。各コンテキストまたはシングル モード ASA を 1 つまたは複数の仮想センサーに割り当てたり、複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
MAC アドレス自動割り当ての機能強化	8.0(2)	MACアドレス形式が変更されました。プレフィックスが使用され、固定開始値（A2）が使用されます。また、フェールオーバー ペアのプライマリ装置とセカンダリ装置のMACアドレスそれぞれに異なるスキームが使用されます。MACアドレスはリロード後も維持されるようになりました。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MACアドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
ASA 5550 および 5580 の最大コンテキスト数の増加	8.4(1)	ASA 5550 の最大セキュリティ コンテキスト数が 50 から 100 に増加しました。ASA 5580 での最大数が 50 から 250 に増加しました。
MAC アドレスの自動割り当てのデフォルトでの有効化	8.5(1)	MACアドレスの自動割り当てが、デフォルトでイネーブルになりました。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。

機能名	プラットフォームリリース	機能情報
MAC アドレス プレフィックスの自動生成	8.6(1)	マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）の MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。プレフィックスを変更する場合、カスタムプレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 （注） フェールオーバーペアのヒットレスアップグレードを維持するため、ASA は、フェールオーバーが有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。ただし、フェールオーバーを使用するときは、生成メソッドをプレフィックスに手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス メソッドを使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]
ASASM 以外のすべてのモデル上での MAC アドレスの自動割り当てはデフォルトでディセーブル	9.0(1)	自動 MAC アドレスの割り当ては ASASM を除いて、デフォルトでディセーブルになりました。 次の画面が変更されました。[Configuration] > [Context Management] > [Security Contexts]。
セキュリティ コンテキストでのダイナミック ルーティング	9.0(1)	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、マルチ コンテキスト モードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャスト ルーティングはサポートされません。

機能名	プラットフォームリリース	機能情報
ルーティング テーブル エントリのための新しいリソース タイプ	9.0(1)	新規リソース タイプ routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 次の画面が変更されました。[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]
マルチ コンテキスト モードのサイトツーサイト VPN	9.0(1)	サイトツーサイト VPN トンネルが、マルチ コンテキスト モードでサポートされるようになりました。
サイトツーサイト VPN トンネルのための新しいリソース タイプ	9.0(1)	新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。 次の画面が変更されました。[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]
IKEv1 SA ネゴシエーションの新しいリソース タイプ	9.1(2)	CPU と暗号化エンジンの過負荷を防ぐため、コンテキストごとに IKEv1 SA ネゴシエーションの最大パーセンテージを設定するための新しいリソース タイプ ikev1 in-negotiation が作成されました。特定の条件（大容量の証明書、CRL、チェックなど）によっては、このリソースを制限する必要がある場合があります。 次の画面が変更されました。[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]
マルチ コンテキスト モードでのリモート アクセス VPN サポート	9.5(2)	次のリモートアクセス機能をマルチ コンテキストモードで使用できるようになりました。 • AnyConnect 3.x 以降（SSL VPN のみ、IKEv2 はサポートしません） • 中央集中型 AnyConnect イメージ設定 • AnyConnect イメージのアップグレード • AnyConnect 接続のコンテキスト リソース管理 （注） マルチ コンテキスト モードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。 次の画面が変更されました。**[Configuration] > [Context Management] > [Resource Class] > [Add Resource Class]**

機能名	プラットフォームリリース	機能情報
マルチ コンテキスト モードの場合の証明書の事前入力/ユーザー名	9.6(2)	AnyConnect SSL サポートが拡張され、これまでシングル モードでのみ使用可能だった証明書の事前入力とユーザー名取得機能の CLI がマルチコンテキストモードでも有効にできるようになりました。 変更された画面はありません。
リモート アクセス VPN のフラッシュ仮想化	9.6(2)	マルチ コンテキスト モードのリモート アクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザーのみに関連付けられ、該当ユーザー対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザー コンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次の画面が変更されました。**[Configuration]** > **[Context Management]** > **[Resource Class]** > **[Add Resource Class]** **[Configuration]** > **[Context Management]** > **[Security Contexts]**
マルチコンテキストデバイスでの AnyConnect クライアント プロファイルのサポート	9.6(2)	AnyConnect クライアント プロファイルがマルチコンテキストのデバイスでサポートされました。ASDM を使用して新しいプロファイルを追加するには、AnyConnect セキュア モビリティ クライアント リリース 4.2.00748 または 4.3.03013 以降が必要です。
マルチ コンテキスト モードの AnyConnect 接続のステートフル フェールオーバー	9.6(2)	マルチ コンテキスト モードで AnyConnect 接続のステートフル フェールオーバーがサポートされました。 変更された画面はありません。
マルチ コンテキスト モードでリモート アクセス VPN ダイナミック アクセス ポリシー（DAP）がサポートされました。	9.6(2)	マルチ コンテキスト モードで、コンテキストごとに DAP を設定できるようになりました。 変更された画面はありません。
マルチ コンテキスト モードでリモート アクセス VPN CoA（認可変更）がサポートされました。	9.6(2)	マルチ コンテキスト モードで、コンテキストごとに CoA を設定できるようになりました。 変更された画面はありません。

機能名	プラットフォームリリース	機能情報
マルチ コンテキスト モードで、リモート アクセス VPN のローカライズがサポートされました。	9.6(2)	ローカリゼーションがグローバルでサポートされました。複数のコンテキストで共有されるローカリゼーション ファイル セットは 1 つだけです。 変更された画面はありません。
IKEv2 のリモート アクセス VPN は、マルチ コンテキスト モードでサポートされています。	9.9(2)	リモート アクセス VPN は、IKEv2 のマルチ コンテキスト モードで構成できます。
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更された画面：**[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]**
HTTPS リソース管理	9.12(1)	リソースクラスの非 ASDM HTTPS セッションの最大数を設定できるようになりました。デフォルトでは、制限はコンテキストあたり最大 6 に設定でき、すべてのコンテキスト全体では最大 100 の HTTPS セッションを使用できます。 新規/変更されたコマンド：**limit-resource http** ASDM サポートはありません。



第 10 章

ハイ アベイラビリティのためのフェールオーバー

この章では、Cisco ASA のハイ アベイラビリティを達成するために、アクティブ/スタンドバイまたはアクティブ/アクティブ フェールオーバーを設定する方法について説明します。

フェールオーバーについて

フェールオーバーの設定では、専用フェールオーバー リンク（および任意でステート リンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブユニットおよびインターフェイスのヘルスがモニターされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。所定の条件に一致すると、フェールオーバーが行われます。

フェールオーバー モード

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバー モードをサポートします。各フェールオーバー モードには、フェールオーバーを判定および実行する独自の方式があります。

- アクティブ/スタンバイ フェールオーバーでは、一方のデバイスがアクティブユニットとしてトラフィックを通過させます。もう一方のデバイスはスタンバイユニットとなり、ア

クティブにトラフィックを通過させません。フェールオーバーが発生すると、アクティブユニットからスタンバイユニットにフェールオーバーし、そのスタンバイユニットがアクティブになります。シングルまたはマルチ コンテキスト モードでは、ASA のアクティブ/スタンバイ フェールオーバーを使用できます。

- アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つのフェールオーバー グループ に分割します。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。一方のグループは、プライマリ ASA でアクティブになるよう割り当てられます。他方のグループは、セカンダリ ASA でアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。

両方のフェールオーバー モードとも、ステートフルまたはステートレス フェールオーバーをサポートします。

フェールオーバー のシステム要件

この項では、フェールオーバー コンフィギュレーションにある ASAのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。 さらに、コンテナ インスタンスでは、同じリソース プロファイル属性を使用する必要があります。

  Firepower 9300 の場合、高可用性は同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシに SM-36、、および SM-44 を配置できます。SM-36 モジュール間、および SM-44 モジュール間に高可用性ペアを作成できます。

- インターフェイスの数とタイプが同じであること。

  プラットフォーム モードとの Firepower 4100/9300 シャーシFirepower 2100 では、フェールオーバー を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。フェールオーバーを有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でそのインターフェイスを変更してから、アクティブユニットで同じ変更を行います。 FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

- 同じモジュール（存在する場合）がインストールされていること。
- 同じ RAM がインストールされていること。

フェールオーバー コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェアイメージファイルおよびコンフィギュレーションファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- コンテキスト モードが同じであること（シングルまたはマルチ）。
- 単一モードの場合：同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。

  マルチコンテキスト モードでは、ファイアウォール モードはコンテキスト レベルで設定され、混合モードを使用できます。
- ソフトウェア バージョンが、メジャー（最初の番号）およびマイナー（2 番目の番号）ともに同じであること。ただし、アップグレードプロセス中は、異なるバージョンのソフトウェアを一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。
- 同じ AnyConnect イメージを持っていること。中断のないアップグレードを実行するときにフェールオーバー ペアのイメージが一致しないと、アップグレード プロセスの最後のリブート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。
- 同じ FIPS モードであること。
- （Firepower 4100/9300）同じフロー オフロード モードを使用し、両方とも有効または無効になっている。

ライセンス要件

フェールオーバー コンフィギュレーションの 2 台の装置は、ライセンスが同じである必要はありません。これらのライセンスは結合され、1 つのフェールオーバー クラスタ ライセンスが構成されます。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。シスコでは、フェールオーバーリンクまたはステートフルフェールオーバーリンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

⚠

注意 フェールオーバー リンクおよびステート リンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信を保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザー名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信を IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータインターフェイス（物理、サブインターフェイス、冗長、または EtherChannel）はいずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワークインターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバーリンク用にのみ使用できます（ステートリンク用としても使用できます）。ほとんどのモデルでは、以下で明示的に説明されていない限り、フェールオーバー用の管理インターフェイスを使用できません。

ASA は、ユーザー データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバー リンクやデータのために使用することもできません。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- 5506-X ～ 5555-X：管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。5506H-X は唯一の例外で、フェールオーバー リンクとして管理インターフェイスを使用できます。
- 5506H-X：フェールオーバー リンクとして管理 1/1 インターフェイスを使用できます。フェールオーバー用に設定した場合は、デバイスをリロードして変更を反映させる必要があります。この場合、管理プロセスに管理インターフェイスが必要であるため、ASA Firepower モジュールも使用できません。
- Firepower 4100/9300：統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。 フェールオーバー リンクに管理タイプのインターフェイスを使用することはできません。
- 他のすべてのモデル：1 GB インターフェイスは、フェールオーバーとステート リンクを組み合わせるには十分な大きさです。

フェールオーバー リンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください:

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットを検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

交替頻度は、ユニットのホールド時間と同じです（**failover polltime unit** コマンド）。

（注） 設定が大きく、ユニットのホールド時間が短い場合、メンバーインターフェイスを交互に切り替えると、セカンダリユニットの参加/再参加を防止できます。この場合、セカンダリユニットが参加するまで、メンバーインターフェイスの 1 つを無効にします。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASAのフェールオーバーインターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他のデバイスのないスイッチを使用する。

- イーサネット ケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASAは、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステートリンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

専用のインターフェイス

ステートリンク専用のデータインターフェイス（物理、冗長、または EtherChannel）を使用できます。専用のステートリンクの要件についてはフェールオーバー リンクのインターフェイス（328 ページ）、ステートリンクの接続についてはフェールオーバー リンクの接続 （329 ページ）を参照してください。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバー リンクとデータ リンクの中断の回避

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、Secure Firewall ASA はデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクの正常性が復元されるまで停止されます。

耐障害性フェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチ セットが 2 つの Secure Firewall ASA 間のフェールオーバー インターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の Secure Firewall ASA がアクティブになります。したがって、次の図で示されている次の 2 つの接続方式は推奨しません。

図 *46 :* 単一のスイッチを使用した接続：非推奨

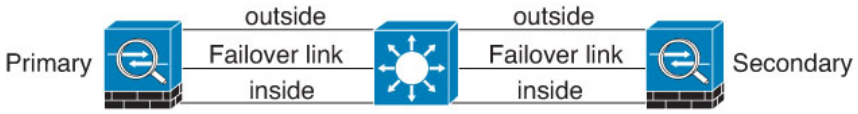
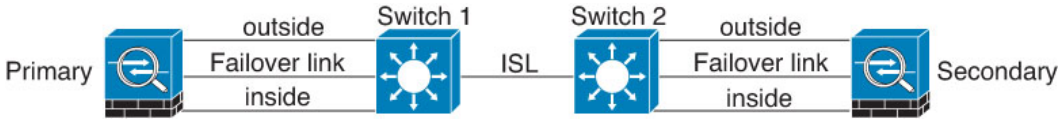


図 *47 : 2* つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *48 :* 異なるスイッチを使用した接続

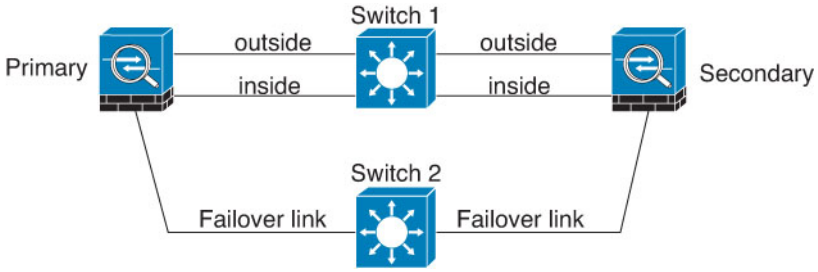
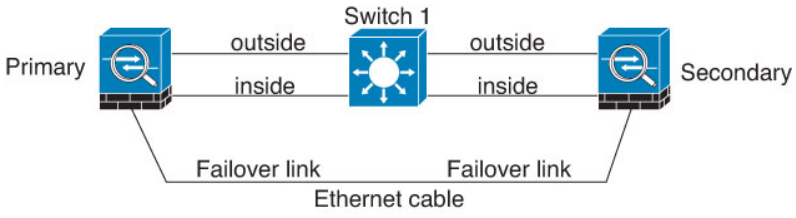


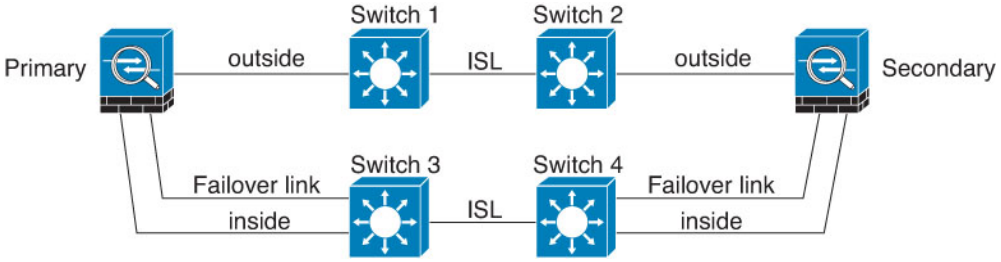
図 *49 :* ケーブルを使用した接続



シナリオ 3：推奨

Secure Firewall ASA データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *50 :* セキュア スイッチを使用した接続



シナリオ 4：推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバー リンクに冗長インターフェイスを使用します。

図 *51 :* 冗長インターフェイスを使用した接続

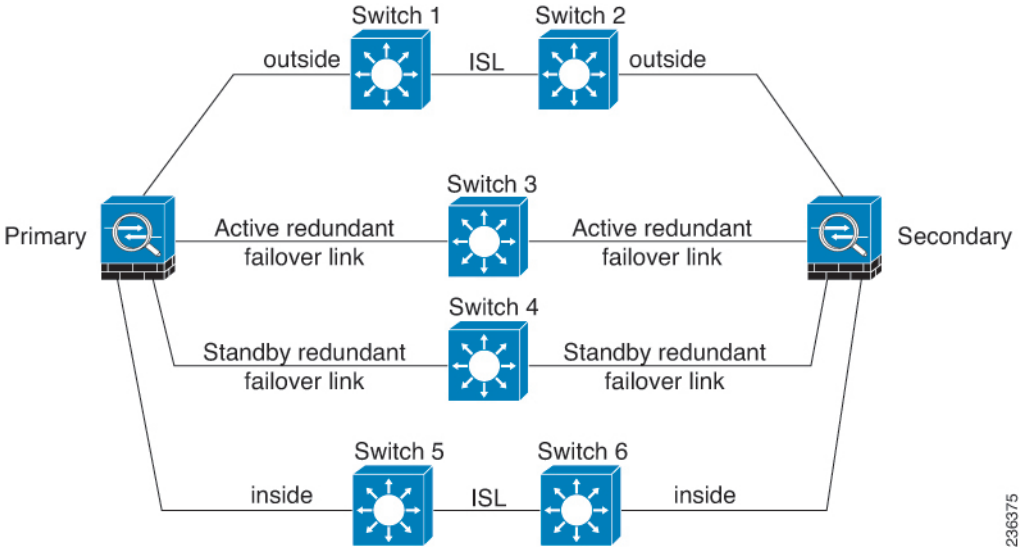
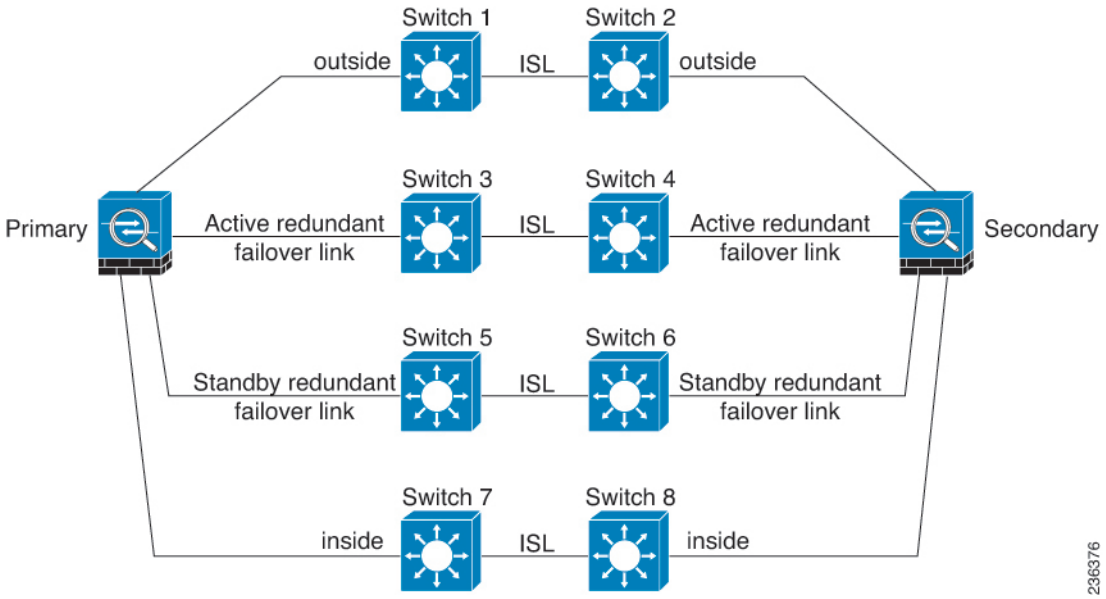


図 *52 : Inter-Switch Link*（*ISL*）を使用した接続



フェールオーバー の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） スタンバイ アドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステート リンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ フェールオーバー の場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. アクティブな装置は常にプライマリ装置の IP アドレスと MAC アドレスを使用します。
2. アクティブ装置が故障すると、スタンバイ装置は故障した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。

3. 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。Secure Firewall ASA は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

アクティブ/アクティブ IP アドレスと MAC アドレス

アクティブ/アクティブ フェールオーバーの場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. プライマリ装置は、フェールオーバー グループ 1 および 2 のコンテキストのすべてのインターフェイスに対して、アクティブおよびスタンバイ MAC アドレスを自動生成します。必要に応じて、たとえば、MAC アドレスの競合がある場合は、MAC アドレスを手動で設定できます。
2. 各装置は、そのアクティブ フェールオーバー グループにアクティブな IP アドレスと MAC アドレスを使用し、そのスタンバイ フェールオーバー グループにスタンバイ アドレスを使用します。たとえば、フェールオーバー グループ 1 でプライマリ装置がアクティブである場合、フェールオーバー グループ 1 のコンテキストでアクティブなアドレスを使用します。フェールオーバー グループ 2 のコンテキストではスタンバイであるため、スタンバイ アドレスを使用します。
3. 装置が故障すると、他の装置は故障したフェールオーバー グループの アクティブな IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
4. 故障した装置がオンラインに戻り、preempt オプションが有効になっている場合、フェールオーバー グループを再開します。

仮想 MAC アドレス

Secure Firewall ASA には、仮想 MAC アドレスを設定する複数の方法があります。1 つの方法のみ使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。手動の方法には、次で説明されている自動生成方法に加えて、インターフェイス モード **mac-address** コマンド、**failover mac address** コマンドが含まれ、アクティブ/アクティブ

フェールオーバーの場合は、フェールオーバー グループ モード **mac address** コマンドが含まれます。

マルチ コンテキスト モードでは、共有インターフェイスに仮想アクティブおよびスタンバイ MAC アドレスを自動的に生成するように ASA を設定でき、これらの割り当てはセカンダリユニットに同期されます（**mac-address auto** コマンドを参照してください）。共有以外のインターフェイスでは、アクティブ/スタンバイ モードの MAC アドレスを手動で設定することができます（アクティブ/アクティブ モードはすべてのインターフェイスに MAC アドレスを自動生成します）。

アクティブ/アクティブ フェールオーバーでは、仮想 MAC アドレスはデフォルト値またはインターフェイスごとに設定できる値のいずれかとともに常に使用されます。

ステートレス フェールオーバーとステートフル フェールオーバー

ASA は、アクティブ/スタンバイ モードとアクティブ/アクティブ モードの両方に対して、ステートレスとステートフルの 2 種類のフェールオーバーをサポートします。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）は VPN フェールオーバー サブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス フェールオーバーは、クライアントレス SSL VPN には推奨されません。

ステートレス フェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）は VPN フェールオーバー サブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス（標準）フェールオーバーは、クライアントレス SSL VPN には推奨できません。

ステートフル フェールオーバー

ステートフル フェールオーバーが有効な場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。アクティブ/アクティブ フェールオーバーの場合は、アクティブとスタンバイのフェールオーバー グループ間でこれが行われます。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ Secure Firewall ASAに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- HTTP 接続テーブル（HTTP 複製を有効にしない場合）。
- HTTP 接続状態（HTTP 複製が有効化されている場合）：デフォルトでは、ステートフル フェールオーバーが有効化されているときには、ASA はHTTPセッション情報を複製しません。HTTP レプリケーションを有効にすることをお勧めします。
- SCTP 接続状態ただし、SCTP インスペクションのステートフル フェールオーバーはベストエフォートです。フェールオーバー中、SACKパケットが失われると、失われたパケットが受信されるまで、新しいアクティブユニットはキューにある他のすべての順序が不正なパケットを破棄します。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションとピンホール。
- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティング グループに割り当てられている場合にだけ有効化されます。
- スタティックおよびダイナミック ルーティング テーブル：ステートフル フェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリ ユニットには最初にプライマリ ユニットをミラーリングするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIBテーブルのエポック番号が増加します。再コンバージェンス中に、OSPF およびEIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIBには新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。

(注) ルートは、アクティブ装置上のリンクアップまたはリンクダウンイベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定された DHCP サーバは、DHCP クライアントにアドレスを付与する前にアドレスが使用されていないことを確認するために ping を送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性がありません。
- Cisco IP SoftPhone セッション：コール セッション ステート情報がスタンバイ装置に複製されるため、Cisco IP SoftPhone セッションの実行中にフェールオーバーが起こっても、コールは実行されたままです。コールが終了すると、IP SoftPhone クライアントは Cisco Call Manager との接続を失います。これは、CTIQBE ハングアップ メッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhone クライアントでは、一定の時間内に CallManager からの応答が受信されない場合、CallManager に到達できないものと判断されて登録が解除されます。
- RA VPN：リモート アクセス VPN エンドユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバー プロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ Secure Firewall ASAに渡されません。

- ユーザー認証（uauth）テーブル
- TCP ステート バイパス接続
- マルチキャスト ルーティング。
- ASA FirePOWER モジュールなどのモジュールのステート情報。
- 選択された次のクライアントレス SSL VPN 機能：
  - スマート トンネル
  - ポート転送
  - プラグイン
  - Java アプレット
  - IPv6 クライアントレスまたは Anyconnect セッション

• Citrix 認証（Citrix ユーザーはフェールオーバー後に再認証が必要です）

フェールオーバーのブリッジ グループ要件

ブリッジグループを使用する場合は、フェールオーバーに関して特別な考慮事項があります。

アプライアンス、ASAv のブリッジグループ必須要件

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチ ポート モードに応じて次の回避策のいずれかを設定できます。

- アクセス モード：スイッチで STP PortFast 機能をイネーブルにします。

```
interface interface_id
  spanning-tree portfast
```

  PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- トランク モード：EtherType アクセス ルールを使用して、ブリッジグループのメンバー インターフェイス上の ASA の BPDU をブロックします。

```
access-list id ethertype deny bpdu
access-group id in interface name1
access-group id in interface name2
```

  BPDU をブロックすると、スイッチの STP はディセーブルになります。ネットワーク レイアウトで ASA を含むループを設定しないでください。

上記のオプションのどちらも使用できない場合は、フェールオーバー機能または STP の安定性に影響する、推奨度の低い次の回避策のいずれかを使用できます。

- インターフェイス モニタリングをディセーブルにします。
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスのホールド時間よりも速く収束するように、STP タイマーを減らします。

フェールオーバーのヘルス モニターリング

ASAは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニターします。この項では、各装置の状態を判断するために、ASAがテストを実行する方法について説明します。

装置のヘルス モニターリング

ASAは、hello メッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで 3 回連続して hello メッセージを受信しなかったときは、フェールオーバー リンクを含む各データ インターフェイスでLANTEST メッセージを送信し、ピアが応答するかどうかを確認します。 FirePOWER 9300 および4100 シリーズでは、hello メッセージよりも信頼性の高い Bidirectional Forwarding Detection（BFD）を有効にできます。ASAが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- ASAがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバーリンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
- ASAがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

最大 1025 のインターフェイスを監視できます（マルチコンテキスト モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニターする必要があります。たとえば、マルチコンテキストモードでは、共有インターフェイスを監視するように1つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニターリングによる利点を得ることができます）。

ユニットは、モニター対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に（デフォルト）、インターフェイステストを実行します。（この時間を変更するには、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Criteria]** > **[Failover Poll Times]** を参照してください。）1 つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、ASAはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**[設定（Configuration）]**> **[デバイス管理（Device Management）]** >**[ハイアベイラビリティとスケーラビリティ（High Availability and Scalability）]** > **[フェールオーバー（Failover）]** > **[基準（Criteria）]** > **[インターフェイスポリシー（Interface Policy）]** を参照）、さらに、アクティ

ブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障した ASA は、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

ASA FirePOWER モジュールがある場合、ASA はバックプレーン インターフェイスを介してモジュールの健全性もモニターします。モジュールの障害は装置の障害と見なされ、フェールオーバーがトリガーされます。この設定は設定可能です。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASA は IPv4 を使用してヘルス モニターリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、ASAは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニターリング テストを実行します。ブロードキャスト pingテストの場合、ASA はIPv6 全ノードアドレス（FE02::1）を使用します。

（注） 障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

インターフェイス テスト

ASAでは、次のインターフェイス テストが使用されます。各テストの時間はデフォルトで約 1.5 秒、またはフェールオーバー インターフェイスの保留時間の 1/16 です（**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Criteria]** > **[Failover Poll Times]** を参照）。

1. リンクアップ/ダウンテスト：インターフェイス ステータスのテストです。リンクアップ/ダウン テストでインターフェイスがダウンしていることが示された場合、ASA は障害が発生し、テストが停止したと見なします。ステータスがアップの場合、ASAはネットワーク アクティビティを実行します。
2. ネットワーク アクティビティテスト：ネットワークの受信アクティビティのテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はARP テストを開始します。
3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、イン

ターフェイスは動作していると見なされます。ユニットが ARP 応答を受信しない場合、ASAは、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はブートストラップ ping テストを開始します。

4. ブロードキャストPingテスト：ping応答が正しいかどうかをテストします。各ユニットがブロードキャストpingを送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARPテストを使用してテストが再開されます。両方の装置が ARP およびブロードキャスト ping テストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理上ダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー 時間

Firepower ハイアベイラビリティペアでは、次のイベントでフェールオーバーがトリガーされます。

- アクティブユニットの 50% を超える Snort インスタンスがダウンした場合
- アクティブユニットのディスク容量使用率が 90% を超えた場合
- アクティブユニットで **no failover active** コマンドが実行された場合、またはスタンバイユニットで **failover active** コマンドが実行された場合

- アクティブユニットで障害が発生したインターフェイスの数がスタンバイユニットよりも多くなった場合
- アクティブデバイスのインターフェイス障害が設定されたしきい値を超えた場合

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。デフォルト値を変更するには、フェールオーバーが発生するしきい値として、障害が発生したインターフェイスの数またはモニター対象インターフェイスの割合を設定します。アクティブデバイスでしきい値を超えると、フェールオーバーが発生します。スタンバイデバイスでしきい値を超えると、ユニットが **Fail** 状態に移行します。

デフォルトのフェールオーバー条件を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

表 *17:*

コマンド	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	デフォルトのフェールオーバー基準を変更します。 インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 250 を設定できます。 インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

（注） CLI または ASDM を使用して手動でフェールオーバーした場合、もしくは ASA をリロードした場合、フェールオーバーはすぐに開始され、次に示すタイマーの影響は受けません。

表 *18 : ASA*

フェールオーバー条件	最小	デフォルト	最大数
アクティブユニットの電源の喪失、ハードウェアのダウン、ソフトウェアのリロードまたはクラッシュにより、モニター対象インターフェイスまたはフェールオーバーリンクで hello メッセージを受信しなくなる。	800 ミリ秒	15 秒	45 秒
アクティブ ユニット メイン ボード インターフェイス リンクがダウンする。	500 ミリ秒	5 秒	15 秒

フェールオーバー条件	最小	デフォルト	最大数
アクティブ ユニットの 4GE モジュール インターフェイス リンクがダウンする。	2 秒	5 秒	15 秒
アクティブ ユニット FirePOWER モジュールは失敗する。	2 秒	2 秒	2 秒
アクティブ ユニットのインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

設定の同期

フェールオーバーには、さまざまなタイプのコンフィギュレーション同期があります。

コンフィギュレーションの複製の実行

コンフィギュレーションの複製は、フェールオーバーペアの一方または両方のデバイスのブート時に実行されます。

アクティブ/スタンバイ フェールオーバーでは、コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。

アクティブ/アクティブ フェールオーバーでは、起動ユニットのプライマリまたはセカンデリ指定に関係なく、2番目に起動したユニットは、最初に起動したユニットから実行コンフィギュレーションを取得します。両方のユニットの起動後、システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態であるユニットから複製されます。

スタンバイ/セカンドユニットが初期スタートアップを完了すると、実行コンフィギュレーションを削除し（アクティブ ユニットとの通信に必要な **failover** コマンドを除く）、アクティブ ユニットはコンフィギュレーション全体をスタンバイ/セカンド ユニットに送信します。複製が開始されると、アクティブ ユニットの ASA コンソールに「Beginning configuration replication: Sending to mate,」というメッセージが表示され、完了すると ASA に「End Configuration Replication to mate.」というメッセージが表示されます。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

コンフィギュレーションを受信する装置の場合、コンフィギュレーションは実行メモリにだけ存在します。コンフィギュレーションをフラッシュ メモリに保存する必要があります。たとえば、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブ状態であるユニット上のシステム実行スペースに **write memory all** コマンドを入力します。コマンドはピア装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。

（注） 複製中、コンフィギュレーションを送信しているユニット上に入力されたコマンドは、ピアユニットに正常に複製されず、コンフィギュレーションを受信するユニット上に入力されたコマンドは、受信したコンフィギュレーションによって上書きできます。コンフィギュレーションの複製処理中には、フェールオーバーペアのどちらの装置にもコマンドを入力しないでください。

ファイルの複製

コンフィギュレーションの同期は次のファイルと構成コンポーネントを複製しません。したがって、これらのファイルが一致するように手動でコピーする必要があります。

- AnyConnect イメージ
- CSD イメージ
- AnyConnect プロファイル

  ASA では、フラッシュ ファイル システムに保存されたファイルではなく、cache:/stc/profiles に保存された AnyConnect クライアント ファイルのキャッシュ済みファイルが使用されます。AnyConnect クライアント プロファイルをスタンバイ装置に複製するには、次のいずれかを実行します。

  - アクティブ装置で **write standby** コマンドを入力します。
  - アクティブ装置でプロファイルを再適用します。
  - スタンバイ装置をリロードします。

- ローカル認証局（CA）
- ASA イメージ
- ASDM イメージ

コマンドの複製

起動した後、アクティブユニットで入力したコマンドはただちにスタンバイユニットに複製されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

アクティブ/アクティブ フェールオーバーでは、システム実行スペースに入力した変更は、フェールオーバー グループ 1 がアクティブ状態である装置から複製されます。

コマンドの複製を行うのに適切な装置上で変更を入力しなかった場合は、コンフィギュレーションは同期されません。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- すべてのコンフィギュレーション コマンド（**mode**、**firewall**、および **failover lan unit** を除く）
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA に複製されないコマンドは、次のとおりです。

- すべての形式の **copy** コマンド（**copy running-config startup-config** を除く）
- すべての形式の **write** コマンド（**write memory** を除く）
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ Secure Firewall ASA に引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

（注） マルチ コンテキスト モードでは、ASA は装置全体（すべてのコンテキストを含む）のフェールオーバーを行いますが、各コンテキストを個別にフェールオーバーすることはできません。

プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリ ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニットが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ ユニットが常にアクティブ ユニットになります。

- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ ユニットの MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。マルチコンテキストモードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ ユニットが行うアクション、スタンバイ ユニットが行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *19*：フェールオーバー イベント

障害イベント	ポリシー（Policy）	アクティブユニットのアクション	スタンバイユニットのアクション	注意
アクティブユニットが故障（電源またはハードウェア）	フェールオーバー	適用対象外	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであったユニットの復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。

障害イベント	ポリシー（Policy）	アクティブユニットのアクション	スタンバイユニットのアクション	注意
スタンバイ ユニットが故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	適用対象外	スタンバイ ユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー リンクに故障とマークする	フェールオーバー リンクに故障とマークする	フェールオーバー リンクがダウンしている間、ユニットはスタンバイ ユニットにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる フェールオーバー リンクに故障とマークする	アクティブになる フェールオーバー リンクに故障とマークする	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置がアクティブになります。
ステート リンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
アクティブユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ ユニットにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイ ユニットが故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブユニットはフェールオーバーを行いません。

アクティブ/アクティブ フェールオーバーの概要

この項では、アクティブ/アクティブ フェールオーバーについて説明します。

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。フェールオーバー グループをプライマリ ASA でアクティブに割り当て、フェールオーバー グループ 2 をセカンデリ ASA でアクティブに割り当てることができます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。たとえば、インターフェイス障害パターンに応じて、フェールオーバー グループ 1 をセカンデリ ASA にフェールオーバーし、続いてフェールオーバー グループ 2 をプライマリ ASA にフェールオーバーすることができます。このイベントは、プライマリ ASA でフェールオーバー グループ 1 のインターフェイスがダウンしたがセカンデリではアップしており、セカンデリ ASA でフェールオーバー グループ 2 のインターフェイスがダウンしたがプライマリ ASA ではアップしている場合に発生する可能性があります。

管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを 1 つ追加し、それをフェールオーバー グループ 2 に割り当てることです。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

（注） 必要に応じて両方のフェールオーバー グループを 1 つの ASA に割り当てることもできますが、この場合、アクティブな ASA を 2 つ持つというメリットはありません。

フェールオーバー グループのプライマリ/セカンデリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

- ペアが同時に起動したときに、プライマリ装置が実行コンフィギュレーションを提供します。
- コンフィギュレーションの各フェールオーバー グループは、プライマリまたはセカンダリ装置プリファレンスが設定されます。プリエンプションで使用すると、このプレファレンスはフェールオーバー グループが起動後に正しいユニットで実行されるようにします。プリエンプションがない場合、両方のグループは最初に起動したユニットで動作します。

起動時のフェールオーバー グループのアクティブ装置の決定

フェールオーバー グループがアクティブになる装置は、次のように決定されます。

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバー グループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバー グループがアクティブ状態）の場合に装置がブートされると、フェールオーバー グループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバー グループのプライマリ プリファレンスまたはセカンダリ プリファレンスには関係ありません。
  - フェールオーバーが発生した。
  - 手動でフェールオーバーを強制実行した。
  - フェールオーバーグループのプリエンプションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバーグループはその装置上で自動的にアクティブになります。

フェールオーバー イベント

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリユニットで両方のフェールオーバーグループをアクティブと指定し、フェールオーバーグループ 1 が故障すると、フェールオーバーグループ 2 はプライマリユニットでアクティブのままですが、フェールオーバーグループ 1 はセカンダリユニットでアクティブになります。

フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1 つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ フェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 *20 :* フェールオーバー イベント

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
装置で電源断またはソフトウェア障害が発生した	フェールオーバー	スタンバイになる 故障とマークする	アクティブになる アクティブに故障とマークする	フェールオーバーペアの装置が故障すると、その装置のアクティブフェールオーバー グループはすべて故障とマークされ、ピア装置のフェールオーバー グループがアクティブになります。
アクティブ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブ グループに故障とマークする	アクティブになる	なし。
スタンバイ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイ グループに故障とマークする	スタンバイ フェールオーバー グループが故障とマークされている場合、インターフェイス フェールオーバー障害しきい値を超えても、アクティブ フェールオーバー グループはフェールオーバーを行いません。
以前にアクティブであったフェールオーバー グループの復旧	フェールオーバーなし	動作なし	動作なし	フェールオーバー グループのプリエンプションが設定されている場合を除き、フェールオーバー グループは現在の装置でアクティブのままです。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。

障害イベント	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	適用対象外	適用対象外	各装置で、フェールオーバーリンクが故障とマークされます。フェールオーバーリンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。

フェールオーバーのライセンス

ほとんどのモデルでは、フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	• アクティブ/スタンバイ：両方のユニットの Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
Asa 5525- x ～ asa 5555-X	• 基本ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	ASAv のフェールオーバー ライセンス （165 ページ）を参照してください。

モデル	ライセンス要件
Firepower 1010	両方のユニットの Security Plus ライセンス。Firepower 1010 のフェールオーバー ライセンス （166 ページ）を参照してください。
Firepower 1100	Firepower 1100 のフェールオーバー ライセンス （166 ページ）を参照してください。
Firepower 2100	Firepower 2100 のフェールオーバー ライセンス （168 ページ）を参照してください。
Firepower 4100/9300	Firepower 4100/9300のフェールオーバーライセンス （170 ページ）を参照してください。
ISA 3000	両方のユニットの Security Plus ライセンス。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

フェールオーバー のガイドライン

コンテキスト モード

- アクティブ/アクティブ モードは、マルチ コンテキスト モードでのみサポートされます。
- マルチ コンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。

モデルのサポート

- ASA 5506W-X：内部 GigabitEthernet 1/9 インターフェイスのインターフェイス モニタリングを無効にする必要があります。これらのインターフェイスは、デフォルトのインターフェイス モニターリング チェックを実行するために通信することができないため、予期されたインターフェイス通信の障害により、スイッチがアクティブからスタンバイに切り替えられ、元に戻ります。
- Firepower 1010：
  - フェールオーバーを使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユ

ニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェールオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLANインターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。理論的には、1つのスイッチ ポートをVLANに配置して、フェールオーバー を正常に使用することができますが、代わりに物理ファイアウォール インターフェイスを使用する設定の方が簡単です。

- ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。

- FirePOWER 9300：シャーシ間フェールオーバーを使用して最良の冗長性を確保することを推奨します。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の ASAv では、レイヤ 2 接続が必要なため、通常の フェールオーバー はサポートされません。代わりに、パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー（381 ページ）を参照してください。
- ASA FirePOWER モジュールはフェールオーバーを直接サポートしていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールが、その転送の時点からトラフィックの検査を開始します。古いインスペクションのステートは転送されません。

  フェールオーバーの動作の整合性を保つために、ハイアベイラビリティな ASA ペアの ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

> **注** ASA FirePOWER モジュールを設定する前に、フェールオーバー ペアを作成します。モジュールが両方のデバイスにすでに設定されている場合は、フェールオーバー ペアを作成する前にスタンバイ デバイスのインターフェイスの設定をクリアします。スタンバイ デバイスの CLI から、 **clear configure interface** コマンドを入力します。

ハイ アベイラビリティのための ASAv フェールオーバー

ASAv を使用してフェールオーバー ペアを作成する場合は、データ インターフェイスを各 ASAv に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASAv に追加されると、ASAv コンソールにエラーが表示される可能性があります。また、フェールオーバー機能にも影響が出ることがあります。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行している接続済みスイッチ ポートが、トポロジの変化を検出すると 30 ～ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング ステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

  interface *interface_id* **spanning-tree portfast**

  この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- ASA フェールオーバーペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。

- すべてのコンテキストにわたり、1 台の装置の最大 1025 のインターフェイスをモニタできます。

- アクティブ/スタンバイ フェールオーバー と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニターすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

- アクティブ/アクティブ フェールオーバーでは、同じコンテキスト内の 2 つのインターフェイスを同じ ASR グループ内で設定することはできません。

- アクティブ/アクティブ フェールオーバーでは、最大 2 つのフェールオーバー グループを定義できます。

- アクティブ/アクティブ フェールオーバーでフェールオーバー グループを削除する場合は、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には常に管理コンテキストが含まれます。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ 1 になります。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

- フェールオーバーの直後に、syslog メッセージの送信元アドレスが数秒間フェールオーバー インターフェイス アドレスになります。

- 評価モードで HA フェールオーバー暗号化を設定すると、システムは暗号化に DES を使用します。エクスポート準拠アカウントを使用してデバイスを登録すると、デバイスはリブート後に AES を使用します。したがって、アップグレードのインストール後など、何

らかの理由でシステムがリブートすると、ピアは通信できなくなり、両方のユニットがアクティブユニットになります。デバイスを登録するまで、暗号化を設定しないことを推奨します。評価モードで暗号化を設定する場合は、デバイスを登録する前に暗号化を削除することを推奨します。

- フェールオーバーでSNMPv3を使用する場合、フェールオーバーユニットを交換すると、SNMPv3ユーザは新しいユニットにレプリケートされません。ユーザを新しいユニットに強制的にレプリケートするには、SNMPv3ユーザをアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます。アクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してスタンバイユニットに直接入力することにより、各ユーザを再設定します。
- ASAは、SNMP クライアントのエンジンデータをピアと共有しません。
- 非常に多数のアクセスコントロールルールとNATルールがある場合、設定のサイズによって効率的な設定のレプリケーションが妨げられる可能性があり、その結果、スタンバイユニットがスタンバイ準備完了状態に達するまでの時間が長くなります。これは、コンソールまたは SSH セッションを介したレプリケーション中にスタンバイユニットに接続する機能にも影響を与える可能性があります。設定のレプリケーションのパフォーマンスを向上させるには、**asp rule-engine transactional-commit access-group** および **asp rule-engine transactional-commit nat** コマンドを使用して、アクセスルールと NAT の両方でトランザクションコミットを有効にします。

フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一のインターフェイス障害でフェールオーバーが行われます。
- インターフェイスのポーリング時間は 5 秒です。
- インターフェイスのホールド時間は 25 秒です。
- 装置のポーリング時間は 1 秒です。
- 装置のホールド時間は 15 秒です。
- 仮想 MAC アドレスはマルチコンテキストモードで無効化されていますが。
- すべての物理インターフェイスをモニターリングします。

アクティブ/スタンバイ フェールオーバーの設定

アクティブ/スタンバイ フェールオーバーを設定するには、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。その他すべての設定をプライマリ装置でのみ行った後、セカンデリ装置に設定を同期させます。

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/スタンバイ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1 **[Wizards]** > **[High Availability and Scalability]** を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 [Failover Peer Connectivity and Compatibility] 画面で、ピア装置の IP アドレスを入力します。このアドレスは、ASDM アクセスがイネーブルになっているインターフェイスである必要があります。

デフォルトでは、ピア アドレスは ASDM 管理インターフェイスのスタンバイ アドレスに割り当てられます。

ステップ 3 [LAN Link Configuration] 画面で次のように設定します。

- [インターフェイス（Interface）]：物理インターフェイス ID、サブインターフェイス ID、冗長インターフェイス ID、または EtherChannel インターフェイス ID を指定できます。Firepower 1010 では、インターフェイスはファイアウォール インターフェイス ID です。スイッチ ポート ID または VLAN ID を指定することはできません。ASA 5506H-X の場合に限り、管理 1/1 インターフェイスをフェールオーバー リンクとして指定できます。その場合は、設定を保存してからデバイスをリロードする必要があります。デバイスをリロードした後は、このインターフェイスと ASA FirePOWER モジュールの両方をフェールオーバーに使用できなくなります。ASA FirePOWER モジュールには管理用インターフェイスが必要であり、そのインターフェイスは 1 つの機能にのみ使用できます。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。
- [Active IP Address]：この IP アドレスは、未使用のサブネット上にある必要があります。このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。
- （オプション）[Communications Encryption]：フェールオーバー リンクの通信を暗号化します。**注**：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます（フェールオーバーの設定変更 （367ページ）を参照）。

ステップ 4 ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address]：この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上にある必要があります。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。

ステップ 5 [Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。

指定された時間が経過した後に、ウィザードはセカンデリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンデリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。
- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting *xx* more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

アクティブ/アクティブ フェールオーバーの設定

ここでは、アクティブ/アクティブ フェールオーバーの設定方法について説明します。

High Availability and Scalability Wizard を使用して、手順を踏んでアクティブ/アクティブ フェールオーバー コンフィギュレーションを作成することができます。

手順

ステップ 1 **[Wizards]** > **[High Availability and Scalability]** を選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 [Failover Peer Connectivity and Compatibility Check] 画面では、ピアの IP アドレスは、ASDM アクセスが有効になっているインターフェイスである必要があります。

デフォルトでは、ピア アドレスは、ASDM の接続先インターフェイスのスタンバイ アドレスに割り当てられます。

ステップ 3 [Security Context Configuration] 画面では、ウィザード内でマルチ コンテキスト モードに変換した場合、管理コンテキストのみが表示されます。ウィザードを終了した後に他のコンテキストを追加できます。

ステップ 4 [LAN Link Configuration] 画面で次のように設定します。

- [Interface]：物理インターフェイス ID、サブインターフェイス ID、冗長インターフェイス ID、または EtherChannel インターフェイス ID を指定できます。ASA 5506H-X の場合に限り、管理 1/1 インターフェイスをフェールオーバー リンクとして指定できます。その場合は、設定を保存してからデバイスをリロードする必要があります。デバイスをリロードした後は、このインターフェイスと ASA FirePOWER モジュールの両方をフェールオーバーに使用できなくなります。ASA FirePOWER モジュールには管理用インターフェイスが必要であり、そのインターフェイスは 1 つの機能にのみ使用できます。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。
- [Active IP Address]：この IP アドレスは、未使用のサブネット上にある必要があります。このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。
- （オプション）[Communications Encryption]：フェールオーバー リンクの通信を暗号化します。**注**：秘密キーの代わりに、IPsec 事前共有キーを使用することをお勧めします。これはウィザードを終了した後に設定できます（フェールオーバーの設定変更 （367ページ）を参照）。

ステップ 5 ステートフル フェールオーバー用に別のインターフェイスを選択する場合は、[State Link Configuration] 画面で次の設定を行います。

- [Active IP Address]：この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上にある必要があります。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。
- [Standby IP Address]：この IP アドレスは、アクティブ IP アドレスと同じネットワーク上にある必要があります。

ステップ 6 [Finish] をクリックすると、ウィザードは [Waiting for Config Sync] 画面を表示します。

指定された時間が経過した後に、ウィザードはセカンデリ装置にフェールオーバー設定を送信し、フェールオーバー設定が完了したことを示す情報画面が表示されます。

- フェールオーバーがセカンデリ装置でイネーブルになっているかどうかわからない場合は、指定した時間だけ待ちます。
- フェールオーバーがすでにイネーブルなことがわかっている場合は、[Skip configuring peer] をクリックします。

- セカンダリ装置でフェールオーバーがイネーブルでないことがわかっている場合は、[Stop waiting *xx* more seconds] をクリックすると、フェールオーバーのブートストラップ設定はすぐにセカンダリ装置に送信されます。

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、フェールオーバーのデフォルト（356ページ）を参照してください。アクティブ/アクティブ モードでは、ほとんどの条件をフェールオーバー グループごとに設定します。ここでは、アクティブ/アクティブ モードでのフェールオーバー グループごとのHTTP複製のイネーブル化について説明します。アクティブ/スタンバイ モードでHTTP複製を設定する場合は、フェールオーバーの設定変更（367ページ）を参照してください。

始める前に

- マルチ コンテキスト モードのシステム実行スペースで次の設定を行います。
- ユニットのヘルス モニターリングの Bidirectional Forwarding Detection（BFD）については次の制限を参照してください。
  - FirePOWER 9300 および 4100 のみ
  - アクティブ/スタンバイのみ
  - ルーテッド モードのみ

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** の順に選択します。

ステップ 2 スタンバイ装置またはコンテキストのコンフィギュレーションを直接変更できないようにするには、[Setup] タブをクリックし、[Disable configuration changes on the standby unit] チェック ボックスをオンにします。

デフォルトでは、スタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。

ステップ 3 [BFD Health Check] で、[Manage] をクリックして、フェールオーバーのヘルス検出に使用するBFD テンプレートを定義します。CPU の使用率が高い場合、通常のユニットのモニターリン

グにより誤ってアラームが発生する可能性があります。BFD メソッドは分散されていてるため、CPU の使用率が高い場合でも動作に影響はありません。

[Configuration] > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Template]** ページが開きます。[Add] をクリックして、シングルホップテンプレートを作成します。マルチホップはサポートされていません。間隔の設定には、ミリ秒を指定できます。マイクロ秒はサポートされていません。テンプレートの詳細については、BFDテンプレートの作成（891ページ）を参照してください。

ステップ 4 [Criteria] タブをクリックします。

ステップ 5 装置のポーリング時間を設定します。

[Failover Poll Times] 領域で、次を設定します。

- [Unit Failover]：装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。
- [Unit Hold Time]：装置がフェールオーバー リンク上で Hello メッセージを受信する必要がある時間（この時間に受信しなかった場合は、装置がピアの障害のテストプロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。

（注） このペインの他の設定はアクティブ/スタンバイ モードにのみ適用されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに残りのパラメータを設定する必要があります。

ステップ 6 （アクティブ/アクティブ モードのみ）[Active/Active] タブをクリックし、フェールオーバー グループを選択して [Edit] をクリックします。

ステップ 7 （アクティブ/アクティブ モードのみ）プリエンプションでの使用時にフェールオーバー グループの優先するロールを変更するには、[Primary] または [Secondary] をクリックします。

ウィザードを使用した場合、フェールオーバー グループ 1 はプライマリ装置に割り当てられ、フェールオーバー グループ 2 はセカンダリ装置に割り当てられます。標準以外の設定が必要な場合は、別の装置を優先するように指定できます。これらの設定は、プリエンプション処理の設定と併用してのみ使用されます。グループの primary または secondary の設定にかかわらず、両方のフェールオーバー グループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。

ステップ 8 （アクティブ/アクティブ モードのみ）フェールオーバー グループ プリエンプションを設定するには、[Preempt after booting with optional delay of] チェック ボックスをオンにします。

グループの primary または secondary の設定にかかわらず、両方のフェールオーバー グループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。

オプションの delay 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ～ 1200 です。

手動でフェールオーバーすると、プリエンプション処理のオプションが無視されます。

（注） ステートフルフェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

ステップ 9 [Interface Policy] を設定します。

- [Number of failed interfaces that triggers failover]：フェールオーバーをトリガーするために必要な障害が発生したインターフェイスの具体的な数を 1 ～ 250 で定義します。障害が発生したモニター対象インターフェイスの数が指定した値を超えると、ASA はフェールオーバーします。
- [Percentage of failed interfaces that triggers failover]：フェールオーバーをトリガーするために必要な障害が発生した設定済みインターフェイスの割合を定義します。障害が発生したモニター対象インターフェイスの数が設定した割合を超えると、ASA はフェールオーバーします。

（注） [Use system failover interface policy] オプションは使用しないでください。現時点ではグループごとのポリシーのみが設定できます。

ステップ 10 （アクティブ/スタンバイ モード）インターフェイスのポーリング時間を設定します。

[Failover Poll Time] 領域で、次を設定します。

- **Monitored Interfaces**：インターフェイスのポーリング時間を指定します。ピアに hello パケットを送信するまで待機する時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。デフォルトは 5 秒です。
- [Link State]：デフォルトでは、フェールオーバーのペアの ASA では、インターフェイスのリンク ステートが 500 ミリ秒ごとに確認されます。polltime はカスタマイズできます。たとえば、polltime を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。範囲は 300 ～ 799 ミリ秒です。
- **Interface Hold Time**：ピア ユニットからの最後に受信した hello メッセージとインターフェイステストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイス テストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、polltime の5倍です。polltime の 5 倍よりも短い holdtime 値は入力できません。

  インターフェイステストを開始するまでの時間（y）を計算するには、次のようにします。

  1. x = (*holdtime*/*polltime*)/2、最も近い整数に丸められます。（.4 以下は切り下げ、.5 以上は切り上げ。）
  2. y = x**polltime*

  たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。

アクティブ/アクティブ モードの場合、[Add/Edit Failover Group] ダイアログボックスでインターフェイス ポーリング時間を設定します。

ステップ 11 （アクティブ/アクティブ モードのみ）HTTP 複製をイネーブルにするには、[Enable HTTP Replication] チェック ボックスをオンにします。

セッションの複製レートについては、「フェールオーバーの設定変更（367 ページ）」の項を参照してください。

（注） フェールオーバーを使用しているときに、スタンバイ装置から HTTP フローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 12 仮想 MAC アドレスを設定します。

- アクティブ/スタンバイ モード：[MAC Addresses] タブをクリックし、[Add] をクリックします。

  [Add/Edit Interface MAC Address] ダイアログボックスが表示されます。

- アクティブ/アクティブ モード：[Active/Active] [タブの下部に移動します。

他の方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

a) [Physical Interface] ドロップダウンリストからインターフェイスを選択します。
b) [Active MAC Address] フィールドに、アクティブ インターフェイスの新しい MAC アドレスを入力します。
c) [Standby MAC Address] フィールドに、スタンバイ インターフェイスの新しい MAC アドレスを入力します。
d) [OK] をクリックします。（アクティブ/アクティブ モードのみ）再度 [OK] をクリックします。

ステップ 13 [Apply] をクリックします。

インターフェイス モニターリングの設定およびスタンバイ アドレスの設定

デフォルトでは、すべての物理インターフェイス、または Firepower 1010 の場合、すべての VLAN インターフェイス、および ASA にインストールされるすべてのハードウェアまたはソフトウェアモジュール（ASA FirePOWER モジュールなど）でモニタリングが有効になっています。インターフェイス モニタリングの場合、Firepower 1010 スイッチ ポートが対象です。

重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。

装置ごとに最大 1025 のインターフェイスをモニターできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。

ウィザードでスタンバイ IP アドレスを設定しなかった場合は、手動で設定できます。

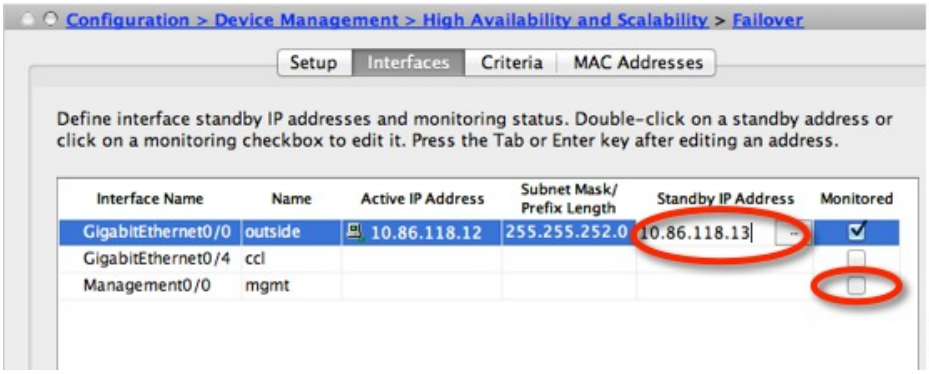
始める前に

マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

手順

ステップ 1 シングル モードでは、**[Configuration]** > **[Device Management]** > **[High Availability]** > **[Failover]** > **[Interfaces]** の順に選択します。

マルチ コンテキスト モードでは、コンテキスト内で [Configuration] > [Device Management] > [Failover] > [Interfaces] を選択します。



設定されているインターフェイスのリストが、ASA FirePOWER モジュールなどのすべてのインストール済みのハードウェア/ソフトウェアモジュールとともに表示されます。[Monitored] カラムに、フェールオーバー基準の一部としてインターフェイスがモニターされているかどうかが表示されます。モニターされている場合は、[Monitored] チェック ボックスがオンになっています。

特定のハードウェア/ソフトウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニターリングを無効化できます。

各インターフェイスの IP アドレスが [Active IP Address] カラムに表示されます。インターフェイスのスタンバイ IP アドレスが設定されている場合は、[Standby IP address] カラムに表示されます。フェールオーバー リンクおよびステート リンクについては IP アドレスは表示されません。これらのアドレスはこのタブから変更できません。

ステップ 2 表示されているインターフェイスのモニターリングをディセーブルにするには、インターフェイスの [Monitored] チェックボックスをオフにします。

ステップ 3 表示されているインターフェイスのモニターリングをイネーブルにするには、インターフェイスの [Monitored] チェックボックスをオンにします。

ステップ 4 スタンバイ IP アドレスを持っていない各インターフェイスに対して、[Standby IP Address] フィールドをダブルクリックしてフィールドに IP アドレスを入力します。

ポイントツーポイント接続に 31 ビット サブネット マスクを使用する場合、スタンバイ IP アドレスを設定しないでください。

ステップ 5 [Apply] をクリックします。

非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）

アクティブ/アクティブ フェールオーバーでの実行中に、ピア装置を経由して開始された接続に対する返送パケットを、装置が受信する場合があります。そのパケットを受信する ASA にはそのパケットの接続情報がないために、パケットはドロップされます。このドロップが多く発生するのは、アクティブ/アクティブ フェールオーバー ペアの 2 台の ASA が異なるサービス プロバイダに接続されており、アウトバウンド接続に NAT アドレスが使用されていない場合です。

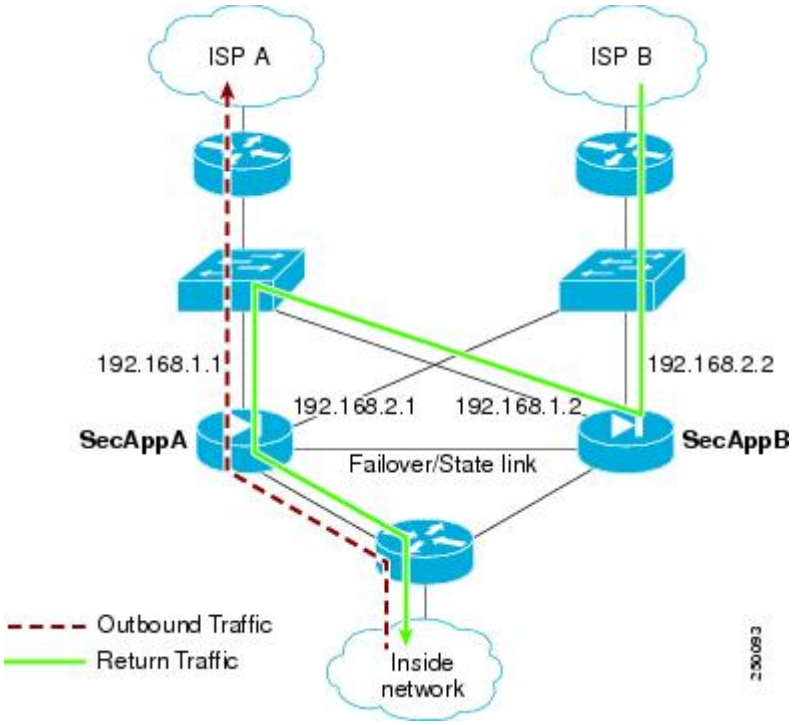
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスがセッション情報を持たないパケットを受信すると、同じグループ（この場合 ASR グループ 1）内のスタンバイ コンテキストの他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。

（注） この機能は、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

次の図に、非対称にルーティングされたパケットの例を示します。

図 *53 : ASR* の例



1. アウトバウンド セッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス外の ISP-A（192.168.1.1）から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターン トラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス外部の ISP-B（192.168.2.2）経由で戻ります。
3. 通常、リターン トラフィックは、そのインターフェイス 192.168.2.2 上にリターン トラフィックに関するセッション情報がないので、ドロップされます。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. このセッション情報は、SecAppB を持つ装置上のスタンバイ状態のインターフェイス outsideISP-A（192.168.1.2）にあります。ステートフル フェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。
5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこから、発信元の装置のインターフェイスを経由して戻ります（SecAppA の 192.168.1.1）。この転送は、必要に応じて、セッションが終了するまで続行されます。

始める前に

- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。
- replication http：HTTP セッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。
- コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキストインターフェイスも ASR グループに含めることはできません。

手順

ステップ 1 プライマリ装置のアクティブ コンテキストで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[ASR Groups]** の順に選択します。

ステップ 2 非対称にルーティングされたパケットを受信するインターフェイスについて、ドロップダウンリストから **ASR グループ ID** を選択します。

ステップ 3 [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

ステップ 4 ASDM をセカンダリ装置に接続し、プライマリ装置のコンテキストと同様のアクティブ コンテキストを選択します。

ステップ 5 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ASR Groups]** の順に選択します。

ステップ 6 この装置の同様のインターフェイスについて、同じ **ASR グループ ID** を選択します。

ステップ 7 [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

フェールオーバー の管理

この項では、フェールオーバーの設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、フェールオーバー を有効化した後に フェールオーバー 装置を管理する方法について説明します。

フェールオーバーの設定変更

ウィザードを使用しない場合や、設定を変更する場合に、手動でフェールオーバーを設定できます。ここでは、ウィザードに含まれていないため手動で設定する必要がある次のオプションについても説明します。

- フェールオーバー トラフィックを暗号化するための IPsec 事前共有キー
- HTTP 複製レート
- HTTP 複製（アクティブ/スタンバイ モード）

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 シングルモードでは、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]** の順に選択します。

マルチ コンテキスト モードでは、システム実行スペースで [Configuration] > [Device Management] > [Failover] > [Setup] を選択します。

ステップ 2 [Enable Failover] チェックボックスをオンにします。

（注） デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

ステップ 3 フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のオプションのいずれかを使用します。

- [IPsec Preshared Key]（優先）：フェールオーバー装置間のフェールオーバー リンクで IPsec LAN-to-LAN トンネルを確立するために、IKEv2 によって使用される事前共有キーです。注：フェールオーバー LAN-to-LAN トンネルは、IPsec（他の VPN）ライセンスには適用されません。
- [Secret Key]：フェールオーバー通信の暗号化に使用される秘密キーを入力します。このフィールドを空白のままにした場合は、コマンド複製中に送信されるコンフィギュレーション内のパスワードまたはキーを含め、フェールオーバー通信がクリアテキストになります。

  [Use 32 hexadecimal character key]：秘密キーに 32 文字の 16 進キーを使用するには、このチェック ボックスをオンにします。

ステップ 4 [LAN Failover] 領域で、フェールオーバー リンクの次のパラメータを設定します。

- [Interface]：フェールオーバー リンクに使用するインターフェイスを選択します。フェールオーバーには専用インターフェイスが必要ですが、ステートフル フェールオーバーとインターフェイスを共有できます。

  このリストには、未設定のインターフェイスまたはサブインターフェイスのみが表示され、フェールオーバー リンクとして選択できます。インターフェイスをフェールオーバー リンクに指定すると、そのインターフェイスは [Configuration] > [Interfaces] ペインでは編集できません。

- [Logical Name]：「failover」などのフェールオーバー通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。
- [Active IP]：インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP アドレスは未使用のサブネット上になければなりません。
- [Standby IP]：インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- [Subnet Mask]：サブネット マスクを指定します。
- [Preferred Role]：この ASA の優先されるロールがプライマリ装置であるかセカンダリ装置であるかを指定するために、[Primary] または [Secondary] を選択します。

ステップ 5 （オプション）次の手順でステート リンクを設定します。

- [Interface]：ステート リンクに使用するインターフェイスを選択します。選択できるのは、未設定のインターフェイスまたはサブインターフェイス、フェールオーバー リンク、または [--Use Named--] オプションです。

  （注） フェールオーバー リンク専用インターフェイスとステート リンク専用インターフェイスの 2 つのインターフェイスを別々に使用することを推奨します。

  未設定のインターフェイスまたはサブインターフェイスを選択した場合、そのインターフェイスの**アクティブ IP**、**サブネット マスク**、**論理名**、および**スタンバイ IP** を入力する必要があります。

  フェールオーバー リンクを選択した場合は、**アクティブ IP**、**サブネット マスク**、**論理名**、および**スタンバイ IP** の値を指定する必要はありません。フェールオーバー リンクに指定されている値が使用されます。

  [--Use Named--] オプションを選択した場合、[Logical Name] フィールドは、名前のついたインターフェイスのドロップダウン リストになります。このリストからインターフェイスを選択します。**アクティブ IP**、**サブネット マスク/プレフィックスの長さ**、**スタンバイ IP** の値を指定する必要はありません。そのインターフェイスに指定された値が使用されます。

- [Logical Name]：「state」などのステート通信に使用するインターフェイスの論理名を指定します。この名前は情報を提供するためのものです。
- [Active IP]：インターフェイスのアクティブ IP アドレスを指定します。IP アドレスは、IPv4 または IPv6 アドレスのどちらにすることもできます。この IP アドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。
- [Standby IP]：インターフェイスのスタンバイ IP アドレスを指定します。アクティブ IP アドレスと同じサブネット上のアドレスを指定します。
- [Subnet Mask]：サブネット マスクを指定します。

- （オプション、アクティブ/スタンバイのみ）[Enable HTTP Replication]：このオプションにより、アクティブ HTTP セッションをスタンバイ ファイアウォールにコピーするステートフル フェールオーバーがイネーブルになります。HTTP 複製を許可しない場合、HTTP 接続はフェールオーバーの発生時に切断されます。アクティブ/アクティブ モードでは、フェールオーバー グループごとに HTTP 複製を設定します。

  （注） フェールオーバーを使用しているときに、スタンバイ装置から HTTP フローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 6 [Replication] 領域で、セッション複製レートを 1 秒あたり接続数で設定します。最小および最大レートはモデルによって決まります。デフォルトは最大レートです。デフォルトを使用するには、[Use Default] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションがデバイスに保存されます。

ステップ 8 フェールオーバーをイネーブルにすると、フェールオーバー ピアを設定するためのダイアログボックスが表示されます。

- 後でフェールオーバー ピアに接続して手動で同様の設定を行う場合は、[No] をクリックします。
- ASDM によって自動的にフェールオーバー ピア上の関連するフェールオーバー設定が行われるようにするには、[Yes] をクリックします。[Peer IP Address] フィールドにピアの IP アドレスを指定します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーを装置レベルで強制するには次を行います。

a) コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。

- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b) 次のいずれかのボタンをクリックします。

- [Make Active] をクリックすると、この装置がアクティブ装置になります。
- [Make Standby] をクリックすると、相手装置がアクティブ装置になります。

ステップ 2 （アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで強制するには次を行います。

a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。# は、制御するフェールオーバー グループの番号です。

b) 次のいずれかのボタンをクリックします。

- [Make Active] をクリックすると、この装置でフェールオーバー グループがアクティブになります。
- [Make Standby] をクリックすると、相手装置でフェールオーバー グループがアクティブになります。

フェールオーバーのディセーブル化

1 つまたは両方の装置でフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。アクティブ/アクティブ フェールオーバー ペアの場合、どの装置を優先するように設定されていようと、フェールオーバー グループはアクティブであるすべての装置でアクティブ状態のまま維持されます。

フェールオーバーをディセーブルにする際、次の特性を参照してください。

- スタンバイ装置/コンテキストはスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません（これは疑似スタンバイ状態と呼ばれます）。
- スタンバイ装置/コンテキストは、アクティブ装置/コンテキストに接続されていない場合でもそのスタンバイ IP アドレスを引き続き使用します。
- スタンバイ装置/コンテキストによる、フェールオーバー上における接続に対するリッスンは継続されます。フェールオーバーをアクティブ装置/コンテキストで再度イネーブルにすると、そのコンフィギュレーションの残りが再同期化された後に、スタンバイ装置/コンテキストが通常のスタンバイ状態に戻ります。
- スタンバイ装置で手動でフェールオーバーをイネーブルにしてアクティブ化しないでください。代わりに、フェールオーバーの強制実行 （370 ページ）を参照してください。スタンバイ装置でフェールオーバーをイネーブルにすると、MAC アドレスの競合が発生し、IPv6 トラフィックが中断される可能性があります。

- 完全にフェールオーバーをディセーブルにするには、no failover コンフィギュレーションをスタートアップ コンフィギュレーションに保存してからリロードします。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 シングルモードでは、**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]** の順に選択します。

マルチ コンテキスト モードでは、システム実行スペースで [Configuration] > [Device Management] > [Failover] > [Setup] を選択します。

ステップ 2 [Enable Failover] チェックボックスをオフにします。

ステップ 3 [Apply] をクリックします。

ステップ 4 完全にフェールオーバーをディセーブルにするには、コンフィギュレーションを保存してをリロードします。

a) [Save] ボタンをクリックします。

b) [Tools] > [System Reload] を選択して、ASA をリロードします。

障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーを装置レベルで復元するには次を行います。

a) コンテキスト モードに応じて画面を選択します。

- シングル コンテキスト モードでは、[Monitoring] > [Properties] > [Failover] > [Status] を選択します。
- マルチ コンテキスト モードでは、システムで [Monitoring] > [Failover] > [System] を選択します。

b) [Reset Failover] をクリックします。

ステップ 2 （アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで復元するには次を行います。

a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。#は、制御するフェールオーバー グループの番号です。

b) [Reset Failover] をクリックします。

コンフィギュレーションの再同期

複製されたコマンドは、実行コンフィギュレーションに保存されます。複製されたコマンドをスタンバイ装置のフラッシュ メモリに保存するには、[File] > [Save Running Configuration to Flash] の順に選択します。

フェールオーバーのモニターリング

このセクションの手順に従うことで、フェールオーバーのステータスをモニターできます。

フェールオーバー メッセージ

フェールオーバーが発生すると、両方の ASA がシステム メッセージを送信します。

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、syslog メッセージ ガイドを参照してください。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。

（注） フェールオーバーの最中に、ASA は論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージ 411001 および 411002 を生成します。これは通常のアクティビティです。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステムパフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

フェールオーバー ステータスのモニターリング

（注） フェールオーバーイベントが発生した後、デバイスのモニターリングを継続するには、ASDM を再起動するか、または [Devices] ペインに表示される別のデバイスに切り替えて、元の ASA に戻る手順を実行する必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニターリングが再確立されないためです。

[Monitoring] > [Properties] > [Failover] を選択して、アクティブ/スタンバイ フェールオーバーをモニターします。

[Monitoring] > [Properties] > [Failover] 領域で次の画面を使用して、アクティブ/アクティブ フェールオーバーをモニターします。

System

[System] ペインには、システムのフェールオーバー状態が表示されます。また、システムのフェールオーバー状態を次の方法で制御できます。

- デバイスのアクティブ/スタンバイ状態を切り替える。
- 障害が発生したデバイスをリセットする。
- スタンバイ装置をリロードする。

フィールド

[Failover state of the system]：表示専用。ASA のフェールオーバー状態を表示します。表示される情報は、**show failover** コマンドで受け取る出力と同じです。表示出力に関する詳細については、コマンド リファレンスを参照してください。

[System] ペインでは、次のアクションを使用できます。

- [Make Active]：アクティブ/スタンバイ コンフィギュレーションで、このボタンをクリックすると、ASA がアクティブ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがアクティブになります。
- [Make Standby]：アクティブ/スタンバイ ペアで、このボタンをクリックすると、ASA がスタンバイ装置になります。アクティブ/アクティブ コンフィギュレーションで、このボタンをクリックすると、ASA で両方のフェールオーバー グループがスタンバイ状態になります。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Reload Standby]：このボタンをクリックして、スタンバイ装置を強制的にリロードします。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

フェールオーバー グループ 1 およびフェールオーバー グループ 2

[Failover Group 1] ペインおよび [Failover Group 2] ペインには、選択したグループのフェールオーバー状態が表示されます。また、グループのアクティブ/スタンバイ状態を切り替えるか、または障害が発生したグループをリセットして、グループのフェールオーバー状態を制御することもできます。

フィールド

[Failover state of Group[*x*]]：表示専用。選択したフェールオーバー グループのフェールオーバー状態を表示します。表示される情報は、**show failover group** コマンドで受け取る出力と同じです。

このペインで次のアクションを実行できます。

- [Make Active]：このボタンをクリックして、フェールオーバー グループを ASA のアクティブ ユニットにします。
- [Make Standby]：このボタンをクリックして、フェールオーバー グループを ASA で強制的にスタンドバイ状態にします。
- [Reset Failover]：このボタンをクリックして、システムを障害状態からスタンバイ状態にリセットします。システムをアクティブ状態にはリセットできません。アクティブ装置でこのボタンをクリックすると、スタンバイ装置がリセットされます。
- [Refresh]：このボタンをクリックして、[system] フィールドのフェールオーバー状態にあるステータス情報をリフレッシュします。

フェールオーバーの履歴

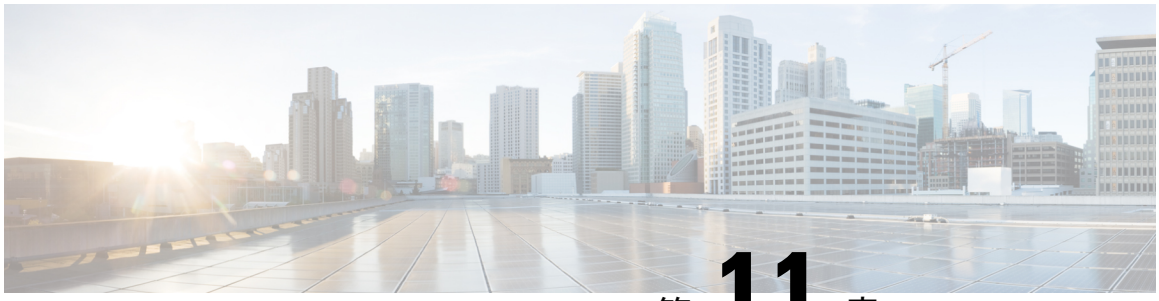
機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバー	7.0(1)	この機能が導入されました。
アクティブ/アクティブ フェールオーバー	7.0(1)	この機能が導入されました。
フェールオーバー キーの 16 進数値サポート	7.0(4)	フェールオーバー リンクの暗号化用に16進数値が指定できるようになりました。 次の画面が変更になりました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。
フェールオーバー キーのマスター パスフレーズのサポート	8.3(1)	フェールオーバー キーが、実行コンフィギュレーションとスタートアップ コンフィギュレーションの共有キーを暗号化するマスターパスフレーズをサポートするようになりました。一方のASAから他方に共有秘密をコピーする場合、たとえば、**more system:running-config** コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。 （注） **failover key** の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。 ASDM の変更はありませんでした。
フェールオーバーにIPv6のサポートが追加	8.2(2)	次の画面が変更されました。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces]。

機能名	リリース	機能情報
「同時」ブートアップ中のフェールオーバー グループのユニットの設定の変更	9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	9.1(2)	フェールオーバー キーに独自の暗号化を使用する代わりに、フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。 （注） フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup]。
ハードウェア モジュールのヘルス モニターリングの無効化	9.3(1)	ASA はデフォルトで、インストール済みハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニターリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニターリングをディセーブルにできます。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Interfaces]

機能名	リリース	機能情報
フェールオーバーペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック	9.3(2)	通常のコンフィギュレーションの同期を除いてスタンバイ装置上で変更ができないように、スタンバイ装置（アクティブ/スタンバイ フェールオーバー）またはスタンバイ コンテキスト（アクティブ/アクティブ フェールオーバー）のコンフィギュレーション変更をロックできるようになりました。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]
ASA 5506H のフェールオーバー リンクとして、管理 1/1 インターフェイスを使用可能	9.5(1)	管理 1/1 インターフェイスは、ASA 5506H に限りフェールオーバー リンクとして設定できるようになりました。この機能により、デバイスの他のインターフェイスをデータインターフェイスとして使用できます。この機能を使用した場合、ASA FirePOWER モジュールは使用できません。このモジュールでは管理 1/1 インターフェイスを通常の管理インターフェイスとして維持することが必須です。 次の画面が変更されました。[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Setup]
キャリア グレード NAT の強化がフェールオーバーおよび ASA クラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 変更された画面はありません。

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバーを使用するときの AnyConnect からのダイナミック ACL の同期時間が改善	9.6(2)	フェールオーバー ペアで AnyConnect を使用するとき、関連付けられているダイナミック ACL（dACL）のスタンバイ ユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。 変更された画面はありません。
マルチ コンテキスト モードの AnyConnect接続のステートフル フェールオーバー	9.6(2)	マルチ コンテキスト モードで AnyConnect接続のステートフル フェールオーバーがサポートされました。 変更された画面はありません。
より迅速に検出を行うためのインターフェイスのリンクステートモニターリングを設定可能	9.7(1)	デフォルトでは、フェールオーバーペアの ASA は、500 ミリ秒ごとにインターフェイスのリンク ステートをチェックします。ポーリングの間隔を 300 ミリ秒から 799 ミリ秒の間で設定できるようになりました。たとえば、ポーリング時間を 300 ミリ秒に設定すると、ASA はインターフェイス障害やトリガーのフェールオーバーをより迅速に検出できます。 次の画面が変更されました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [Failover] > [Criteria]**

機能名	リリース	機能情報
FirePOWER 9300 および 4100 でのアクティブ/スタンバイ フェールオーバーヘルス モニターリングで、双方向フォワーディング検出（BFD）がサポートされました。	9.7(1)	FirePOWER 9300 および 4100 上のアクティブ/スタンバイ ペアの 2 つのユニット間のフェールオーバーヘルス チェックに対して、双方向フォワーディング検出（BFD）を有効にできるようになりました。ヘルス チェックに BFD を使用すると、デフォルトのヘルス チェックより信頼性が高まり、CPU の使用を抑えることができます。 次の画面が変更されました。 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Setup]**



第 11 章

パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー

この章では、Microsoft Azure などのパブリック クラウド環境で、Cisco ASAv のハイ アベイラビリティを実現するためにアクティブ/バックアップ フェールオーバーを構成する方法について説明します。

パブリック クラウドでのフェールオーバーについて

冗長性を確保するために、ASAv をアクティブ/バックアップ高可用性（HA）設定でパブリック クラウド環境に展開します。パブリック クラウドでの HA は、アクティブな ASAv の障害がバックアップ ASAv へのシステムの自動フェールオーバーをトリガーするのを許可するステートレスなアクティブ/バックアップ ソリューションを実装します。

次のリストは、HA パブリック クラウド ソリューションの主要コンポーネントを示しています。

- **アクティブ ASAv**：HA ピアのファイアウォール トラフィックを処理するように設定された HA ペア内の ASAv。
- **バックアップ ASAv**：ファイアウォール トラフィックを処理せず、アクティブな ASAv に障害が発生した場合にアクティブな ASAv を引き継ぐ HA ペア内の ASAv。これは、フェールオーバーの際にピアの識別情報を引き継がないため、スタンバイではなくバックアップと呼ばれます。

- **HA エージェント**：ASAv 上で実行され、ASAv の HA ロール（アクティブ/バックアップ）を判断し、その HA ピアの障害を検出し、その HA ロールに基づいてアクションを実行する軽量プロセス。

物理 ASA および非パブリック クラウドの仮想 ASA では、Gratuitous ARP 要求を使用してフェールオーバー条件を処理しますが、バックアップ ASA は、アクティブな IP アドレスと MAC アドレスに関連付けられていることを示す Gratuitous ARPP を送信します。ほとんどのパブリック クラウド環境では、このようなブロードキャスト トラフィックは許可されていません。このため、パブリック クラウドの HA 設定では、フェールオーバーが発生したときに通信中の接続を再起動する必要があります。

アクティブ装置の状態がバックアップ装置によってモニターされ、所定のフェールオーバー条件に一致しているかどうかが判別されます。所定の条件に一致すると、フェールオーバーが行われます。フェールオーバー時間は、パブリック クラウド インフラストラクチャの応答性に応じて、数秒～ 1 分を超える場合があります。

アクティブ/バックアップ フェールオーバーについて

アクティブ/バックアップ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。バックアップ装置は積極的にトラフィックを渡したり、アクティブ装置と設定情報を交換したりしません。アクティブ/バックアップ フェールオーバーでは、障害が発生した装置の機能を、バックアップ ASAv デバイスに引き継ぐことができます。アクティブ装置が故障すると、バックアップ状態に変わり、そしてバックアップ装置がアクティブ状態に変わります。

プライマリ/セカンダリの役割とアクティブ/バックアップ ステータス

アクティブ/バックアップ フェールオーバーを設定する場合、1 つの装置をプライマリとして設定し、もう 1 つの装置をセカンダリとして設定します。この時点で、2 つの装置は、デバイスとポリシーの設定、およびイベント、ダッシュボード、レポート、ヘルス モニターリングで、2 つの個別のデバイスとして機能します。

フェールオーバー ペアの 2 つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がバックアップであるか、つまりどちらの装置がアクティブにトラフィックを渡すかということに関連します。両方の装置がトラフィックを渡すことができますが、プライマリ装置だけがロード バランサ プローブに応答し、構成済みのルートをプログラミングしてルートの接続先として使用します。バックアップ装置の主な機能は、プライマリ装置の正常性を監視することです。両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。

フェールオーバー接続

バックアップ ASAv は、TCP を介して確立されたフェールオーバー接続を使用して、アクティブ ASAv の正常性を監視します。

- アクティブ ASAv は、リッスン ポートを開くことで接続サーバーとして機能します。

- バックアップ ASAv は、接続ポートを使用してアクティブ ASAv に接続します。
- 通常、ASAv 装置間で何らかのネットワーク アドレス変換が必要な場合を除き、リッスン ポートと接続ポートは同じです。

フェールオーバー接続の状態によって、アクティブ ASAv の障害を検出します。バックアップ ASAv は、フェールオーバー接続が切断されたことを確認すると、アクティブ ASAv で障害が発生したと判断します。同様に、バックアップ ASAv がアクティブ装置に送信されたキープアライブ メッセージに対する応答を受信しない場合も、アクティブ ASAv で障害が発生したと判断します。

関連項目

ポーリングと Hello メッセージ

バックアップ ASAv はフェールオーバー接続を介してアクティブ ASAv に Hello メッセージを送信し、Hello 応答の返信を期待します。メッセージのタイミングには、ポーリング間隔、つまりバックアップの ASAv 装置による Hello 応答の受信と次の Hello メッセージの送信との間の時間間隔が使用されます。応答の受信は、ホールド時間と呼ばれる受信タイムアウトによって強制されます。Hello 応答の受信がタイムアウトすると、アクティブ ASAv で障害が発生したとみなされます。

ポーリング間隔とホールド時間間隔は設定可能なパラメータです（アクティブ/バックアップ フェールオーバーの設定 （391 ページ） を参照）。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はバックアップ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がバックアップ装置になります。

フェールオーバー イベント

アクティブ/バックアップ フェールオーバーでは、フェールオーバーがユニットごとに行われます。次の表に、各障害イベントに対するフェールオーバー アクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、バックアップ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *21* : フェールオーバー イベント

障害イベント	ポリシー（**Policy**）	アクティブアクション	バックアップアクション	注
バックアップ装置がフェールオーバー接続のクローズを確認	フェールオーバー	適用対象外	アクティブになる アクティブに故障とマークする	これは標準のフェールオーバーの使用例です。
アクティブ装置がフェールオーバー接続のクローズを確認	フェールオーバーなし	バックアップを障害としてマークする	n/a	非アクティブ装置へのフェールオーバーは発生しません。
アクティブ装置がフェールオーバーリンクでTCPタイムアウトを確認	フェールオーバーなし	バックアップを障害としてマークする	動作なし	アクティブ装置がバックアップ装置から応答を受信しない場合、フェールオーバーは発生しません。
バックアップ装置がフェールオーバーリンクでTCPタイムアウトを確認	フェールオーバー	適用対象外	アクティブになる アクティブに故障とマークする アクティブ装置にフェールオーバーコマンドの送信を試行する	バックアップ装置はアクティブ装置が動作を続行できないと見なし、引き継ぎます。 アクティブ装置がまだ起動しているが時間内に応答を送信できない場合、バックアップ装置はフェールオーバーコマンドをアクティブ装置に送信します。
アクティブ認証の失敗	フェールオーバーなし	動作なし	動作なし	バックアップ装置はルートテーブルを変更するため、バックアップ装置が Azure に認証する必要がある唯一の装置になります。 アクティブ装置が Azure に認証されているかどうかは関係ありません。

障害イベント	ポリシー（Policy）	アクティブアクション	バックアップアクション	注
バックアップ認証の失敗	フェールオーバーなし	バックアップを未認証としてマークする	動作なし	バックアップ装置がAzureに認証されていない場合、フェールオーバーは発生しません。
アクティブ装置が意図的なフェールオーバーを開始	フェールオーバー	バックアップになる	アクティブになる	アクティブ装置は、フェールオーバーリンク接続を閉じることでフェールオーバーを開始します。 バックアップ装置は接続のクローズを確認し、アクティブ装置になります。
バックアップ装置が意図的なフェールオーバーを開始	フェールオーバー	バックアップになる	アクティブになる	バックアップ装置は、フェールオーバーメッセージをアクティブ装置に送信することによってフェールオーバーを開始します。 アクティブ装置はメッセージを確認すると、接続を閉じてバックアップ装置になります。 バックアップ装置は接続のクローズを確認し、アクティブ装置になります。
以前にアクティブであった装置の復旧	フェールオーバーなし	バックアップになる	片方をバックアップとマークする	フェールオーバーは確実に必要でない限り発生しません。

障害イベント	ポリシー（Policy）	アクティブアクション	バックアップアクション	注
アクティブ装置がバックアップ装置からのフェールオーバーメッセージを確認する	フェールオーバー	バックアップになる	アクティブになる	ユーザーが手動フェールオーバーを開始した場合に発生する可能性があります。または、バックアップ装置がTCPタイムアウトを確認したが、アクティブ装置がバックアップ装置からメッセージを受信できる場合に発生する可能性があります。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

パブリック クラウドでの高可用性の ASAv フェールオーバー

冗長性を確保するために、ASAv をアクティブ/バックアップ高可用性（HA）設定でパブリック クラウド環境に展開します。

- Microsoft Azure パブリッククラウドでのみサポートされています。ASAv VM を設定する場合、サポートされる vCPU の最大数は 8、サポートされる最大メモリは 64 GB RAM です。サポートされるインスタンスの包括的なリストについては、『ASAv Getting Started Guide』を参照してください。
- アクティブな ASAv の障害がバックアップ ASAv へのシステムの自動フェールオーバーをトリガーするのを許可するステートレスなアクティブ/バックアップ ソリューションを実装します。

制限事項

- フェールオーバーはミリ秒ではなく、秒単位で行われます。
- HA の役割の決定と HA 装置として参加できるかどうかは、HA ピア間、および HA 装置と Azure インフラストラクチャとの間の TCP 接続に依存します。ASAv が HA 装置として参加できない状況がいくつかあります。
  - HA ピアへのフェールオーバー接続を確立できない。
  - Azure から認証トークンを取得できない。
  - Azure で認証できない。

- アクティブ装置からバックアップ装置に設定が同期されることはありません。フェールオーバートラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。
- フェールオーバー ルートテーブルの制限

  パブリッククラウドの HA のルートテーブルには次の制限があります。

  - 設定できるルートテーブルの数は最大 16 個です。
  - ルートテーブルで設定できるルートの数は最大 64 個です。

  いずれの場合も、制限に達すると、ルートテーブルまたはルートを削除して再試行することを推奨するアラートが表示されます。
- ASDM サポートはありません。
- IPSec リモート アクセス VPN はサポートされていません。

  (注) パブリック クラウドでサポートされる VPN トポロジについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide』を参照してください。
- ASAv 仮想マシン インスタンスは、同じ可用性セットにある必要があります。Azure の現在の ASAv ユーザーの場合、既存の導入から HA にアップグレードすることはできません。インスタンスを削除し、Azure マーケットプレイスから ASAv 4 NIC HA オファリングを導入する必要があります。

パブリッククラウドでのフェールオーバーのライセンス

ASAv は Cisco Smart Software Licensing を使用します。スマート ライセンスは、通常の操作に必要です。各 ASAv は、ASAv プラットフォーム ライセンスを使用して別々にライセンスを取得する必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。ASAv の正確なライセンス要件については、『Cisco ASA Series Feature Licenses』ページを参照してください。

パブリッククラウドでのフェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートレスなフェールオーバーのみ。
- フェールオーバートラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

- フェールオーバーの TCP 制御ポート番号は 44442 です。
- Azure ロード バランサの健全性プローブ ポート番号は 44441 です。
- 装置のポーリング時間は 5 秒です。
- 装置のホールド時間は 15 秒です。
- ASAv はプライマリインターフェイス（Management 0/0）のヘルスプローブに応答します。

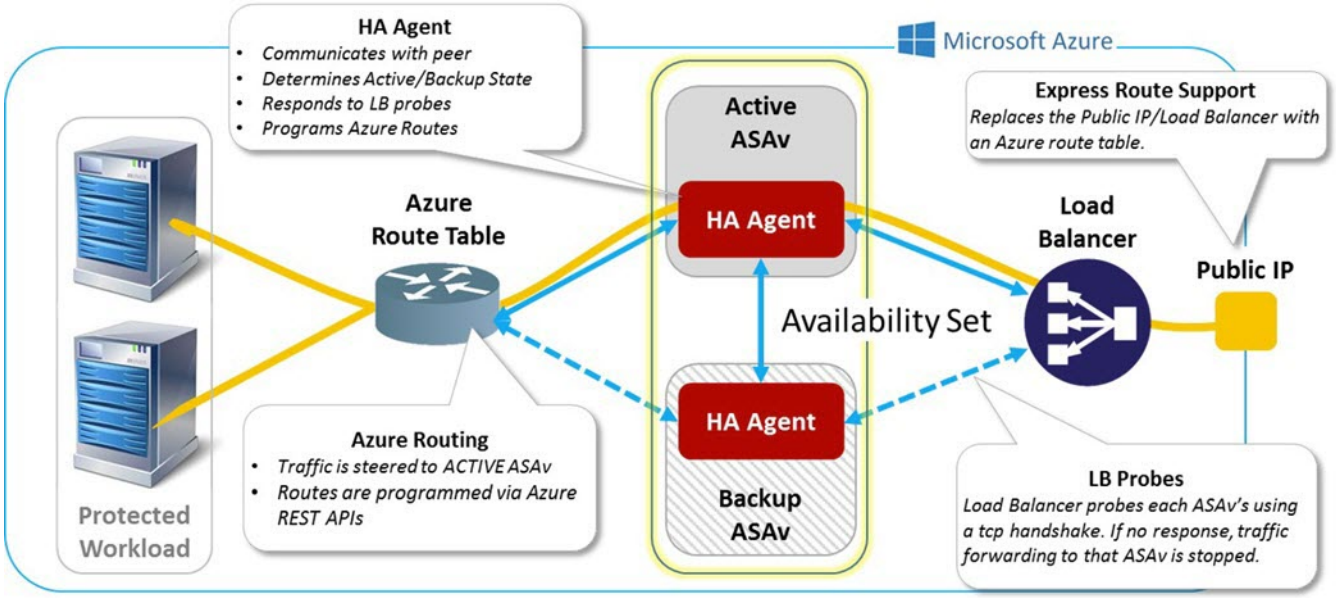
（注） フェールオーバーポート番号、ヘルスプローブポート番号、ポーリング時間、およびプライマリインターフェイスを変更するオプションについては、オプションのフェールオーバー パラメータの設定 （393 ページ）を参照してください。

Microsoft Azure での ASAv 高可用性について

次の図に、Azure での ASAv HA 導入の概要を示します。アクティブ/バックアップ フェールオーバー設定の 2 つの ASAv インスタンスの背後で、ワークロードが保護されます。Azure ロードバランサは、3 ウェイ TCP ハンドシェイクを使用して両方の ASAv 装置をプローブします。アクティブ ASAv は、3 ウェイ ハンドシェイクを完了して健全であることを示しますが、バックアップ ASAv は意図的に応答しません。ロードバランサに応答しないことで、バックアップ ASAv はロード バランサには正常ではないように見え、トラフィックが送信されません。

フェールオーバーでは、アクティブ ASAv がロードバランサ プローブへの応答を停止し、バックアップ ASAv が応答を開始することで、すべての新しい接続がバックアップ ASAv に送信されます。バックアップ ASAv は、ルートテーブルを変更してトラフィックがアクティブ装置からバックアップ装置にリダイレクトされるように API 要求を Azure ファブリックに送信します。この時点で、バックアップ ASAv がアクティブ装置になり、アクティブ装置はフェールオーバーの理由に応じてバックアップ装置になるか、またはオフラインになります。

図 *54 : Azure* での *ASAv HA* の導入



自動的に API 呼び出しによって Azure ルート テーブルが変更されるようにするには、ASAv HA ユニットに Azure Active Directory のクレデンシャルが必要です。Azure は、簡単に言えばサービス アカウントであるサービス プリンシパルの概念を採用しています。サービス プリンシパルを使用すると、あらかじめ定義された Azure リソース セット内でタスクを実行するのに十分な権限と範囲のみを持つアカウントをプロビジョニングできます。

ASAv HA の導入で、サービス プリンシパルを使用して Azure サブスクリプションを管理できるようにするには、次の 2 つの手順を行います。

1. Azure Active Directory アプリケーションとサービス プリンシパルを作成します（Azure サービス プリンシパルについて （389 ページ） を参照）。
2. サービス プリンシパルを使用して Azure で認証するように ASAv インスタンスを設定します（アクティブ/バックアップ フェールオーバーの設定 （391 ページ） を参照）。

関連項目

ロード バランサの詳細については、Azure のマニュアルを参照してください。

Azure サービス プリンシパルについて

Azure リソース（ルート テーブルなど）へのアクセスまたはリソースの変更が必要となるアプリケーションがある場合は、Azure Active Directory（AD）アプリケーションを設定し、必要な権限を割り当てる必要があります。この方法は、以下の理由から、自分のクレデンシャルでアプリケーションを実行するよりも推奨されます。

- 自分の権限とは異なる権限をアプリケーション ID に割り当てることができる。通常、割り当てる権限は、アプリケーションが実行する必要があるものだけに制限します。

- 職責が変わった場合でも、アプリケーションのクレデンシャルを変更する必要がない。
- 無人スクリプトの実行時に、証明書を使用して認証を自動化できる。

Azure ポータルに Azure AD アプリケーションを登録すると、アプリケーション オブジェクトとサービス プリンシパル オブジェクトの 2 つのオブジェクトが Azure AD テナントに作成されます。

- **アプリケーション オブジェクト**：Azure AD アプリケーションは、そのアプリケーションが登録されている Azure AD テナント（アプリケーションの「ホーム」テナント）にある唯一のアプリケーション オブジェクトによって定義されます。
- **サービス プリンシパル オブジェクト**：サービス プリンシパル オブジェクトは、特定のテナントでのアプリケーションの使用に関するポリシーと権限を定義し、アプリケーション実行時のセキュリティ プリンシパルの基礎を提供します。

Azure は、『*Azure Resource Manager Documentation*』で Azure AD アプリケーションとサービス プリンシパルを作成する方法について説明しています。詳しい手順については、次のトピックを参照してください。

- リソースにアクセスできる Azure AD アプリケーションとサービス プリンシパルをポータルで作成する
- Azure PowerShell を使用して資格情報でのサービス プリンシパルを作成する

（注） サービス プリンシパルを設定したら、**ディレクトリ ID**、**アプリケーション ID**、および**秘密鍵**を取得します。これらは、Azure 認証クレデンシャルを設定するために必要です（アクティブ/バックアップ フェールオーバーの設定 （391 ページ） を参照）。

Azure での ASAv 高可用性の設定要件

図 54 : Azure での ASAv HA の導入 （389 ページ） で説明しているのと同じ設定を導入するには、以下が必要です。

- 次の Azure 認証情報（Azure サービス プリンシパルについて （389 ページ） を参照）
  - ディレクトリ ID
  - Application ID
  - 秘密鍵
- 次の Azure ルート情報（Azure ルート テーブルの設定 （394 ページ） を参照）。
  - Azure サブスクリプション ID
  - ルート テーブル リソース グループ
  - テーブル名

- アドレス プレフィックス
- ネクスト ホップ アドレス。

- 次の ASA 設定（アクティブ/バックアップ フェールオーバーの設定 （391 ページ）、パブリック クラウドでのフェールオーバーのデフォルト （387 ページ） を参照）
  - アクティブ/バックアップ IP アドレス
  - HA エージェント通信ポート
  - ロード バランサのプローブ ポート
  - ポーリング間隔

（注） プライマリ装置とセカンダリ装置の両方で基本のフェールオーバー設定を構成します。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

アクティブ/バックアップ フェールオーバーの設定

アクティブ/バックアップ フェールオーバーを設定するには、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

始める前に

- Azure 可用性セットで ASAv HA ペアを導入します。
- Azure サブスクリプション ID とサービス プリンシパルの Azure 認証クレデンシャルを含む、Azure 環境情報を入手します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** の順に選択します。

ステップ 2 [Cloud] タブで、[Unit] チェックボックスをオンにして [Failover Unit] ドロップダウン オプションを展開します。

ステップ 3 [Failover Unit] ドロップダウン メニューから [primary] を選択します。

両方の HA 装置が同時に起動した場合は、プライマリ装置がアクティブな HA ロールを引き受けます。

ステップ 4 （オプション）[Port] チェックボックスをオンにして、[Control] および [Probe] フィールドを展開します。

a) [Control] フィールドに有効な TCP 制御ポートを入力します。または、デフォルトのポート 44442 のままにします。

制御ポートは、アクティブ ASAv とバックアップ ASAv の間で TCP フェールオーバー接続を確立します。

b) [Probe] フィールドに有効な TCP プローブ ポートを入力します。または、デフォルトのポート 44441 のままにします。

プローブ ポートは、Azure ロード バランサ プローブの宛先ポートとして使用される TCP ポートです。

ステップ 5 （オプション）[Time] チェックボックスをオンにして、[Poll Time] および [Hold Time] フィールドを展開します。

a) [Poll Time] フィールドに有効な時間（秒）を入力します。または、デフォルトの 5 秒のままにします。

ポーリング時間の範囲は、1 ～ 15 秒です。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

b) [Hold Time] フィールドに有効な時間（秒）を入力します。または、デフォルトの 15 秒のままにします。

hello パケットを受信できなかったときから装置が失敗としてマークされるまでの時間が、保持時間によって決まります。ホールド時間の範囲は 3 ～ 60 秒です。装置のポーリング時間の 3 倍未満のホールド時間の値を入力することはできません。

ステップ 6 [Peer] チェックボックスをオンにして、[Peer IP-Address] および [Peer Port] フィールドを展開します。

a) [Peer IP-Address] フィールドに、HA ピアへの TCP フェールオーバー制御接続を確立するために使用する IP アドレスを入力します。

b) （オプション）[Peer Port] フィールドに有効な TCP 制御ポートを入力します。mataha,デフォルトのポート 44442 のままにします。

ピア ポートは、アクティブ ASAv とバックアップ ASAv の間で TCP フェールオーバー接続を確立します。

ステップ 7 [Authentication] チェックボックスをオンにして、[Application-id]、[Directory-id]、および [Key] フィールドを展開します。

Azure サービス プリンシパルの認証クレデンシャルを設定できます。この認証クレデンシャルにより、ASAv HA ピアがルート テーブルなどの Azure リソースにアクセスしたり変更できるようになります。サービス プリンシパルを使用すると、定義済みの Azure リソース セット内でタスクを実行するための最小限の権限を持つ Azure アカウントをプロビジョニングできます。ASAv HA の場合は、ユーザー定義のルートを変更するのに必要な権限に制限されます（Azure サービス プリンシパルについて （389 ページ） を参照）。

a) Azure サービス プリンシパルの Azure アプリケーション ID を [Application-id] フィールドに入力します。

Azure インフラストラクチャからアクセス キーを要求するときは、このアプリケーション ID が必要です。

b) Azure サービス プリンシパルの Azure ディレクトリ ID を [Directory-id] フィールドに入力します。

Azure インフラストラクチャからアクセス キーを要求するときは、このディレクトリ ID が必要です。

c) Azure サービス プリンシパルの Azure 秘密鍵を [Key] フィールドに入力します。

Azureインフラストラクチャからアクセスキーを要求するときは、この秘密鍵が必要です。[Encrypt] フィールドがオンの場合、この秘密鍵は実行コンフィギュレーションで暗号化されます。

ステップ 8 [Subscription] チェックボックスをオンにして、[Sub-id] フィールドを展開します。

これは、更新が必要なルート テーブルが属するアカウントのサブスクリプション ID です。

ステップ 9 [Enable Cloud Failover] チェックボックスをオンにします。

ステップ 10 [Apply] をクリックします。

デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

ステップ 11 セカンダリ装置でまだフェールオーバーが有効になっていない場合は、[Device List] からセカンダリ ASAv に接続するか、または ASAv の IP アドレス **https***://asa_ip_address/***admin** を使用して新しい ASDM セッションを開始します。

ステップ 12 手順 1 ～ 10 を繰り返して、セカンダリ装置でアクティブ/バックアップ フェールオーバーを設定します。

プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

次のタスク

必要に応じて、追加のパラメータを設定します。

- Azure ルート情報の設定（Azure ルート テーブルの設定 （394 ページ） を参照）。

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

Azure ルート テーブルの設定

ルート テーブル設定は、ASAv がアクティブなロールを引き継ぐときに更新する必要のあるAzureユーザー定義ルートに関する情報で構成されています。フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルートテーブル情報を使用して自動的にルートを自身に向けます。

（注） アクティブ装置とバックアップ装置の両方でAzureルートテーブル情報を設定する必要があります。

始める前に

- プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。
- Azure サブスクリプション ID とサービス プリンシパルの Azure 認証クレデンシャルを含む、Azure 環境情報を入手します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** の順に選択します。

ステップ 2 [Route-Table] タブをクリックして、[Add] をクリックします。

a) [Route Table Name] フィールドに、ルート テーブルの名前を入力します。

最大 16 個のルート テーブルを設定できます。または、ルート テーブル リストのエントリを編集または削除できます。

b) （オプション）[Sub-id] フィールドに、Azure サブスクリプション ID を入力します。

ここで対応する Azure サブスクリプション ID を指定することで、2 つ以上の Azure サブスクリプションのユーザー定義ルートを更新できます。Azure サブスクリプション ID を指定せずに [Route Table Name] を入力すると、グローバル パラメータが使用されます。

（注） **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** からアクティブ/バックアップ フェールオーバーを設定するときに、Azure サブスクリプション ID を入力します（アクティブ/バックアップ フェールオーバーの設定 （391 ページ）を参照）。

ステップ 3 [Route-Table-Mode] をクリックします。ルート テーブルへのエントリを追加、編集、または削除できます。

ステップ 4 [Add] をクリックします。

Azure ユーザー定義ルートに対して次の値を入力します。

a) [Route Table] ドロップダウン リストからルート テーブルを選択します。
b) [Azure Resource Group] フィールドに、Azure ルート テーブルを含む Azure リソース グループの名前を入力します。
c) [Route Name] フィールドに、ルートの一意の名前を入力します。
d) [Prefix Address/Mask] フィールドに、CIDR 表記で IP アドレス プレフィックスを入力します。
e) [Next Hop Address] フィールドに、ネクストホップ アドレスを入力します。これは ASAv 上のインターフェイス IP アドレスです。

（注） 最大 64 個のルートを設定できます。

ステップ 5 [Apply] をクリックして変更内容を保存します。

パブリック クラウドでのフェールオーバーの管理

この項では、フェールオーバーを有効にした後でクラウド内の フェールオーバー 装置を管理する方法について説明します。ある装置から別の装置にフェールオーバーを強制的に変更する方法についても説明します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次のコマンドを実行します。

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択します。
ステップ 2 装置レベルでフェールオーバーを強制するには、次のいずれかのボタンをクリックします。

- 装置をアクティブ装置にするには、[Make Active] をクリックします。
- 装置をスタンバイ装置にするには、[Make Standby] をクリックします。

ルートの更新

Azure のルートの状態がアクティブ ロールの ASAv と矛盾している場合は、ASAv でルート更新を強制できます。

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択します。

ステップ 2 [Update Route] をクリックします。

このコマンドは、アクティブ ロールの ASAv でのみ有効です。認証に失敗すると、出力は `Route changes failed` となります。

Azure 認証の検証

Azure で ASAv HA の導入を成功させるには、サービス プリンシパルの設定が完全かつ正確である必要があります。適切な Azure 認証がないと、ASAv 装置はリソースにアクセスして、フェールオーバーを処理したりルート更新を実行したりできません。フェールオーバー設定をテストして、Azure サービス プリンシパルの次の要素に関連するエラーを検出できます。

- ディレクトリ ID
- Application ID
- Authentication Key

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択します。

ステップ 2 [Test Authentication] をクリックします。

認証に失敗すると、コマンド出力は `Authentication Failed` となります。

ディレクトリ ID またはアプリケーション ID が正しく設定されていない場合、Azure は認証トークンを取得するための REST 要求で指定されたリソースを認識しません。この条件エントリのイベント履歴は次のようになります。

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

ディレクトリ ID またはアプリケーション ID は正しいが、認証キーが正しく設定されていない場合、Azure は認証トークンを生成する権限を許可しません。この条件エントリのイベント履歴は次のようになります。

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

パブリック クラウドでのフェールオーバーのモニター

この項では、フェールオーバー ステータスをモニターする方法について説明します。

フェールオーバー ステータス

（注） フェールオーバーイベントが発生した後、デバイスのモニターリングを継続するには、ASDMを再起動するか、または [Devices] ペインに表示される別のデバイスに切り替えて、元の ASA に戻る手順を実行する必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニターリングが再確立されないためです。

- アクティブ/バックアップ フェールオーバー ステータスをモニターするには、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** を選択し、[Failover Status] をクリックします。
- タイムスタンプ、重大度レベル、イベントタイプ、およびイベントテキストを含むフェールオーバー イベント履歴を表示するには、**[Monitoring]** > **[Properties]** > **[Failover]** > **[History]** を選択します。

フェールオーバー メッセージ

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、syslog メッセージ ガイドを参照してください。Syslog メッセージの範囲は 1045xx と 1055xx です。

（注） フェールオーバーの最中に、ASA は論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージを生成します。これは通常のアクティビティです。

スイッチオーバー中に生成される syslog の例を次に示します。

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error:
Unknown error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
 Active unit
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
```

```
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

パブリック クラウドの導入に関連する各 syslog には、装置の役割が最初に追加されます（(Primary) または (Secondary)）。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

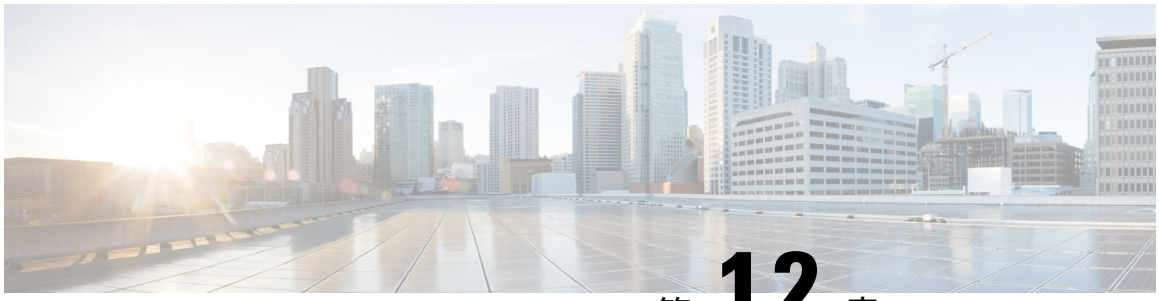
（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステム パフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

パブリック クラウドでのフェールオーバーの履歴

機能名	リリース	機能情報
Microsoft Azure でのアクティブ/バックアップ フェールオーバー	7.9(1)	この機能が導入されました。



第 12 章

ASA クラスタ

クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。クラスタリングでサポートされない機能 （481 ページ） を参照してください。

ASA クラスタリングの概要

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのユニットとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーン ネットワーク。クラスタ制御リンクと呼ばれます。

- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータが次のいずれかの方法を使用します。

- スパンド EtherChannel（推奨）：クラスタ内の複数のメンバのインターフェイスをグループ化して 1 つの EtherChannel とします。この EtherChannel がユニット間のロード バランシングを実行します。
- ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してユニット間のロード バランシングを実行します。
- 等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミック ルートを使用してユニット間のロード バランシングを実行します。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。ここでは、各メンバーのロールの特長について説明します。

Bootstrap Configuration

各デバイスで、最小限のブートストラップ コンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。通常、クラスタリングを有効にする最初のノードが制御ノードになります。以降のノードに対してクラスタリングをイネーブルにすると、そのノードはデータノードとしてクラスタに参加します。

制御ノードとデータノードの役割

クラスタ内のメンバーの 1 つが制御ノードになります。複数のクラスタメンバーが同時にオンラインになる場合、制御ノードは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。一般的には、クラスタを作成した後で最初に追加したノードが制御ノードとなります。これは単に、その時点でクラスタに存在する唯一のノードであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ノード上のみで実行する必要があります。コンフィギュレーションは、データノードに複製されます。物理的アセット（たとえばインターフェイス）の場合は、制御ノードのコンフィギュレーションがすべてのデータノード上でミラーリングされます。たとえば、内部インターフェイスとしてイーサネット 1/2 を設定し、外部インターフェイスとしてイーサネット 1/1 を設定した場合、これらのインターフェイスは内部および外部インターフェイスとしてデータノードでも使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

クラスタ インターフェイス

データインターフェイスは、スパンドEtherChannelとして設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータインターフェイスのタイプが同一であることが必要です。詳細については、クラスタ インターフェイスについて（414ページ）を参照してください。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、クラスタ制御リンク（414ページ）を参照してください。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

ASA クラスタ管理

ASAクラスタリングを使用することの利点の1つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理インターフェイスについては、専用管理インターフェイスの1つを使用することを推奨します。管理インターフェイスは、個別インターフェイスとして設定することも（ルーテッドモードとトランスペアレントモードの両方）、スパンドEtherChannelインターフェイスとして設定することもできます。

管理用には、個別インターフェイスを使用することを推奨します（スパンドEtherChannelをデータインターフェイスに使用している場合でも）。個別インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンドEtherChannelインターフェイスでは、現在の制御ユニットへのリモート接続しかできません。

（注） スパンドEtherChannelインターフェイスモードを使用しているときに、管理インターフェイスを個別インターフェイスとして設定する場合は、管理インターフェイスに対してダイナミックルーティングをイネーブルにすることはできません。スタティックルートを使用する必要があります。

個別インターフェイスの場合は、メインクラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の制御ユニットに属します。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ユニット（現在の制御ユニットも含まれます）がその範囲内のローカルアドレスを使用できるようになります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の制御ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、制御ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバーに接続します。

スパンド EtherChannel インターフェイスの場合は、IP アドレスは 1 つだけ設定でき、その IP アドレスは常に制御ユニットに関連付けられます。EtherChannel インターフェイスを使用してデータユニットに直接接続することはできません。管理インターフェイスは個別インターフェイスとして設定することを推奨します。各ユニットに接続できるようにするためです。デバイス ローカル EtherChannel を管理に使用できます。

制御ユニット管理とデータユニット管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。また、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。
- ノードごとのSyslogモニタリング（コンソールレプリケーションが有効な場合にコンソールに送信される Syslog を除く）。
- SNMP
- NetFlow

暗号キー複製

制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有のMACアドレスおよびIPアドレスを使用するのに対し、クラスタで受信したパケットは、グローバルMACアドレスおよびIPアドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト IDは、LISP インスペクションを使用するフローモビリティ、データセンターのサイト間クラスタリングのパフォーマンスを向上し、ラウンドトリップ時間の遅延を減少させるためのディレクタ ローカリゼーション、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトにある接続のサイト冗長性を有効にするためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：ASA クラスタリングの要件と前提条件 （404 ページ）
- サイト間のガイドライン：ASA クラスタリングのガイドライン （407 ページ）
- クラスタ フロー モビリティの設定：クラスタ フロー モビリティの設定 （446 ページ）

- ディレクタ ローカリゼーションの有効化：ASA クラスタの基本パラメータの設定 （438 ページ）
- サイト冗長性の有効化：ASA クラスタの基本パラメータの設定 （438 ページ）
- サイト間での例：サイト間クラスタリングの例 （476 ページ）

ASA クラスタリングのライセンス

クラスタユニットは、各ユニット上で同じライセンスを必要としません。一般的には、制御ユニット用のライセンスのみを購入します。データユニットは制御ユニットのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5516-X	基本ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
Firepower 4100/9300 シャーシ	Firepower 4100/9300 の ASA クラスタライセンス （172 ページ）を参照してください。
他のすべてのモデル	サポートしない

ASA クラスタリングの要件と前提条件

モデルの要件

- ASA 5516-x：最大 2 ユニット
- ASA 5525-X、5545-X、および 5555-X：最大 2 ユニット
- ASA FirePOWER モジュール：ASA FirePOWER モジュールはクラスタリングを直接サポートしていませんが、クラスタ内でこれらのモジュールを使用できます。クラスタ内の ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

ASA FirePOWER モジュールを設定する前に、クラスタを作成します。モジュールがデータユニットにすでに設定されている場合、クラスタにこれらを追加する前に、デバイスのインターフェイスの構成をクリアします。CLI から **clear configure interface** コマンドを入力します。

ASA のハードウェアおよびソフトウェア要件

クラスタ内のすべてのユニット：

- 同じ DRAM を使用する同じモデルである必要があります。フラッシュ メモリの容量は同一である必要はありません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレス アップグレードがサポートされます。
- セキュリティ コンテキスト モードが一致している必要があります（シングルまたはマルチ）。
- （シングル コンテキスト モード）ファイアウォール モードが一致している必要があります（ルーテッドまたはトランスペアレント）。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタメンバーは、制御ユニットと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。

スイッチ要件

- ASA でクラスタリングを設定する前に、スイッチのコンフィギュレーションを完了する必要があります。
- サポートされているスイッチのリストについては、『Cisco ASA Compatibility』[英語] を参照してください。

ASA の要件

- ユニットを管理ネットワークに追加する前に、一意の IP アドレスを各ユニットに提供します。
  - ASA への接続および管理 IP アドレスの設定に関する詳細については、「使用する前に」の章を参照してください。
  - 制御ユニット（通常は最初にクラスタに追加されたユニット）で使用される IP アドレスを除き、これらの管理 IP アドレスは一時的に使用されるだけです。

- データユニットがクラスタに参加すると、管理インターフェイス設定はマスターユニットからの複製に置き換えられます。

- クラスタ制御リンクでジャンボ フレームを使用する場合は（推奨）、クラスタリングをイネーブルにする前に、ジャンボ フレームの予約をイネーブルにする必要があります。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect（DCI）に確保する必要があります。

$$\frac{\#\text{ of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCI の最小帯域幅は、1 つのメンバーに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバーの場合。
  - 合計 4 クラスタ メンバー
  - 各サイト 2 メンバー
  - メンバーあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。
- 3 サイトの 6 メンバーの場合、サイズは増加します。
  - 合計 6 クラスタ メンバー
  - サイト 1 は 3 メンバー、サイト 2 は 2 メンバー、サイト 3 は 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。
- 2 サイトの 2 メンバーの場合。
  - 合計 2 クラスタ メンバー
  - 各サイト 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

その他の要件

ターミナル サーバーを使用して、すべてのクラスタ メンバ ユニットのコンソール ポートにアクセスすることをお勧めします。初期設定および継続的な管理（ユニットがダウンしたときなど）では、ターミナル サーバーがリモート管理に役立ちます。

ASA クラスタリングのガイドライン

コンテキスト モード

モードは、各メンバー ユニット上で一致している必要があります。

ファイアウォール モード

シングル モードの場合、ファイアウォール モードがすべてのユニットで一致している必要があります。

フェールオーバー

フェールオーバーは、クラスタリングではサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

スイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンク インターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンク インターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一

に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシング アルゴリズムは変更しないでください。

- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

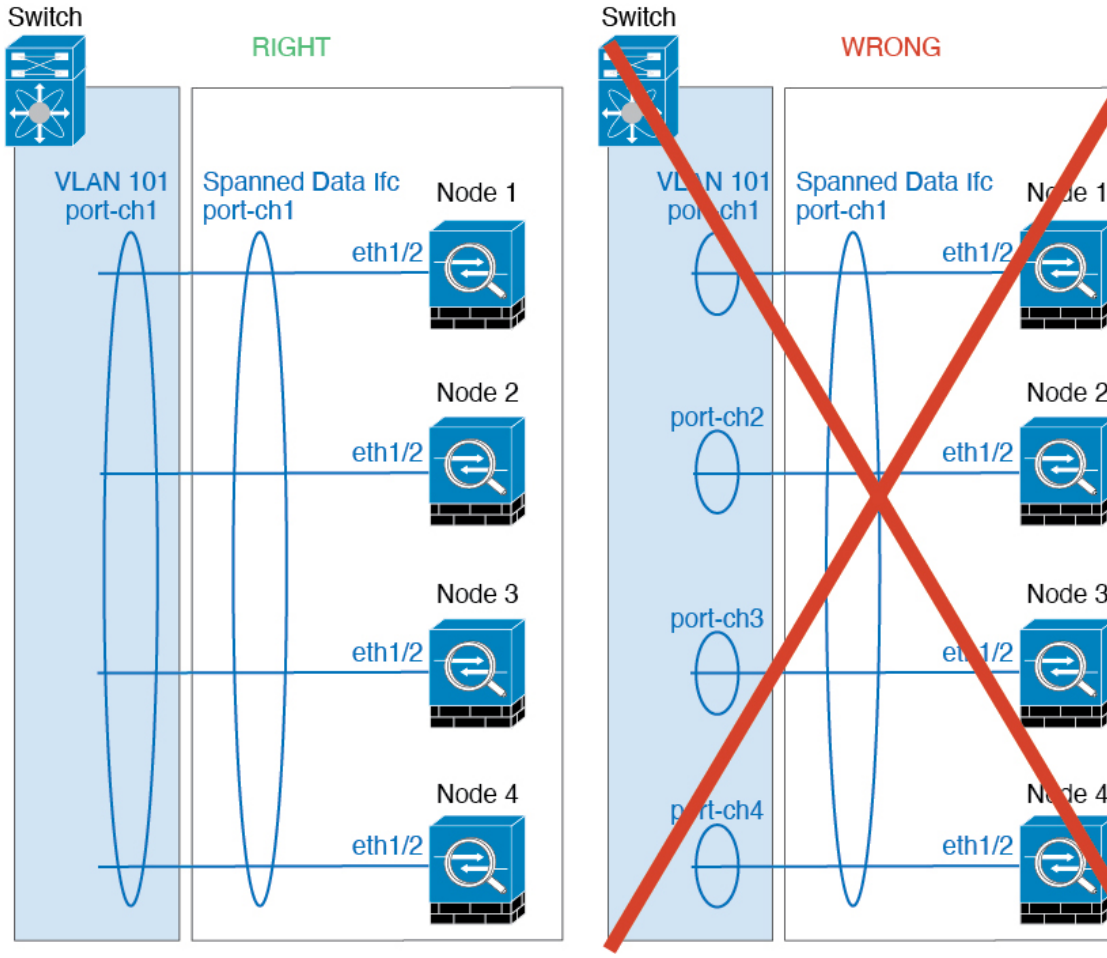
  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能をディセーブルにする必要があります。

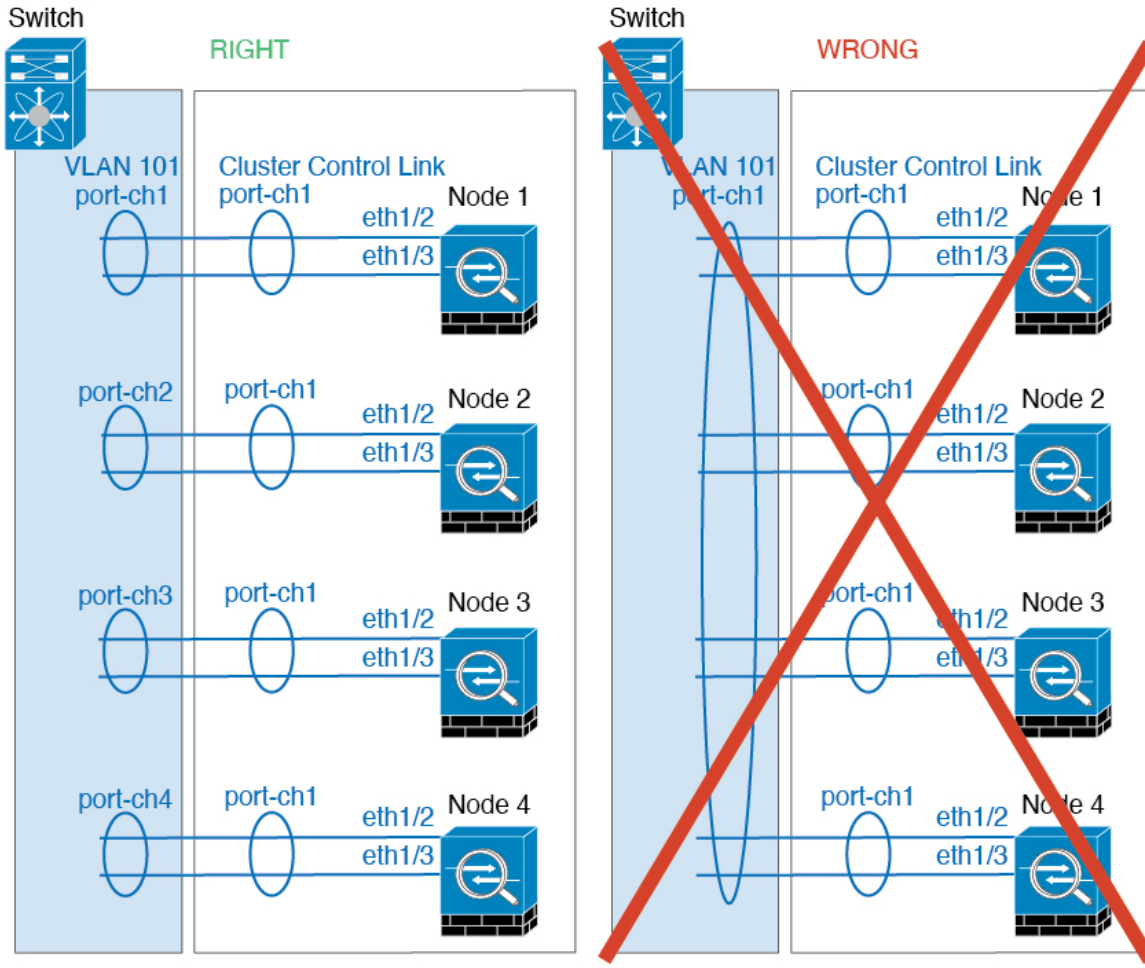
EtherChannel

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単

一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間のガイドライン

サイト間クラスタリングについては、次のガイドラインを参照してください。

- 次のインターフェイスおよびファイアウォールモードで Inter-Site クラスタリングをサポートします。

インターフェイス モード	ファイアウォール モード	
	ルーテッド	トランスペアレント
個別インターフェイス	○	該当なし
スパンド EtherChannel	対応	対応

- 個別インターフェイス モードでは、マルチキャスト ランデブー ポイント（RP）に向けて ECMP を使用する場合、ネクストホップとしてメイン クラスタ IP アドレスを使用する RP IP アドレスのスタティック ルートを使用することをお勧めします。このスタティック ルートは、データユニットにユニキャスト PIM 登録パケットが送信されるのを防ぎます。デー

タユニットがPIM登録パケットを受け取った場合、パケットはドロップされ、マルチキャストストリームは登録できません。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- ASAは専用リンクであるため、データセンター相互接続（DCI）で使用されている場合でも、クラスタ制御リンクで転送されるデータトラフィックを暗号化しません。オーバーレイトランスポート仮想化（OTV）を使用する場合、またはローカル管理ドメインの外部でクラスタ制御リンクを拡張する場合は、OTE を介した 802.1AE MacSec などの境界ルータで暗号化を設定できます。
- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタ ローカリゼーションを有効にすると、ローカル ディレクタのロールは（サイト ID に従って）常に接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。
- ディレクタ ローカリゼーションでは、次のトラフィック タイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション クエリ。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じMACアドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバーがサイト 2 のメンバーに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイアウォール用に各サイトのデータ ネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想IPおよびMACアドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカルゲートウェイ ルータ宛てのトラフィックがDCI経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが1つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。

- トランスペアレントモードでは、クラスタがHSRPルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして ASA に追加する必要があります（ブリッジ グループのスタティック MAC アドレスの追加 （830 ページ）を参照）。隣接ルータで HSRP が使用される場合、HSRP IP アドレス宛てのトラフィックは HSRP MAC アドレスに送信されますが、リターントラフィックは特定のルータのインターフェイスの MAC アドレスから HSRP ペアで送信されます。したがって、ASA MACアドレステーブルは通常、HSRP IPアドレスの ASA ARP テーブルエントリが期限切れになり、ASA が ARP 要求を送信して応答を受信した場合にのみ更新されます。ASA の ARP テーブルエントリはデフォルトで 14400 秒後に期限切れになりますが、MAC アドレステーブルエントリはデフォルトで 300 秒後に期限切れになるため、MAC アドレステーブルの期限切れトラフィックのドロップを回避するために静的 MAC アドレスエントリが必要です。
- スパンド EtherChannel を使用したルーテッド モードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが 1 つのサイトで到達不能になった場合、トラフィックが他のサイトのクラスタノードに正常に到達できるようにフィルタを削除する必要があります。ダイナミック ルーティングは、サイト間クラスタが拡張セグメントのファースト ホップ ルータとして機能する場合はサポートされません。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、ASA 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイス モニターリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバー ポートがダウンし、サーバーが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージが ASA クラスタに送信されます。このようなメッセージにより、ASA クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 個別インターフェイス モードの VXLAN はサポートされていません。スパンド EtherChannel モードでのみ VXLAN をサポートしています。
- シスコは、スパンド EtherChannel モードの IS-IS をサポートしません。個別インターフェイス モードのみが IS-IS をサポートします。

- クラスタ内のすべてのユニットに変更が複製されるまでには時間がかかります。たとえば、オブジェクトグループを使用するアクセスコントロールルール（展開時に複数のルールに分割される）を追加するなどの大きな変更を行うと、変更の完了に必要な時間がクラスタユニットが成功メッセージで応答できるタイムアウトを超える可能性があります。この場合、「failed to replicate command」というメッセージが表示されることがあります。このメッセージは無視できます。

ASA クラスタリングのデフォルト

- スパンド EtherChannel を使用するときは、cLACP システム ID は自動生成され、システムプライオリティはデフォルトで 1 です。
- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が5分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

ASA クラスタリングの設定

クラスタリングを設定するには、次のタスクを実行します。

（注） クラスタリングを有効または無効にするには、コンソール接続（CLIの場合）またはASDM接続を使用します。

コンフィギュレーションのバックアップ（推奨）

データユニットでクラスタリングをイネーブルにすると、現在のコンフィギュレーションは同期したアクティブユニットの設定に置き換えられます。クラスタ全体を解除する場合、使用可能な管理インターフェイス コンフィギュレーションのバックアップ コンフィギュレーションを取っておくと役立つ場合があります。

始める前に

各ユニットのバックアップを実行します。

手順

ステップ 1 **[ツール（Tools）] > [バックアップ設定（Backup Configurations）]** を選択します。

ステップ 2 最低でも実行コンフィギュレーションをバックアップします。詳細な手順については、コンフィギュレーションまたはその他のファイルのバックアップと復元（1209 ページ）を参照してください。

ユニットのケーブル接続およびインターフェイスの設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。次に、インターフェイスを設定します。

クラスタ インターフェイスについて

データインターフェイスは、スパンドEtherChannelとして設定することも、個別インターフェイスとして設定することもできます。1 つのクラスタ内のすべてのデータインターフェイスのタイプが同一であることが必要です。また、各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。可能な場合は、クラスタ制御リンクにEtherChannelを使用することを推奨します。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 状態の複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク インターフェイスとネットワーク

次の例外を除き、クラスタ制御リンクには任意のデータ インターフェイスを使用できます。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。

- 管理 *x/x* インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。

EtherChannel インターフェイスまたは冗長インターフェイスを使用できます。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、ASA クラスタ制御リンク インターフェイスだけが含まれるようにしてください。

2 メンバー クラスタの場合、ASA と ASA の間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンクのサイジング

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- ネットワークアクセスに対する AAA は一元的な機能であるため、すべてのトラフィックが制御ユニットに転送されます。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

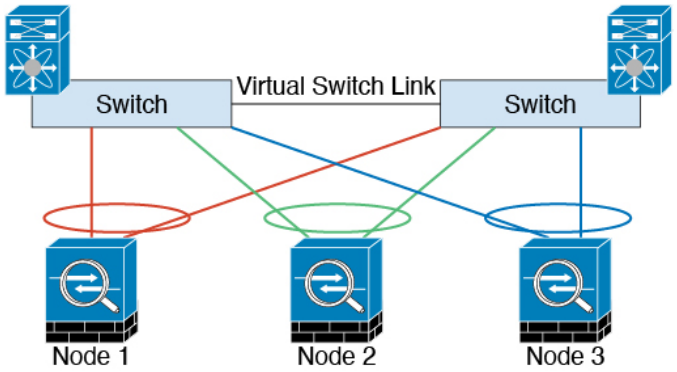
（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンクの冗長性

クラスタ制御リンクにはEtherChannelを使用することを推奨します。冗長性を実現しながら、EtherChannel 内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリン

クがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内のファイアウォール インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

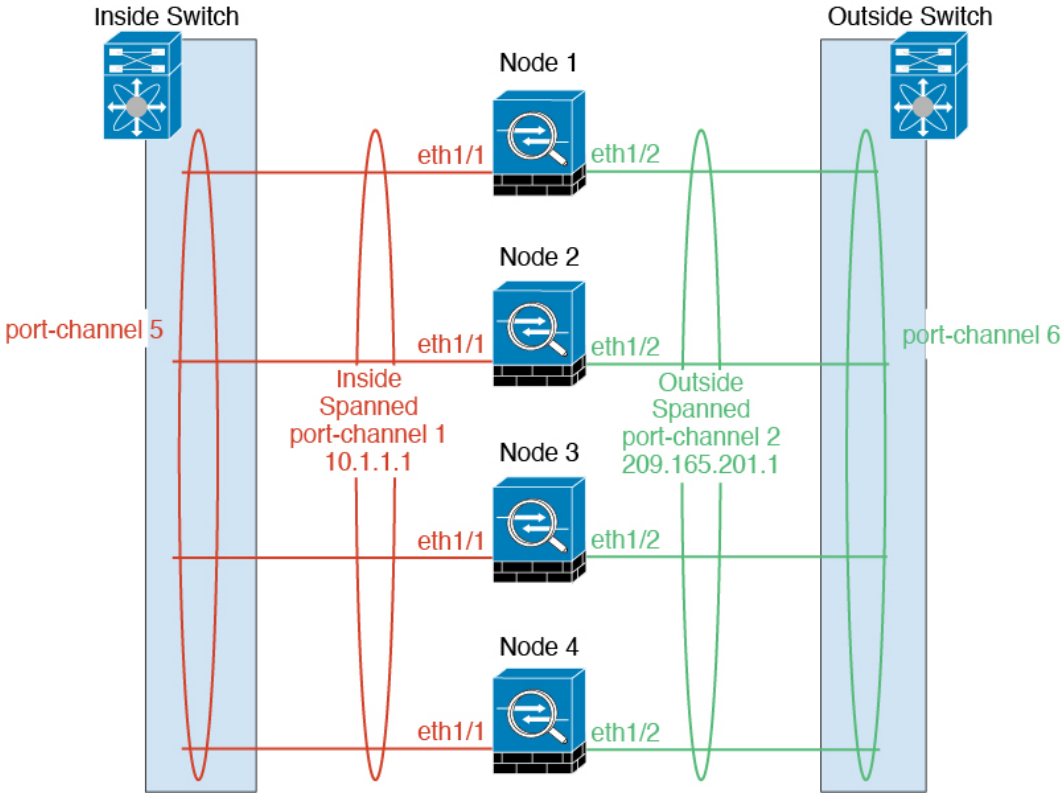
クラスタ制御リンクの障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャット ダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。

（注） ASA が非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（制御ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

スパンド EtherChannel（推奨）

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォールモードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジ グループ メンバのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



スパンド *EtherChannel* の利点

EtherChannel 方式のロードバランシングは、次のような利点から、他の方式よりも推奨されます。

- 障害検出までの時間が短い。
- コンバージェンス時間が短い。個別インターフェイスはルーティング プロトコルに基づきトラフィックをロード バランシングしますが、ルーティング プロトコルはリンク障害時にコンバージェンスが遅くなることがよくあります。
- コンフィギュレーションが容易である。

最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロード バランシング ハッシュ アルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内の同じ ASA に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュ アルゴリズムとして使用することを推奨します。
- ASA をスイッチに接続するときは、同じタイプのライン カードを使用します。すべてのパケットに同じハッシュ アルゴリズムが適用されるようにするためです。

ロード バランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

（注） ASA では、デフォルトのロードバランシング アルゴリズムを変更しないでください。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。

EtherChannel 内のリンク数はロード バランシングに影響を及ぼします。

対称ロード バランシングは常に可能とは限りません。NAT を設定する場合は、フォワード パケットとリターン パケットとで IP アドレスやポートが異なります。リターン トラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターン トラフィックを正しいユニットにリダイレクトする必要があります。

EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコル ステータスをモニターします。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

VSS または *vPC* への接続

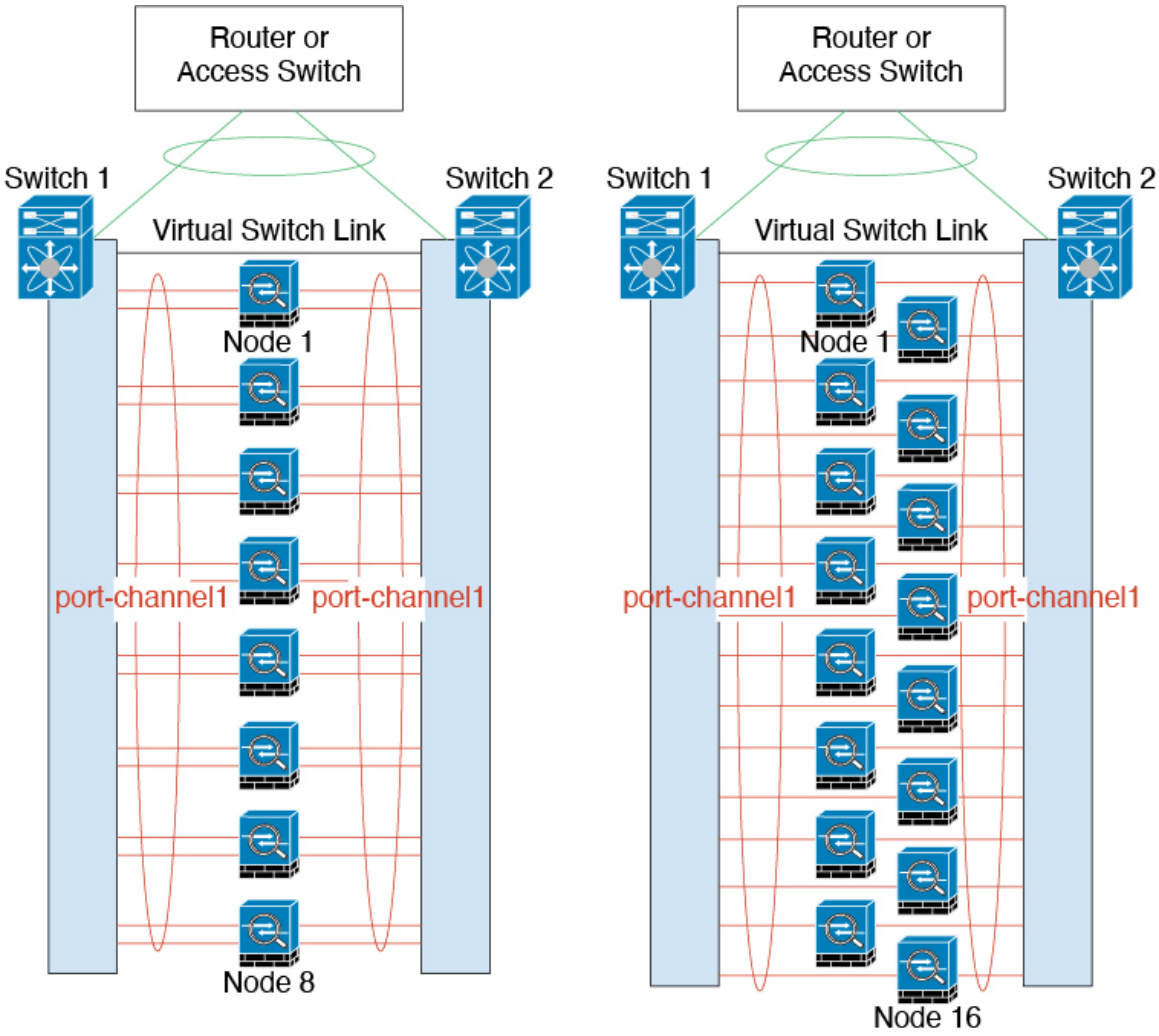
1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブ リンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

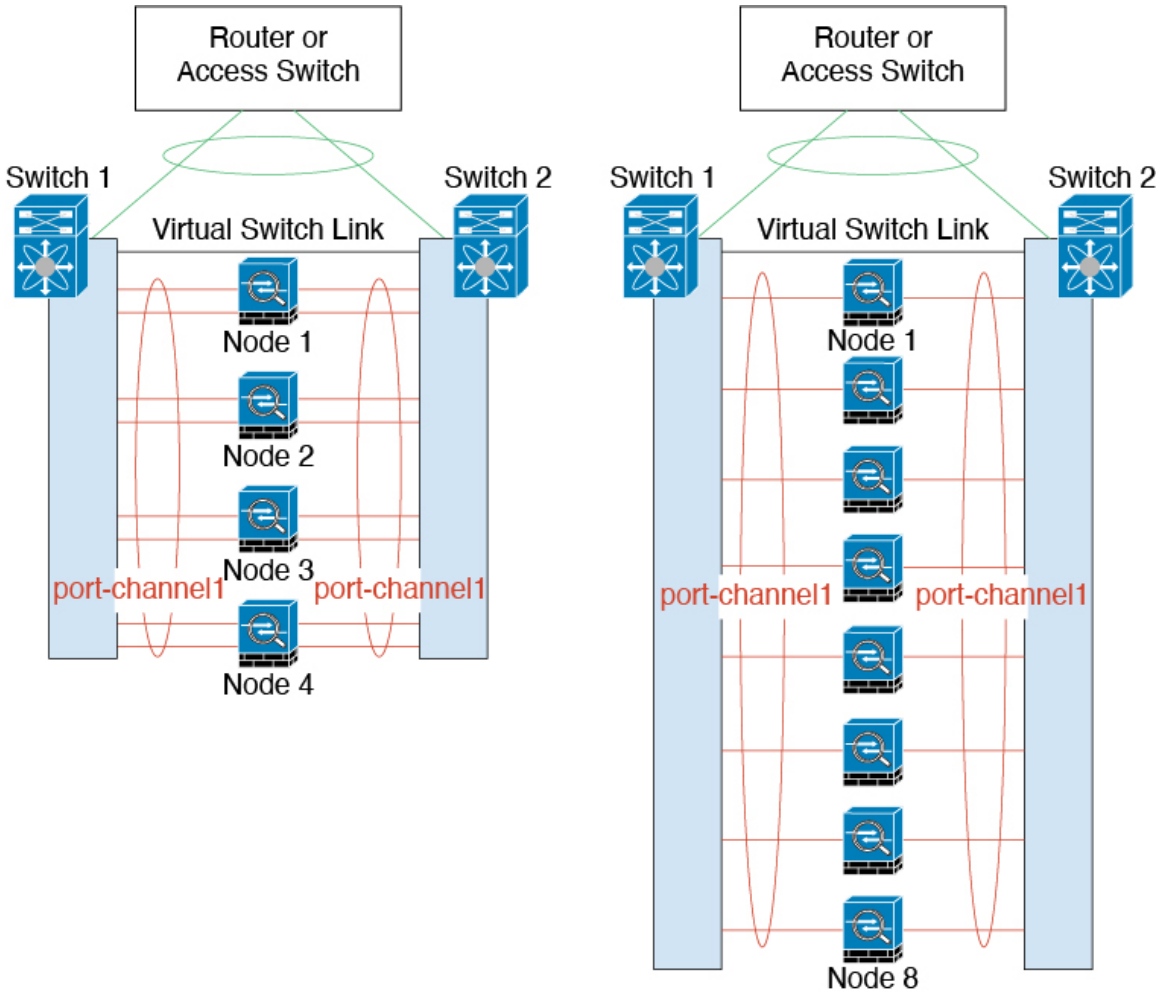
EtherChannel で 8 個のアクティブ リンクをサポートするスイッチの場合、VSS/vPC で 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブ リンクを設定できます。

スパンド EtherChannel で 8 個より多くのアクティブ リンクを使用する場合は、スタンバイ リンクも使用できません。9 ～ 32 個のアクティブ リンクをサポートするには、スタンバイ リンクの使用を可能にする cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。それでも、必要であれば、たとえば 1 台のスイッチに接続するときに、8 個のアクティブ リンクと 8 個のスタンバイ リンクを使用できます。

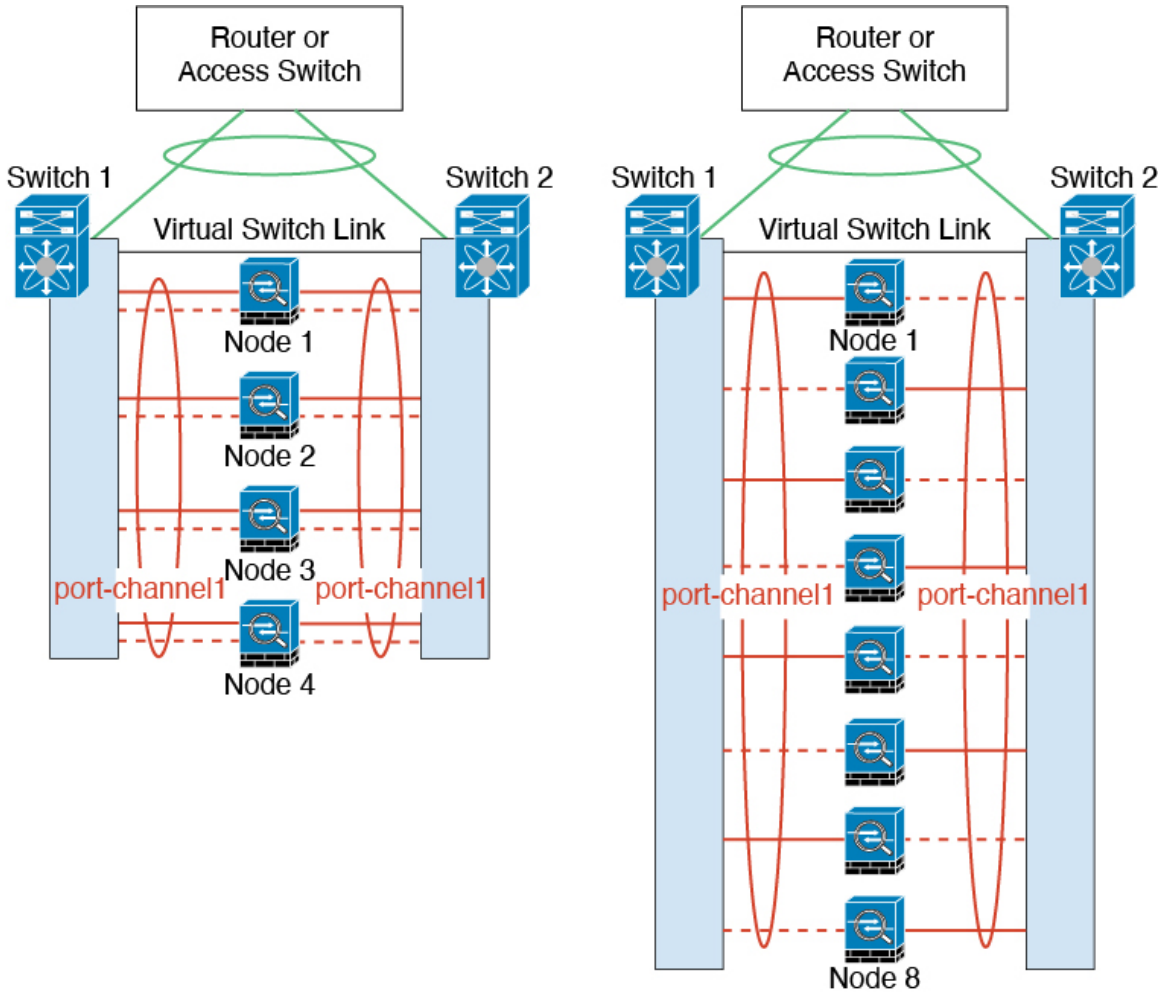
次の図では、8 ASA クラスタおよび 16 ASA クラスタでの 32 アクティブ リンクのスパンド EtherChannel を示します。



次の図では、4 ASA クラスタおよび 8 ASA クラスタでの 16 アクティブ リンクのスパンド EtherChannel を示します。

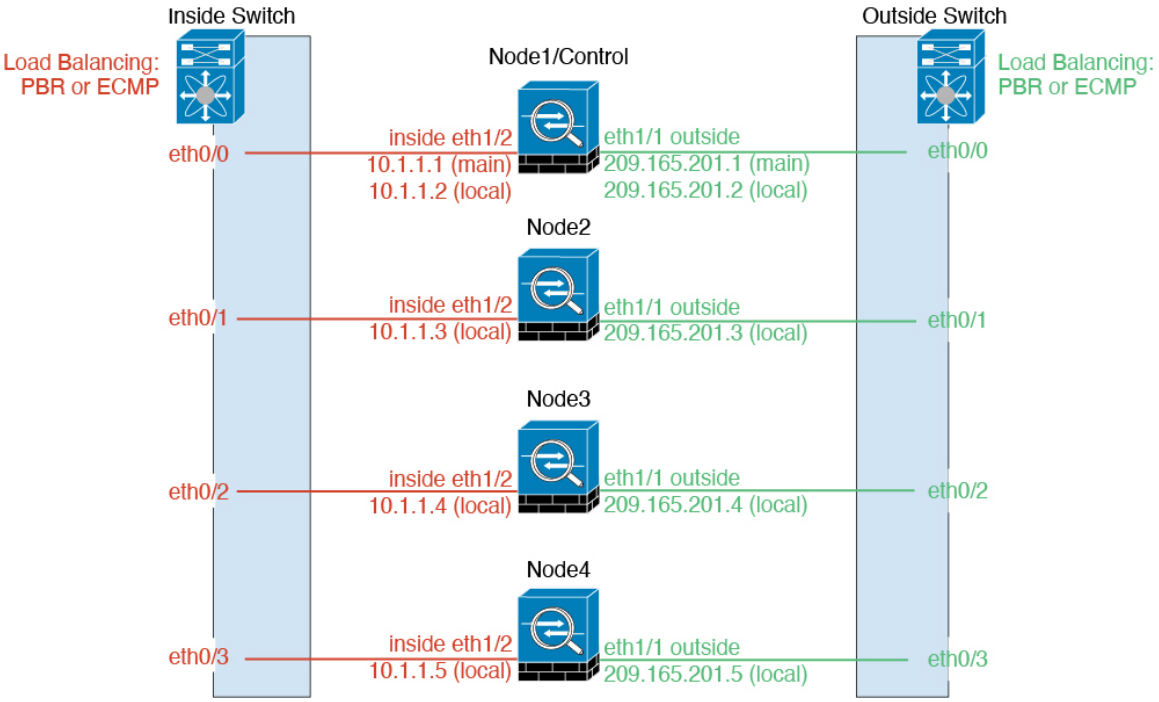


次の図では、4 ASA クラスタおよび 8 ASA クラスタでの従来の 8 アクティブ リンク/8 スタンバイ リンクのスパンド EtherChannel を示します。アクティブ リンクは実線で、非アクティブ リンクは点線で示しています。cLACP ロードバランシングは、EtherChannel のリンクのうち最良の 8 本を自動的に選択してアクティブにできます。つまり、cLACP は、リンク レベルでのロード バランシング実現に役立ちます。



個別インターフェイス（ルーテッド ファイアウォール モードのみ）

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のローカル *IP* アドレスを持ちます。インターフェイス コンフィギュレーションは制御ノード上だけで行う必要があるため、このインターフェイス コンフィギュレーションの中で IP アドレスプールを設定して、このプールのアドレスをクラスタノード（制御ノード用を含む）のインターフェイスに使用させることができます。メインクラスタ *IP* アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ノードに属します。ローカル IP アドレスは、常にルーティングの制御ノードアドレスです。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。ただし、ロード バランシングを別途する必要があります（この場合はアップストリーム スイッチ上で）。



ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロード バランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA 間で分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 ASA をモニターします。これで、PBR は、特定の ASA の到達可能性に基づいてルート マップをイネーブルまたはディセーブルにできます。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MACアドレスを維持します。ロードバランシング方法の1つが、等コストマルチパス（ECMP）ルーティングです。

この方法が推奨されるのは、すでにECMPを使用しており、既存のインフラストラクチャを活用したい場合です。

ECMPルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannelのように、送信元および宛先のIPアドレスや送信元および宛先のポートのハッシュを使用してネクストホップの1つにパケットを送信できます。ECMP ルーティングにスタティック ルートを使用する場合は、ASA の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニターリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA を設定する必要があります。

Nexus Intelligent Traffic Director（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。Intelligent Traffic Director（ITD）とは、Nexus 5000、6000、7000 および9000スイッチシリーズの高速ハードウェア ロードバランシング ソリューションです。従来の PBR の機能を完全に網羅していることに加え、簡略化された構成ワークフローを提供し、粒度の細かい負荷分散を実現するための複数の追加機能を備えています。

ITD は、IP スティッキ性、双方向フロー対称性のためのコンシステント ハッシュ法、仮想 IP アドレッシング、ヘルスモニターリング、高度な障害処理ポリシー（N+M冗長性）、加重ロードバランシング、およびアプリケーション IP SLA プローブ（DNS を含む）をサポートします。ロードバランシングの動的な性質により、PBR に比べて、すべてのクラスタ メンバーでより均一なトラフィック分散を実現します。双方向フロー対称性を実現するために、接続のフォワードおよびリターンパケットが同じ ASA に送信されるように ITD を設定することを推奨します。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

クラスタユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

手順

クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

（注） クラスタに参加するようにユニットを設定する前に、少なくとも、アクティブなクラスタ制御リンク ネットワークが必要です。

アップストリームとダウンストリームの機器も設定する必要があります。たとえば、EtherChannel を使用する場合は、EtherChannel のアップストリーム/ダウンストリーム機器を設定する必要があります。

制御ユニットでのクラスタ インターフェイス モードの設定

クラスタリング用に設定できるインターフェイスのタイプは、スパンドEtherChannel と個別インターフェイスのいずれか一方のみです。1 つのクラスタ内でインターフェイス タイプを混在させることはできません。

（注） 制御ユニットからデータユニットを追加しない場合は、制御ユニットだけでなく全ユニットのインターフェイスモードをこの項の説明に従って手動で設定する必要があります。制御ユニットからセカンダリユニットを追加する場合は、ASDM がデータユニットのインターフェイス モードを自動的に設定します。

始める前に

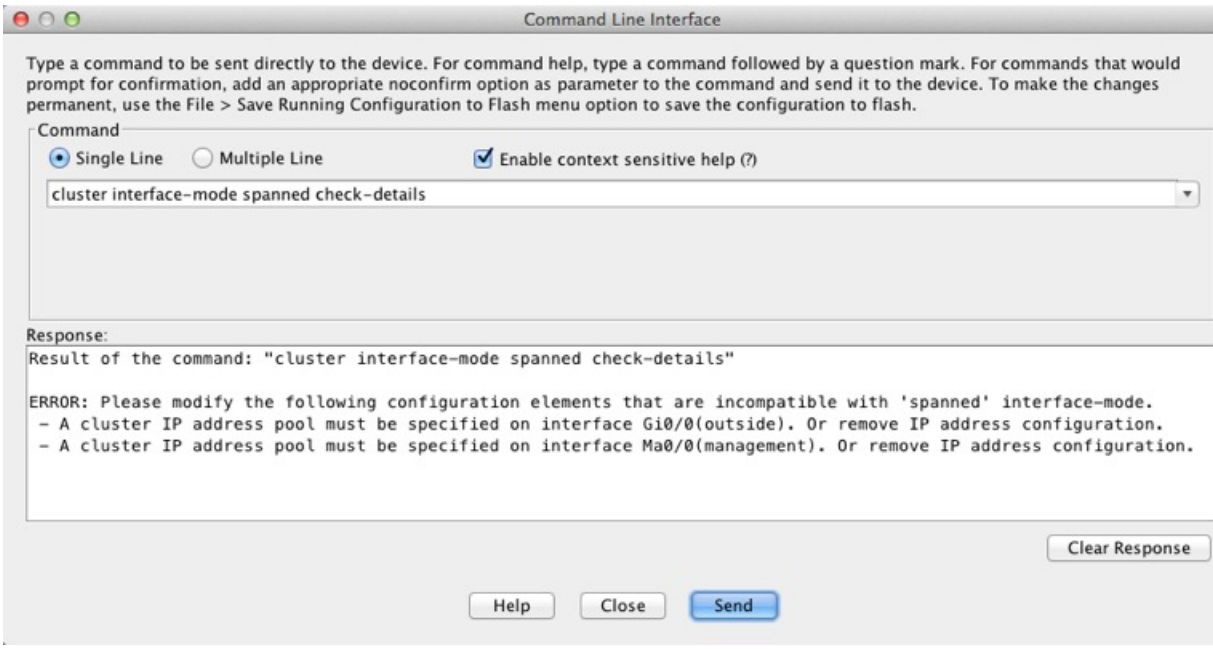
- 管理専用インターフェイスはいつでも、個別インターフェイス（推奨）として設定できます（スパンドEtherChannel モードのときでも）。管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。
- スパンドEtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミックルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。
- マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのインターフェイス タイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッド モードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレントモードで許可される唯一のインターフェイス タイプであるからです。

手順

ステップ 1 制御ユニットの ASDM で、**[Tools]** > **[Command Line Interface]** の順に選択します。互換性のないコンフィギュレーションを表示し、強制的にインターフェイス モードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

cluster interface-mode {**individual** | **spanned**} **check-details**

例：

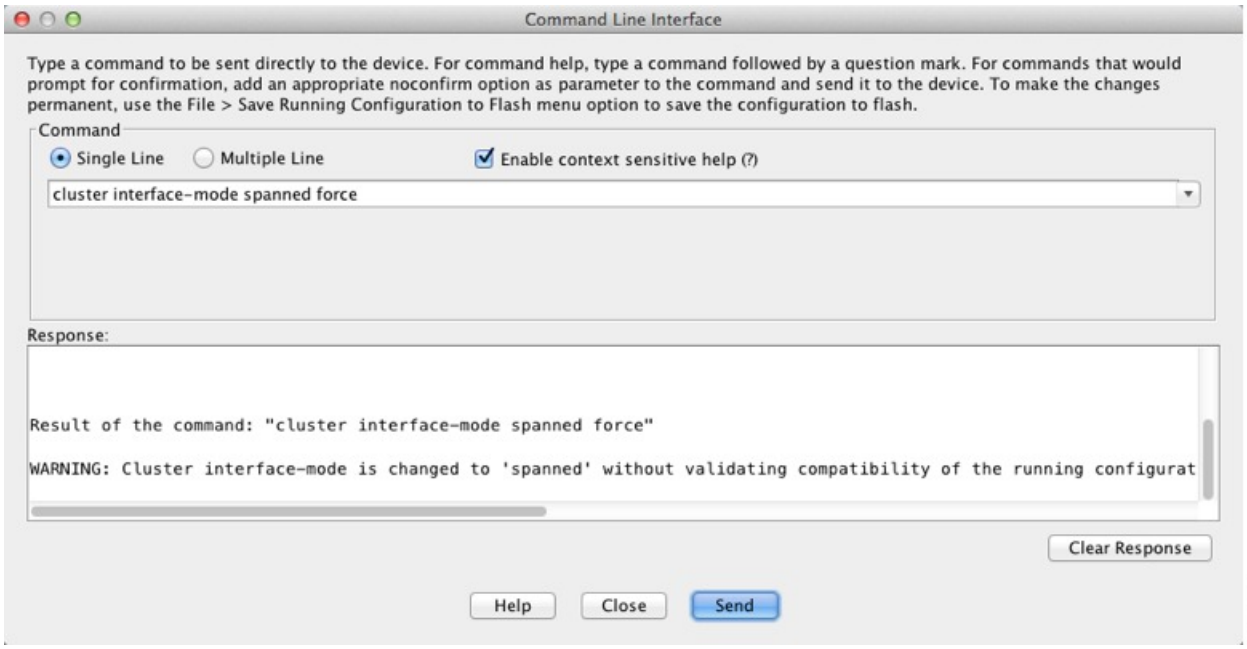


注意 インターフェイスモードを設定した後は、常にインターフェイスに接続できるようになります。ただし、クラスタリング要件に適合するように管理インターフェイスを設定する前にASAをリロードすると（たとえば、クラスタIPプールを追加するため）、クラスタと互換性のないインターフェイス コンフィギュレーションが削除されるため、再接続できなくなります。その場合は、コンソール ポートに接続してインターフェイス コンフィギュレーションを修正する必要があります。

ステップ2 クラスタリング用にインターフェイス モードを設定します。

cluster interface-mode {**individual** | **spanned**} **force**

例：



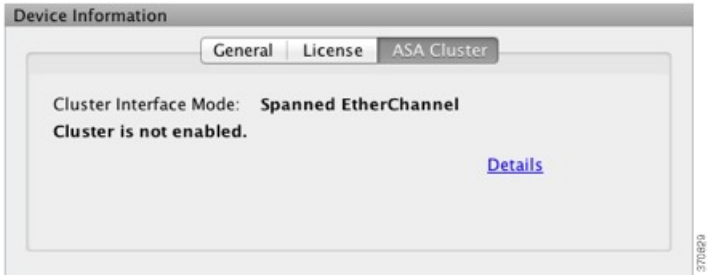
デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

force オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソール ポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

ステップ 3 ASDM を終了し、リロードします。クラスタ インターフェイス モードに正しく対応するように ASDM を再起動する必要があります。リロードの後、ホーム ページに [ASA Cluster] タブが表示されます。



（推奨、マルチコンテキストモードでは必須）制御ユニットでのインターフェイスの設定

クラスタリングを有効にする前に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。少なくとも、ASDM が現在接続されている管理インターフェイスを変更する必要があります。他のインターフェイスについては、クラスタリングをイネーブルにする前またはした後で設定できます。完全なコンフィギュレーションが新しいクラスタ メンバと同期するように、すべてのインターフェイスを事前に設定することを推奨します。 マルチ コンテキスト モードでは、この項の手順を使用して、既存のインターフェイスを修正するか、新しいインターフェイスを設定する必要があります。一方、シングルモードでは、この項を省略し、High Availability and Scalability ウィザードで共通インターフェイス パラメータを設定できます（高可用性ウィザードを使用したクラスタの作成または参加（434 ページ）を参照）。個別インターフェイス用の EtherChannel の作成などの高度なインターフェイス設定はウィザードでは実行できないことに注意してください。

ここでは、クラスタリング互換となるようにインターフェイスを設定する方法について説明します。データインターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。各方式は別のロードバランシング メカニズムを使用します。同じ構成で両方のタイプを設定することはできませんが、管理インターフェイスは例外で、スパンド EtherChannel モードであっても個別インターフェイスにできます。

個別インターフェイスの設定（管理インターフェイスに推奨）

個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メイン クラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のプライマリ ユニットに属します。

スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定することを推奨します。個別管理インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、現在のプライマリ ユニットへの接続しかできません。

始める前に

- 管理専用インターフェイスの場合を除き、個別インターフェイス モードであることが必要です。

- マルチ コンテキスト モードの場合は、この手順を各コンテキストで実行します。まだコンテキスト コンフィギュレーション モードに入っていない場合は、**changeto context** *name* コマンドを入力します。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- 個別インターフェイスの場合は、ネイバー デバイスでのロード バランシングを設定する必要があります。管理インターフェイスには、外部のロードバランシングは必要ありません。
- （オプション）インターフェイスをデバイスローカル EtherChannel インターフェイスとして設定する、冗長インターフェイスを設定する、およびサブインターフェイスを設定する作業を必要に応じて行います。
  - EtherChannel の場合、この EtherChannel はユニットに対してローカルであり、スパンド EtherChannel ではありません。
  - 管理専用インターフェイスを冗長インターフェイスにすることはできません。
- ASDM を使用して管理インターフェイスにリモートに接続している場合は、将来のセカンダリ ユニットの現在の IP アドレスは一時的なものです。
  - 各メンバには、プライマリ ユニットで定義されたクラスタ IP プールから IP アドレスが割り当てられます。
  - クラスタ IP プールには、将来のセカンダリ IP アドレスを含む、ネットワークですでに使用中のアドレスを含めることはできません。

    次に例を示します。

    1. プライマリ ユニットに 10.1.1.1 を設定します。
    2. 他のユニットには、10.1.1.2、10.1.1.3、10.1.1.4 を使用します。
    3. プライマリ ユニットのクラスタの IP プールを設定する場合、使用中であるために .2、.3、.4 のアドレスをプールに含めることはできません。
    4. 代わりに、.5、.6、.7、.8 のような、ネットワークの他の IP アドレスを使用する必要があります。

       注 プールには、プライマリ ユニットを含むクラスタのメンバ数分のアドレスが必要です。元の .1 アドレスはメイン クラスタ IP アドレスであり、現在のプライマリ ユニットのものです。

    5. クラスタに参加すると古い一時的なアドレスは放棄され、他の場所で使用できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** ペインを選択します。

ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。インターフェイスのパラメータを設定します。次のガイドラインを参照してください。

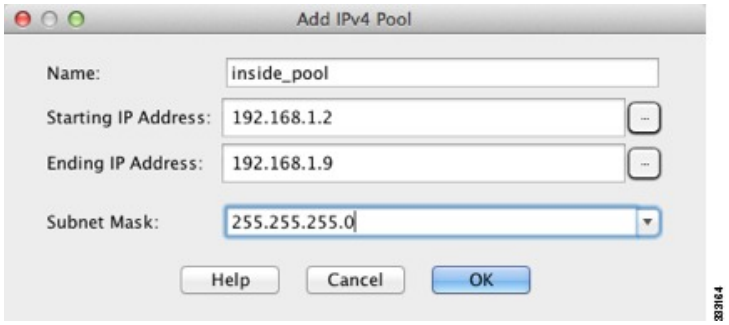
- （スパンド EtherChannel モードの管理インターフェイスでは必須）[このインターフェイスを管理専用にする（Dedicate this interface to management only）]：インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。デフォルトでは、管理タイプのインターフェイスは管理専用として設定されます。トランスペアレントモードでは、このコマンドは管理タイプのインターフェイスに対して常にイネーブルになります。
- [Use Static IP]：DHCP と PPPoE はサポートされません。

ステップ 3 IPv4 クラスタ IP プール、MAC アドレス プール、およびサイト別の MAC アドレスを追加するには、[Advanced] タブをクリックして、[**ASA Cluster**] エリア パラメータを設定します。

a) [IP Address Pool] フィールドの横にある [...] ボタンをクリックしてクラスタ IP プールを作成します。表示される有効範囲は、[General] タブで設定するメイン IP アドレスにより決定します。

b) [Add] をクリックします。

c) メイン クラスタの IP アドレスを含まないアドレス範囲を設定します。ネットワーク内で現在使用されているアドレスも含みません。範囲は、たとえば 8 アドレスというように、クラスタのサイズに合わせて十分に大きくする必要があります。



d) [OK] をクリックして、新しいプールを作成します。

e) 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。

プール名が [IP Address Pool] フィールドに表示されます。

f) （任意）（オプション）MAC アドレスを手動で設定する場合は、[MAC Address Pool] を設定します。

ステップ 4 IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

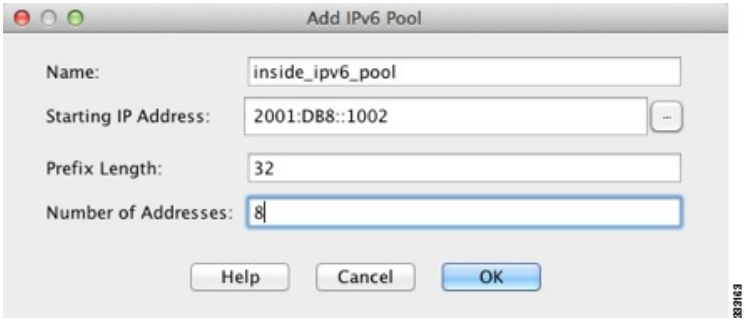
a) [Enable IPv6] チェックボックスをオンにします。

b) [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Enable address autoconfiguration] オプションはサポートされません。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

c) [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。
d) [...] ボタンをクリックして、クラスタ IP プールを設定します。
e) [Add] をクリックします。



f) プールの開始 IP アドレス（ネットワーク プレフィックス）、プレフィックス長、アドレス数を設定します。
g) [OK] をクリックして、新しいプールを作成します。
h) 作成した新しいプールを選択して、[Assign] をクリックし、次に [OK] をクリックします。

[ASA Cluster IP Pool] フィールドにプールが表示されます。

i) [OK] をクリックします。

ステップ 5 [OK] をクリックして、[Interfaces] ペインに戻ります。

ステップ 6 [適用（Apply）] をクリックします。

スパンド EtherChannel の設定

スパンド EtherChannel は、クラスタ内のすべての ASA に広がるものであり、EtherChannel の動作の一部としてロード バランシングを行うことができます。

始める前に

- スパンド EtherChannel インターフェイス モードにする必要があります。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。ブリッジ仮想インターフェイス（BVI）の設定 （685 ページ）を参照してください。
- EtherChannel には最大および最小のリンク数を指定しないでください。EtherChannel の最大および最小のリンク数の指定は、ASA とスイッチのどちらにおいても行わないことを推奨します。これらを使用する必要がある場合は、次の点に注意してください。

- ASA 上で設定されるリンクの最大数は、クラスタ全体のアクティブ ポートの合計数です。スイッチ上で設定された最大リンク数の値が、ASA での値を超えていないことを確認してください。
- ASA 上で設定される最小リンク数は、ポートチャネル インターフェイスを起動するための最小アクティブ ポート数（ユニットあたり）です。スイッチ上では、最小リンク数はクラスタ全体の最小リンク数であるため、この値は ASA での値とは一致しません。

- デフォルトのロードバランシング アルゴリズムを変更しないでください。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。
- スパンド EtherChannel を使用している場合、クラスタリングが完全にイネーブルになるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 **[Add]** > **[EtherChannel Interface]** の順に選択します。

[Add EtherChannel Interface] ダイアログボックスが表示されます。

ステップ 3 次をイネーブルにします。

- **[Port Channel ID]**
- **[Span EtherChannel across the ASA cluster]**
- [**Enable Interface**]（デフォルトでオンになります）
- [Members in Group]：[Members in Group] リストに、インターフェイスを少なくとも 1 つ追加する必要があります。ユニットごとに複数のインターフェイスが EtherChannel に含まれていると、VSS または vPC のスイッチに接続する場合に役立ちます。デフォルトでは、クラスタの全メンバで最大 16 個のアクティブ インターフェイスのうち、スパンド EtherChannel が使用できるのは 8 個だけであることに注意してください。残りの 8 インターフェイスはリンク障害時のためのスタンバイです。8 個より多くのアクティブ インターフェイスを使用するには（ただしスタンバイ インターフェイスではなく）、ダイナミック ポート プライオリティをディセーブルにします。ダイナミック ポート プライオリティを

ディセーブルにすると、クラスタ全体で最大 32 個のアクティブ リンクを使用できます。たとえば、16 台の ASA から成るクラスタの場合は、各 ASA で最大 2 個のインターフェイスを使用でき、スパンド EtherChannel の合計は 32 インターフェイスとなります。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。

この画面の残りのフィールドは、この手順の後半で説明します。

ステップ 4 （オプション）すべてのメンバー インターフェイスについて、メディア タイプ、二重通信、速度、フロー制御のポーズ フレームを上書きするには、[Configure Hardware Properties] をクリックします。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

[OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 5 MAC アドレスおよびオプション パラメータを設定するには、[Advanced] タブをクリックします。

- [MAC Address Cloning] 領域で、EtherChannel の手動グローバル MAC アドレスを設定します。スタンバイ MAC アドレスを設定しないでください。無視されます。潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在の制御ユニットに留まります。MAC アドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

  マルチコンテキスト モードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

- （ルーテッド モード）サイト間クラスタリングの場合、[ASA Cluster] 領域で、**サイト固有の MAC アドレス**および IP アドレスを設定するために、[Add] をクリックして、サイト ID（1 ～ 8）の MAC アドレスおよび IP アドレスを指定します。最大 8 つのサイトで上記の手順を繰り返します。サイト固有の IP アドレスは、グローバル IP アドレスと同じサブネット上にある必要があります。ユニットで使用するサイト固有の MAC アドレスおよび IP アドレスは、各ユニットのブートストラップ コンフィギュレーションに指定したサイト ID によって異なります。

- （オプション）VSS または vPC の 2 台のスイッチに ASA を接続する場合は、[Enable load balancing between switch pairs in VSS or vPC mode] チェックボックスをオンにして、VSS ロード バランシングをイネーブルにする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。

  [Member Interface Configuration] 領域で、**1** または **2** のどちらのスイッチに特定のインターフェイスを接続するかを特定する必要があります。

（注） [Minimum Active Members] と [Maximum Active Members] は設定しないことを推奨します。

ステップ 6 （オプション）この EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 7 （マルチ コンテキスト モード）この手順を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

a) [OK] をクリックして変更内容を確定します。
b) インターフェイスを割り当てます。
c) ユーザーが設定するコンテキストを変更します。[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
d) [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択し、カスタマイズするポートチャネル インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 8 [General] タブをクリックします。

ステップ 9 （トランスペアレント モード）[Bridge Group] ドロップダウン リストから、このインターフェイスを割り当てるブリッジ グループを選択します。

ステップ 10 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 11 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

ステップ 12 （ルーテッド モード）IPv4 アドレスに対して [Use Static IP] オプション ボタンをクリックし、IP およびマスクを入力します。DHCP と PPPoE はサポートされません。ポイントツーポイント接続の場合、31 ビットのサブネットマスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。トランスペアレント モードの場合は、EtherChannel インターフェイスではなく、ブリッジ グループ インターフェイスの IP アドレスを設定します。

ステップ 13 （ルーテッド モード）IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

トランスペアレント モードの場合は、EtherChannel インターフェイスではなく、ブリッジ グループ インターフェイスの IP アドレスを設定します。

a) [Enable IPv6] チェックボックスをオンにします。
b) [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

（注） [Enable address autoconfiguration] オプションはサポートされません。

c) [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、2001:DB8::BA98:0:3210/64。
d) （オプション）ホスト アドレスとして Modified EUI-64 インターフェイス ID を使用するには、[EUI-64] チェックボックスをオンにします。この場合は、単に [Address/Prefix Length] フィールドにプレフィックスを入力します。
e) [OK] をクリックします。

ステップ 14 [OK] をクリックして、[Interfaces] 画面に戻ります。

ステップ 15 [Apply] をクリックします。

高可用性ウィザードを使用したクラスタの作成または参加

クラスタ内の各ノードがクラスタに参加するには、ブートストラップ設定が必要です。（制御ノードになる）1 台のノード上で High Availability and Scalability ウィザードを実行してクラスタを作成し、データノードを追加します。

（注） 制御ノードに対して、cLACP システム ID および優先順位のデフォルトを変更する場合、ウィザードは使用できず、クラスタを手動で設定する必要があります。

始める前に

- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- クラスタ制御リンクの MTU を最大の 9198 に設定することを推奨します。そのためには、この手順を続ける前に各ノードでジャンボフレームの予約を有効にする必要があります。ジャンボ フレームの予約には、ASA のリロードが必要です。
- クラスタ制御リンク インターフェイスに使用するインターフェイスは、接続されたスイッチでアップ状態になっている必要があります。
- 稼働中のクラスタにノードを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがありますが、これは想定内の動作です。

手順

ステップ 1 **[Wizards]** > **[High Availability and Scalability Wizard]** の順に選択します。次の手順でこのウィザードのガイドラインを確認してください。

ステップ 2 [Interfaces] 画面からは新しい EtherChannel を作成できません（クラスタ制御リンクを除く）。

ステップ 3 [ASA Cluster Configuration] 画面で、ブートストラップの設定を構成します。

- [メンバーの優先順位（Member Priority）]：制御ノード選定用に、このノードの優先順位を 1 ～ 100 の範囲内で設定します。1 が最高の優先順位です。
- [（ルーテッドモード、スパンド EtherChannel モード）サイトインデックス（(Routed mode; Spanned EtherChannel mode) Site Index）]：サイト間クラスタリングを使用する場合は、こ

のノードのサイト ID を設定して、サイト固有の MAC アドレス（1 ～ 8）が使用されるようにします。

- （オプション）[共有キー（Shared Key）]：クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。

- （オプション）[Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]：接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。

  （注） サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。

- （オプション）[クラスタ内のこのデバイスのヘルスモニタリングを有効にする（Enable health monitoring of this device within the cluster）]：クラスタ ノード ヘルス チェック機能を有効にします。ノードのヘルスを確認するため、ASA のクラスタノードはクラスタ制御リンクで他のノードにハートビート メッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。

  （注） 何らかのトポロジ変更を行うとき（たとえば、データインターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加など）は、ヘルス チェックをディセーブルにし、ディセーブルにしたインターフェイスのモニタリングもディセーブルにする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェックを再度有効にできます。

  - [デバイスが障害状態だと見なされるまでの待機時間（Time to Wait Before Device Considered Failed）]：この値は、ノードのキープアライブ ステータス メッセージの間隔を指定します。範囲は 0.3 ～ 45 秒です。デフォルトは 3 秒です。

  - （オプション）[Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support]：クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのノードがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバーインターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はハートビート メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。このオプションをイネーブルにすると、ASA はクラ

スタ制御リンクのすべてのEtherChannelインターフェイスでハートビートメッセージをフラッディングして、少なくとも1台のスイッチがそれを受信できることを確認します。

- （オプション）[コンソール出力を複製する（Replicate console output）]：データノードから制御ノードへのコンソール複製を有効にします。この機能はデフォルトで無効に設定されています。ASAは、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート1つだけです。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。
- [Cluster Control Link]：クラスタ制御リンク インターフェイスを指定します。
  - [MTU]：クラスタ制御リンクインターフェイスの最大伝送ノードを指定します。データインターフェイスの最大MTUより少なくとも100バイト高い値（1400 ～ 9198バイトの範囲）を指定します。デフォルトのMTUは1500バイトです。すでにジャンボフレームの予約を有効にしている場合は、MTUを最大値に設定することを推奨します。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。たとえば、最大MTUは9198バイトであるため、データインターフェイスの最大MTUは9098になり、クラスタ制御リンクは9198に設定できます。**注**：まだジャンボフレームの予約を有効にしていない場合は、ウィザードを終了し、ジャンボフレームを有効にしてから、この手順を再開する必要があります。

ステップ4 [ヘルスモニタリング対象のインターフェイス（Interfaces for Health Monitoring）]画面で、一部のインターフェイスを障害のモニタリング対象から除外できます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ASA Firepowerモジュールなどのハードウェアモジュールをモニタリング対象から除外するには、[サービスモジュールをクラスタのヘルスモニタリングから除外する（Exempt Service Module from Cluster health monitoring）]チェックボックスをオンにします。

（注） 何らかのトポロジ変更を行うとき（たとえば、データインターフェイスの追加または削除、ASAまたはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSSまたはvPCを形成するスイッチの追加など）は、ヘルスチェックをディセーブルにし、ディセーブルにしたインターフェイスのモニタリングもディセーブルにする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェックを再度有効にできます。

ステップ5 [インターフェイス自動再結合設定（Interface Auto Rejoin settings）]画面で、インターフェイスまたはクラスタ制御リンクで障害が発生した場合の自動再結合設定をカスタマイズします。タイプごとに、次のオプションを設定できます。

- [Maximum Rejoin Attempts]：クラスタへの再結合の試行回数を定義するために、[Unlimited]または0 ～ 65535の範囲で値を設定します。**0**は自動再結合をディセーブルにします。デ

フォルト値は、クラスタ インターフェイスの場合は [Unlimited]、データ インターフェイスの場合は **3** です。

- [Rejoin Interval]：再結合試行間隔の時間を定義するために、2 ～ 60 の範囲で間隔を設定します。デフォルト値は **5** 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [Interval Variation]：1 ～ 3 の範囲で設定して、間隔を増加させるかどうかを定義します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタインターフェイスの場合は **1**、データインターフェイスの場合は **2** です。

ステップ 6 [Finish] をクリックします。

ステップ 7 ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルトコンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するには [OK] をクリックします。[Cancel] をクリックすると、クラスタリングはイネーブルになりません。

しばらくすると、ASDM がクラスタをイネーブルにして ASA に再接続し、ASA がクラスタに追加されたことを確認する [Information] 画面が表示されます。

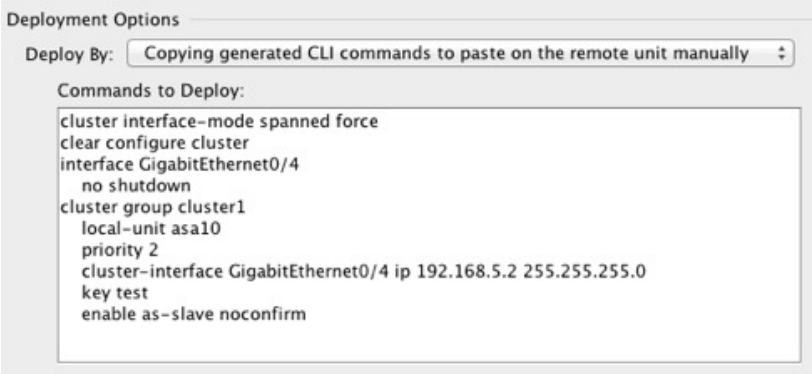
（注） 場合によっては、ウィザードの完了後にクラスタに参加した際にエラーが発生する可能性があります。ASDM が切断されていると、ASDM はそれに続くエラーを ASA から受信しません。ASDM に再接続した後もクラスタリングがディセーブルの場合は、ASA コンソール ポートに接続して、クラスタリングがディセーブルになっている詳細なエラー状況を判断する必要があります。たとえば、クラスタ制御リンクがダウンしている可能性があります。

ステップ 8 データノードを追加するには、[はい（Yes）] をクリックします。

制御ノードからウィザードを再実行する場合、ウィザードを最初に開始するときに [クラスタに別のメンバーを追加する（Add another member to the cluster）] オプションを選択してデータノードを追加できます。

ステップ 9 [Deployment Options] 領域で、次の [Deploy By] オプションのいずれかを選択します。

- [今すぐリモートユニットにCLIコマンドを送信する（Sending CLI commands to the remote unit now）]：ブートストラップ設定をデータノード（一時）管理 IP アドレスに送信します。データノード管理 IP アドレス、ユーザー名、パスワードを入力します。
- [生成された CLI コマンドを手動でコピーして、リモートユニットに貼り付ける（Copying generated CLI commands to paste on the remote unit manually）]：データノードの CLI でコマンドをカットアンドペーストできる、または ASDM の CLI ツールを使用できるようにコマンドを生成します。[Commands to Deploy] ボックスで、後で使用するためのコマンドを選択してコピーします。



クラスタリング動作のカスタマイズ

クラスタリング ヘルス モニターリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

制御ノードで次の手順を実行します。

ASA クラスタの基本パラメータの設定

制御ノード上のクラスタ設定をカスタマイズできます。クラスタへのノードの追加にウィザードを使用しない場合は、クラスタパラメータを手動で設定できます。すでにクラスタリングがイネーブルであれば、いくつかのクラスタ パラメータを編集できます。クラスタリングがイネーブルになっている間は編集できないものは、グレイ表示されます。この手順には、ウィザードに含まれていない高度なパラメータも含まれます。

始める前に

- ウィザードを使用せず、手動でクラスタに参加する場合は、クラスタに参加する前に、各ノードでクラスタ制御リンクインターフェイスを事前設定する必要があります。シングルインターフェイスの場合、イネーブルにする必要があります。他の設定を構成しないでください。EtherChannel インターフェイスの場合は、イネーブルにして、EtherChannel モードをオンに設定します。
- マルチコンテキストモードでは、制御ノード上のシステム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** の順に選択します。

すでにクラスタにデバイスが追加されていて、それが制御ノードの場合は、このペインは [クラスタ設定（Cluster Configuration）] タブにあります。

ステップ 2 [Configure ASA cluster settings] チェックボックスをオンにします。

チェックボックスをオフにすると、設定が消去されます。パラメータの設定がすべて完了するまで、[Participate in ASA cluster] をオンにしないでください。

（注） クラスタリングをイネーブルにした後、[Configure ASA cluster settings] チェックボックスをオフにする場合は、結果をよく理解したうえで行ってください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3 次のブートストラップ パラメータを設定します。

- [Cluster Name]：クラスタに名前を付けます。名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。ノードごとに設定できるクラスタは1つだけです。クラスタのすべてのメンバが同じ名前を使用する必要があります。
- [Member Name]：このクラスタ メンバの固有の名前を 1 ～ 38 文字の ASCII 文字列で指定します。
- [メンバーの優先順位（Member Priority）]：制御ノード選定用に、このノードの優先順位を 1 ～ 100 の範囲内で設定します。1 が最高の優先順位です。
- [（ルーテッドモード、スパンドEtherChannelモード）サイトインデックス（(Routed mode; Spanned EtherChannel mode) Site Index）]：サイト間クラスタリングを使用する場合は、このノードのサイト ID を設定して、サイト固有の MAC アドレス（1 ～ 8）が使用されるようにします。
- （オプション）[Site Periodic GARP]：ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチングインフラストラクチャを常に最新の状態に保ちます。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。各スパンド EtherChannel のノードと、サイト MAC および IP アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。GARP 間隔を 1 ～ 1000000 秒に設定します。デフォルトは 290 秒です。

  クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバ

ルMACアドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

- （オプション）[Shared Key]：クラスタ制御リンクの制御トラフィックの暗号キーを設定します。共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、暗号キーを生成するために使用されます。このパラメータは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリアテキストとして送信されます。パスワードの暗号化サービスをイネーブルにする場合にも、このパラメータを設定する必要があります。

- （オプション）[Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]：接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。

- [Enable cluster load monitor]：クラスタメンバのトラフィック負荷をモニターできるようになりました。対象には、合計接続数、CPUとメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのノードが負荷を処理できる場合は、ノードのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能はデフォルトでイネーブルになっています。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ノードでクラスタリングを手動で無効にすることを選択できます。

  次の値を設定します。

  - [**Time Interval**]: モニターリングメッセージ間の時間を、10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。

  - [**Number Of interval**]: ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

  トラフィック負荷を表示するには、**[Monitoring]** > **[ASA Cluster]** > **[Cluster Load-Monitoring]** を参照してください。

- （オプション）[クラスタ内でこのデバイスのヘルスモニタリングを有効にする（Enable health monitoring of this device within the cluster）]：クラスタノードのヘルスチェック機能を有効にして、ノード ハートビート ステータス メッセージ間の時間間隔を決定します。0.3 から 45 秒の間で選択できます。デフォルトは 3 秒です。**注**：新しいノードをクラスタに追加していて、ASA またはスイッチのトポロジが変更される場合、クラスタが完成するまでこの機能を一時的にディセーブルにし、ディセーブルにされたインターフェイスのインターフェイス モニタリングもディセーブルにする必要があります（**[構成（Configuration）] > [デバイス管理（Device Management）] > [ハイアベイラビリティとスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタインターフェイスヘルスモニタリング（Cluster Interface Health Monitoring）]**）。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ノードのヘルスを確認するため、ASAのクラスタノードはクラスタ制御リンクで他の

ノードにハートビート メッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。

- （オプション）[Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support]：クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合は、このオプションをイネーブルにすることが必要になる場合があります。一部のスイッチでは、VSS/vPC の 1 つのノードがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバーインターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はハートビートメッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。このオプションをイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでハートビートメッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。

- （オプション）[デバウンス時間（Debounce Time）]：ASA がインターフェイスを障害が発生していると見なし、クラスタからノードが削除されるまでのデバウンス時間を設定します。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからノードを削除するまで指定されたミリ秒数待機します。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。

- （オプション）[コンソール出力を複製する（Replicate console output）]：データノードから制御ノードへのコンソール複製を有効にします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート 1 つだけです。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。

- （オプション）**クラスタリング フロー モビリティをイネーブルにします。**LISP インスペクションの設定 （448 ページ）を参照してください。

- （オプション）[Enable Director Localization for inter-DC cluster]：データセンターのサイト間クラスタリングでパフォーマンスを向上させてラウンドトリップ時間の遅延を短縮するには、ディレクタ ローカリゼーションをイネーブルにします。通常、新しい接続はロードバランスされて、特定のサイト内のクラスタ メンバーにより所有されます。ただし、ASA はディレクタの役割を任意のサイトでメンバーに割り当てます。ディレクタ ローカリゼーションにより、追加のディレクタ役割がイネーブルになります。これは、所有者と同じサ

イトに存在するローカル ディレクタと、任意のサイトに配置できるグローバル ディレクタです。所有者とディレクタを同じサイトに配置することで、パフォーマンスが向上します。また、元の所有者で障害が発生した場合、ローカルディレクタは、同じサイトで新しい接続所有者を選択します。クラスタ メンバーが別のサイトで所有されている接続のパケットを受信する場合は、グローバル ディレクタが使用されます。

- （オプション）[Site Redundancy]：サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。ディレクタ ローカリゼーションとサイトの冗長性は別々の機能です。そのうちの 1 つまたは両方を設定することができます。
- （オプション）[構成同期アクセラレーションを有効にする（Enable config sync acceleration）]：データノードが制御ノードと同じ構成の場合、構成の同期をスキップし、結合を高速化します。この機能はデフォルトでイネーブルになっています。この機能は各ノードで設定され、制御ノードからデータノードに複製されません。

  （注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがノードに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。

- [並列構成のレプリケートを有効にする（Enable parallel configuration replicate）]：データノードと並行して設定変更が同期化されるように、制御ノードを有効にします。そうしないと、同期が順番に実行され、多くの時間がかかることがあります。
- [Cluster Control Link]：クラスタ制御リンク インターフェイスを指定します。このインターフェイスは、設定されている名前を使用できません。使用可能なインターフェイスがドロップダウン リストに表示されます。
  - [Interface]：インターフェイス ID、できればEtherChannelを指定します。サブインターフェイスと管理タイプ インターフェイスは許可されません。
  - [IP Address]：IP アドレスにはIPv4アドレスを指定します。IPv6は、このインターフェイスではサポートされません。
  - [Subnet Mask]：サブネット マスクを指定します。
  - [MTU]：クラスタ制御リンクインターフェイスの最大伝送ノードを指定します。データインターフェイスの最大 MTU より少なくとも 100 バイト高い値（1400 ～ 9198 バイトの範囲）を指定します。デフォルトのMTUは1500バイトです。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。クラスタ制御リンクの MTU を最大値に設定することを推奨します。そのためには、ジャンボフレームの予約を有効にする必要があります。ジャンボフレームの予約には、ASA のリロードが必要です。たとえば、最大MTUは9198バイトであるため、データインターフェイスの最大MTUは9098になり、クラスタ制御リンクは 9198 に設定できます。

- （オプション）[Cluster LACP]：スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間でEtherChannelのネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの（仮想）デバイスであるかのように見えます。
  - [Enable static port priority]：LACP のダイナミック ポート プライオリティをディセーブルにします。一部のスイッチはダイナミック ポート プライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。さらに、8 個より多くのアクティブなスパンドEtherChannelメンバのサポートがイネーブルになります（最大 32 メンバ）。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。
  - [Virtual System MAC Address]：MAC アドレス形式である cLACP システム ID を設定します。すべての ASA が同じシステム ID を使用します。これは制御ノードによって自動生成され（デフォルト）、すべてのセカンダリノードに複製されます。あるいは *H.H.H* の形式で手動で指定することもできます。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。ただし、この値は、クラスタリングを無効にした場合にのみ変更できます。
  - [System Priority]：1 ～ 65535 の範囲でシステム プライオリティを設定します。プライオリティは意思決定を担当するノードの決定に使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。このパラメータは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。ただし、この値は、クラスタリングを無効にした場合にのみ変更できます。

ステップ 4 [Participate in ASA cluster] チェックボックスをオンにして、クラスタに参加します。

ステップ 5 [Apply] をクリックします。

インターフェイスのヘルス モニターリングおよび自動再結合の設定

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニターリングをディセーブルにすることができます。任意のポート チャネル ID、冗長 ID、単一の物理インターフェイス ID、またはASA Firepowerモジュールなどのソフトウェア/ハードウェア モジュールをモニターできます。ヘルス モニターリングは VLAN サブインターフェイス、または VNI やBVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニターリングは設定できません。このリンクは常にモニターされています。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Interface Health Monitoring]** の順に選択します。

ステップ 2 [Monitored Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックして [Unmonitored Interfaces] ボックスにそのインターフェイスを移動します。

インターフェイス ステータス メッセージによって、リンク障害が検出されます。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニターリングをディセーブルにすることができます。ポートチャネル ID と冗長 ID、または単一の物理インターフェイス ID を指定できます。ヘルス モニターリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニターリングは設定できません。このリンクは常にモニターされています。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ASA またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし（**[構成（Configuration）]** > **[デバイス管理（Device Management）]** > **[高可用性とスケーラビリティ（High Availability and Scalability）]** > **[ASAクラスタ（ASA Cluster）]**）、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

ステップ 3 （任意） ASA FirePOWER モジュールなどのハードウェアまたはソフトウェア モジュールを免除するには、[Exempt Service Module from Cluster Health Monitoring] チェックボックスをオンにします。

ステップ 4 インターフェイス、システム、またはクラスタ制御リンクに障害が発生した場合の自動再結合の設定をカスタマイズするには、[Auto Rejoin] タブをクリックします。各タイプに関して **[Edit]** をクリックして次の設定を行います。

- [Maximum Rejoin Attempts]：クラスタへの再結合の試行回数を定義するために、[Unlimited] または 0 ～ 65535 の範囲で値を設定します。**0** は自動再結合をディセーブルにします。デフォルト値は、クラスタ インターフェイスの場合は [Unlimited]、データ インターフェイスおよびシステムの場合は [3] です。
- [Rejoin Interval]：再結合試行間隔の時間を定義するために、2 ～ 60 の範囲で間隔を設定します。デフォルト値は **5** 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。

- [Interval Variation]：1 ～ 3 の範囲で設定して、間隔を増加させるかどうかを定義します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタ インターフェイスの場合は [1]、データ インターフェイスおよびシステムの場合は [2] です。

デフォルト設定に戻すには、[Restore Defaults] をクリックします。

ステップ 5 [適用（Apply）] をクリックします。

クラスタ TCP 複製の遅延の設定

TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップ フローが作成される前にユニットが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のユニットに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster Replication]**.の順に選択します。

ステップ 2 [Add] をクリックして次の値を設定します。

- [Replication delay]：1 ～ 15 の範囲で秒数を設定します。
- [HTTP]：すべての HTTP トラフィックの遅延を設定します。
- **[Source Criteria]**
  - [Source]：送信元 IP アドレスを設定します。
  - [Service]：（オプション）送信元ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。
- **[Destination Criteria]**
  - [Source]：宛先 IP アドレスを設定します。
  - [Service]：（オプション）宛先ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。

ステップ 3 [OK] をクリックします。

ステップ 4 [Apply] をクリックします。

サイト間機能の設定

サイト間クラスタリングの場合、冗長性と安定性を高めるために、設定をカスタマイズできます。

クラスタ フロー モビリティの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

LISP インスペクションについて

LISP トラフィックを検査することで、サイト間のフローのモビリティを有効にできます。

LISP について

VMware vMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンター サーバ モビリティをサポートするには、サーバの移動時にサーバへの入力ルートをルータが更新できる必要があります。Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID、つまりエンドポイント ID（EID）をその場所、つまりルーティング ロケータ（RLOC）から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

LISP では、LISP の出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、ファースト ホップ ルータ、マップ リゾルバ（MR）、およびマップ サーバ（MS）などのある一定のロールにおいてルータとサーバが必要です。サーバが別のルータに接続されていることをサーバのファースト ホップ ルータが感知すると、そのルータは他のすべてのルータとデータベースを更新し、クライアントに接続されている ITR がトラフィックを代行受信してカプセル化し、新しいサーバの場所に送信できるようにします。

ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISP の統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフロー オーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーニング」または「ヘアピニング」と呼ばれます。

LISP 統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR 間でやり取りされる LISP トラフィックを検査し、フローの所有者を新しいサイトに変更できます。

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。

- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々のノードに属しているフローは新しいオーナーには移動されません。半分散されたフローにはSIPなどのアプリケーションが含まれており、親フローとそのすべての子フローが同じASAによって所有されます。
- クラスタはレイヤ3および4のフロー状態を移動させるだけです。一部のアプリケーション データが失われる可能性があります。
- 短時間のフローまたはビジネスに不可欠でないフローの場合、オーナーの移動は有用でない可能性があります。インスペクション ポリシーを設定するときに、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

ASA LISP の実装

この機能には、複数の相互に関係する設定が含まれています（それらについてはすべてこの章で説明します）。

1. （任意）ホストまたはサーバIPアドレスに基づく検査対象EIDの制限：ファースト ホップ ルータは、ASAクラスタが関与していないホストまたはネットワークにEID通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネットワークのみにEIDを制限できます。たとえば、クラスタが2つのサイトのみに関与しているが、LISPが3つのサイトで実行されている場合は、クラスタに関与している2つのサイトに対してのみEIDを含める必要があります。
2. LISPトラフィック インスペクション：ASAは、ファーストホップルータとITRまたはETRの間で送信されるEID通知メッセージにおいて、UDPポート4342上のLISPトラフィックを検査します。ASAは、EIDとサイトIDを関連付けるEIDテーブルを保持します。たとえば、最初のホップ ルータの送信元IPアドレスとITRまたはETRの宛先アドレスをもつLISPトラフィックを検査する必要があります。LISPトラフィックにはディレクタが割り当てられておらず、LISPトラフィック自体はクラスタ状態の共有に参加しないことに注意してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPSトラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。
4. サイトID：ASAは、各クラスタノードのサイトIDを使用して新しいオーナーを特定します。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP インスペクションの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

始める前に

- ASA クラスタの基本パラメータの設定 （438 ページ） に従って、各クラスタ ユニットをサイト ID に割り当てます。
- LISP のトラフィックはデフォルト インスペクション トラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

手順

ステップ 1 （任意） LISP インスペクション マップを設定して、IP アドレスに基づいて検査済みの EID を制限し、LISP の事前共有キーを設定します。

a) **[構成（Configuration）] > [ファイアウォール（Firewall）] > [オブジェクト（Objects）] > [検査マップ（Inspect Maps）] > [LISP]**を選択します。
b) [Add] をクリックして、新しいマップを追加します。
c) 名前（最大 40 文字）と説明を入力します。
d) **Allowed-EID access-list** については、[Manage] をクリックします。

[ACL Manager] が開きます。

ファースト ホップ ルータまたは ITR/ETR は、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信することがあります。このため、クラスタに関連するサーバーまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

e) ファイアウォールの設定ガイドに従って、少なくとも 1 つの ACE で ACL を追加します。
f) 必要に応じて、**検証キー**を入力します。

暗号化キーをコピーした場合は、[Encrypted]オプション ボタンをクリックします。

g) [OK] をクリックします。

ステップ 2 サービス ポリシー ルールを追加して LISP インスペクションを設定します。

a) **[構成（Configuration）] > [ファイアウォール（Firewall）] > [サービスポリシールール（Service Policy Rules）]**を選択します。
b) [追加（Add）] をクリックします。
c) [Service Policy] ページで、インターフェイスへのルールまたはグローバルなルールを適用します。

既存のサービス ポリシーで使用するものがあれば、そのポリシーにルールを追加します。デフォルトで、ASA には **global_policy** と呼ばれるグローバル ポリシーが含まれま

す。ポリシーをグローバルに適用しない場合は、インターフェイスごとに 1 つのサービス ポリシーを作成することもできます。LISP インスペクションは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービス ポリシーを適用する必要はありません。トラフィックが両方向のクラスに一致する場合、ルールを適用するインターフェイスに出入りするトラフィックのすべてが影響を受けます。

d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)]をオンにします。
e) [Next] をクリックします。
f) インスペクションを行うトラフィックを指定します。ファースト ホップ ルータと UDP ポート 4342 の ITR または ETR の間のトラフィックを指定します。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
g) [Next] をクリックします。
h) [Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。
i) [LISP] チェックボックスをオンにします。
j) （オプション）[Configure] をクリックして、作成したインスペクション マップを選択します。
k) [Finish] をクリックして、サービス ポリシー ルールを保存します。

ステップ 3 サービス ポリシー ルールを追加して、重要なトラフィックのフロー モビリティを有効化します。

a) **[構成（Configuration）] > [ファイアウォール（Firewall）] > [サービスポリシールール（Service Policy Rules）]**を選択します。
b) [追加（Add）] をクリックします。
c) [Service Policy] ページで、LISP インスペクションに使用する同じサービス ポリシーを選択します。
d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)]をオンにします。
e) [Next] をクリックします。
f) サーバーがサイトを変更するときに最適なサイトに再割り当てする、ビジネス クリティカルなトラフィックを指定します。たとえば、フロー モビリティを HTTPS トラフィックおよび/または特定のサーバーへのトラフィックのみに制限できます。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
g) [Next] をクリックします。
h) [Rule Actions] ウィザード ページまたはタブで、[Cluster] タブを選択します。
i) [Enable Cluster flow-mobility triggered by LISP EID messages] チェックボックスをオンにします。
j) [Finish] をクリックして、サービス ポリシー ルールを保存します。

ステップ 4 **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタ設定（Cluster Members）]**の順に選択し、[クラスタリングフローモビリティを有効にする（Enable Clustering flow mobility）] チェックボックスをオンにします。

ステップ 5 [適用（Apply）] をクリックします。

クラスタノードの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタノードを管理できます。

制御ノードからの新しいデータノードの追加

制御ノードからクラスタにデータノードを追加できます。High Availability and Scalability ウィザードを使用してデータノードを追加することもできます。制御ノードからデータノードを追加すると、クラスタ制御リンクを設定でき、追加する各データノードにクラスタインターフェイス モードを設定できるというメリットがあります。

または、データノードにログインし、ノード上で直接クラスタリングを設定することもできます。ただし、クラスタリングをイネーブルにした後は、ASDMセッションが切断されるので、再接続する必要があります。

始める前に

- マルチコンテキストモードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[構成（Configuration）]>[デバイスリスト（Device List）] ペインで、アクティブなデバイスの IP アドレスの下にある [システム（System）] をダブルクリックします。
- 管理ネットワーク上でブートストラップ コンフィギュレーションを送信する場合は、データノードにアクセス可能な IP アドレスがあることを確認してください。

手順

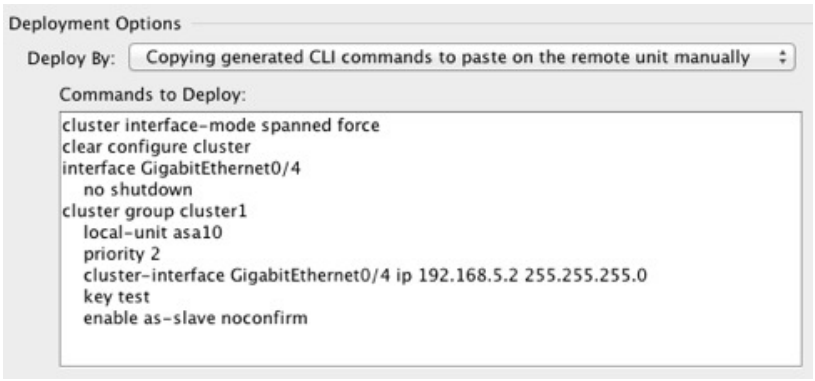
ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタメンバー（Cluster Members）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 次のパラメータを設定します。

- [メンバー名（Member Name）]：このクラスタメンバーの固有の名前を 1 ～ 38 文字の ASCII 文字列で指定します。
- [メンバーの優先順位（Member Priority）]：制御ノード選定用に、このノードの優先順位を 1 ～ 100 の範囲内で設定します。1 が最高の優先順位です。

- [クラスタ制御リンク（Cluster Control Link）] > [IPアドレス（IP Address）]：制御ノードのクラスタ制御リンクと同じネットワーク上で、クラスタ制御リンクのこのメンバーに一意の IP アドレスを指定します。
- [展開オプション（Deployment Options）] 領域で、次の [Deploy By] オプションのいずれかを選択します。
  - [今すぐリモートユニットにCLIコマンドを送信する（Sending CLI commands to the remote unit now）]：ブートストラップ設定をデータノード（一時）管理 IP アドレスに送信します。データノード管理 IP アドレス、ユーザー名、パスワードを入力します。
  - [生成されたCLIコマンドを手動でコピーして、リモートユニットに貼り付ける（Copying generated CLI commands to paste on the remote unit manually）]：データノードの CLI でコマンドをカットアンドペーストできる、または ASDM の CLI ツールを使用できるようにコマンドを生成します。[展開するコマンド（Commands to Deploy）] ボックスで、後で使用するためのコマンドを選択してコピーします。



ステップ 4 [OK] をクリックし、さらに [適用（Apply）] をクリックします。

非アクティブノードになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのノード上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのノードをクラスタから完全に削除します。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタ設定（Cluster Members）]** の順に選択します。

ステップ 2 [Participate in ASA cluster] チェックボックスをオフにします。

（注） [Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3 [Apply] をクリックします。

制御ノードからのデータノードの非アクティブ化

データノードを非アクティブにするには、次の手順を実行します。

（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスのIPアドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）]** の順に選択します。

ステップ 2 削除するデータノードを選択して [削除（Delete）] をクリックします。

データノードのブートストラップ コンフィギュレーションは同じであり、その設定を失うことなく以後データノードを再追加できます。

ステップ 3 [適用（Apply）] をクリックします。

クラスタへの再参加

ノードがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。ただし、ASDMでクラスタリングを手動で無効にした場合、設定を保存してリロードしなかった場合は、ASDMでクラスタリングを再び有効にできます。リロード後、管理インターフェイスは無効になるため、コンソール アクセスがクラスタリングを再び有効にする唯一の方法です。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] >

[Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 ASDM にまだアクセスしている場合は、再イネーブル化するノードに ASDM を接続して、ASDM でクラスタリングを再び有効にすることができます。

新しいメンバーとして追加していない限り、データノードのクラスタリングを制御ノードから再び有効にすることはできません。

a) **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）]** の順に選択します。
b) [Participate in ASA cluster] チェックボックスをオンにします。
c) [Apply] をクリックします。

ステップ 2 ASDM を使用できない場合：コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 3 クラスタリングをイネーブルにします。

enable

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各ノードの現在のコンフィギュレーションは（アクティブユニットから同期されて）同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IPアドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

始める前に

コンソールポートを使用する必要があります。クラスタのコンフィギュレーションを削除すると、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスがシャットダウンされます。

手順

ステップ 1 セカンダリノードの場合、クラスタリングを次のようにディセーブルにします。

cluster group *cluster_name* **no enable**

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがデータノード上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ 2 クラスタ コンフィギュレーションをクリアします。

clear configure cluster

ASAは、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ 3 クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ 4 バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy *backup_cfg* **running-config**

例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

ステップ 5 コンフィギュレーションをスタートアップに保存します。

write memory

ステップ 6 バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

制御ノードの変更

⚠

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 [Monitoring] > [ASA Cluster] > [Cluster Summary] を選択します。

ステップ 2 ドロップダウンリストから制御ノードにするデータノードを選択し、制御ノードにするボタンをクリックします。

ステップ 3 制御ノードの変更を確認するように求められます。[Yes] をクリックします。

ステップ 4 ASDM を終了し、メイン クラスタ IP アドレスを使用して再接続します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのノードに、または特定のノードに送信するには、次の手順を実行します。**show** コマンドをすべてのノードに送信すると、すべての出力が収集されて現在のノードのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

始める前に

コマンドライン インターフェイス ツールでこの手順を実行します。[Tools] > [Command Line Interface] を選択します。

手順

すべてのノードにコマンドを送信します。ノード名を指定した場合は、特定のノードに送信します。

cluster exec [**unit** *node_name*] コマンド

例：

```
ciscoasa# cluster exec show xlate
```

ノード名を表示するには、**cluster exec unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャファイルをクラスタ内のすべてのノードから同時に TFTP サーバにコピーするには、制御ノードで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ノードから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にノード名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 と asa2 はクラスタノード名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各ノードの EtherChannel 情報が表示されています。

```
ciscoasa# cluster exec show port-channel summary
master(LOCAL):**************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

ASA クラスタのモニターリング

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニターリング

クラスタの状態のモニターリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [Cluster Summary]**

  このペインには、接続相手のノードとクラスタのその他のノードの情報が表示されます。また、このペインでプライマリノードを変更することができます。

- **[Cluster Dashboard]**

  プライマリノードのホームページの [クラスタダッシュボード（Cluster Dashboard）] と [クラスタファイアウォールダッシュボード（Cluster Firewall Dashboard）] を使用してクラスタをモニタできます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

[Wizards] > [Packet Capture Wizard]

クラスタ全体のトラブルシューティングをサポートするには、制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

クラスタリソースのモニタリング

クラスタリソースのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [CPU]**

  このペインでは、クラスタノード全体の CPU 使用率を示すグラフまたはテーブルを作成することができます。

- [Monitoring] > [ASA Cluster] > [System Resources Graphs] > [Memory]。このペインでは、クラスタノード全体の [空きメモリ（Free Memory）] と [使用済みメモリ（Used Memory）] を表示するグラフまたはテーブルを作成することができます。

クラスタトラフィックのモニタリング

クラスタトラフィックのモニタリングについては、次の画面を参照してください。

- [モニタリング（Monitoring）] > [ASAクラスタ（ASA Cluster）] > [トラフィックグラフ（Traffic Graphs）] > [接続（Connections）]。

  このペインでは、クラスタメンバー全体の接続を示すグラフまたはテーブルを作成することができます。

- [モニタリング（Monitoring）] > [ASAクラスタ（ASA Cluster）] > [トラフィックグラフ（Traffic Graphs）] > [スループット（Throughput）]。

  このペインでは、クラスタメンバー全体のトラフィックのスループットを示すグラフまたはテーブルを作成することができます。

- **[モニタリング（Monitoring）] > [ASAクラスタ（ASA Cluster）] > [クラスタ負荷のモニタリング（Cluster Load-Monitoring）]**

  ここでは、[ロードモニタの情報（Load Monitor-Information）] ペインと [ロードモニタの詳細（Load-Monitor Details）] ペインについて説明します。**ロードモニタの情報**には、最後のインターバルのクラスタメンバーのトラフィック負荷、および設定された間隔の合計数の平均（デフォルトでは 30）が表示されます。各間隔の各測定値を表示するには、[ロードモニタの詳細（Load-Monitor Details）] ペインを使用します。

クラスタ制御リンクのモニターリング

クラスタの状態のモニターリングについては、次の画面を参照してください。

[Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link]。

このペインでは、クラスタ制御リンクの [Receival] および [Transmittal] 容量使用率を表示するグラフまたはテーブルを作成することができます。

クラスタのルーティングのモニターリング

クラスタのルーティングについては、次の画面を参照してください。

- **[Monitoring] > [Routing] > [LISP-EID Table]**

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

[Configuration] > [Device Management] > [Logging] > [Syslog Setup]

クラスタ内の各ノードは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

ASA クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

ASA およびスイッチのコンフィギュレーションの例

次のコンフィギュレーション例は、ASA とスイッチ間の次のインターフェイスを接続します。

ASA インターフェイス	スイッチ インターフェイス
イーサネット1/2	GigabitEthernet 1/0/15
イーサネット 1/3	GigabitEthernet 1/0/16
イーサネット 1/4	GigabitEthernet 1/0/17
イーサネット 1/5	GigabitEthernet 1/0/18

ASA の設定

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 制御ユニットのブートストラップ設定

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 データユニットのブートストラップ設定

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
```

```
 key emphyri0
 enable as-slave
```

制御ユニットのインターフェイス設定

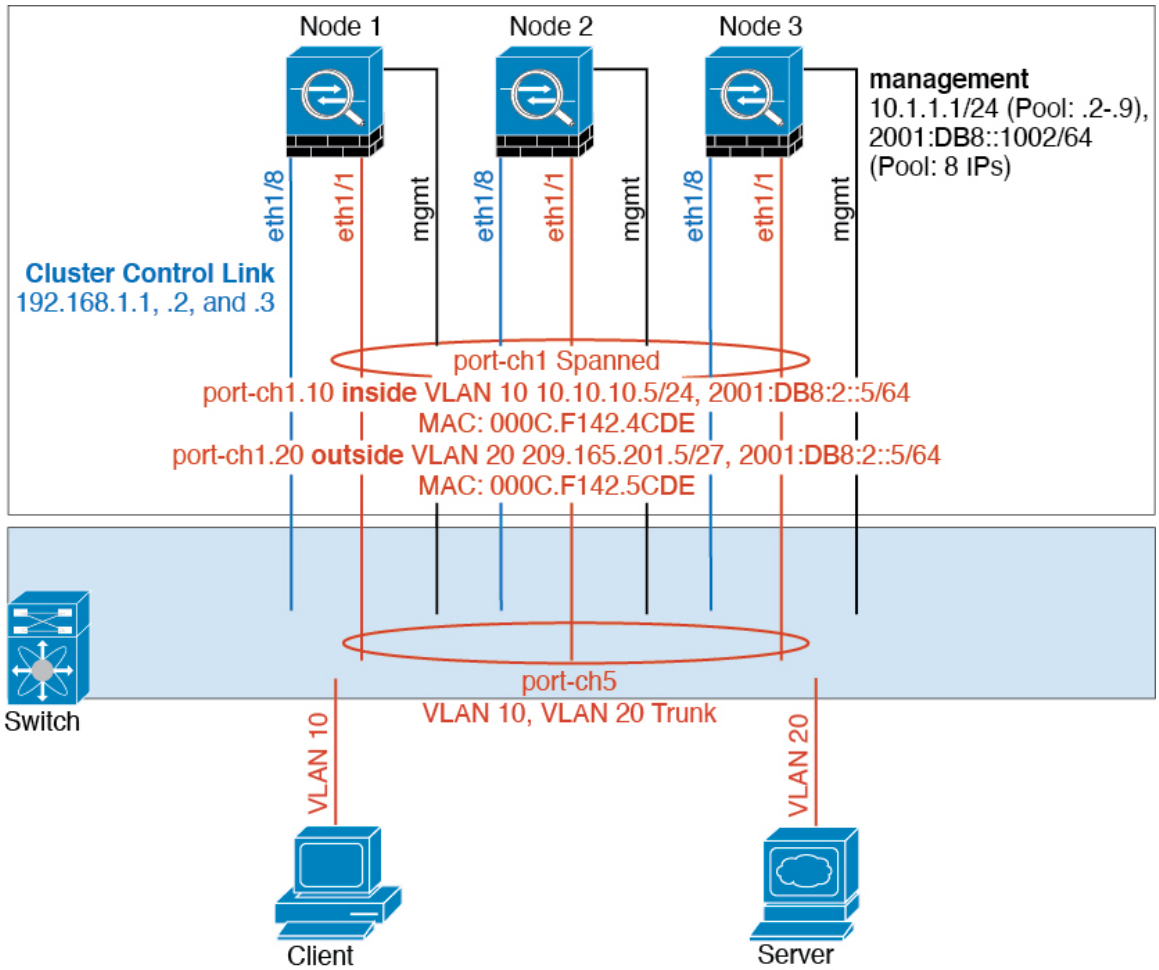
```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface Ethernet1/2
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/3
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/4
 channel-group 11 mode active
 no shutdown
!
interface Ethernet1/5
 channel-group 11 mode active
 no shutdown
!
interface Management1/1
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Cisco IOS スイッチのコンフィギュレーション

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
```

```
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。ASA が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ユニット 1 制御ユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa1
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ユニット 2 データユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ユニット 3 データユニットのブートストラップ設定

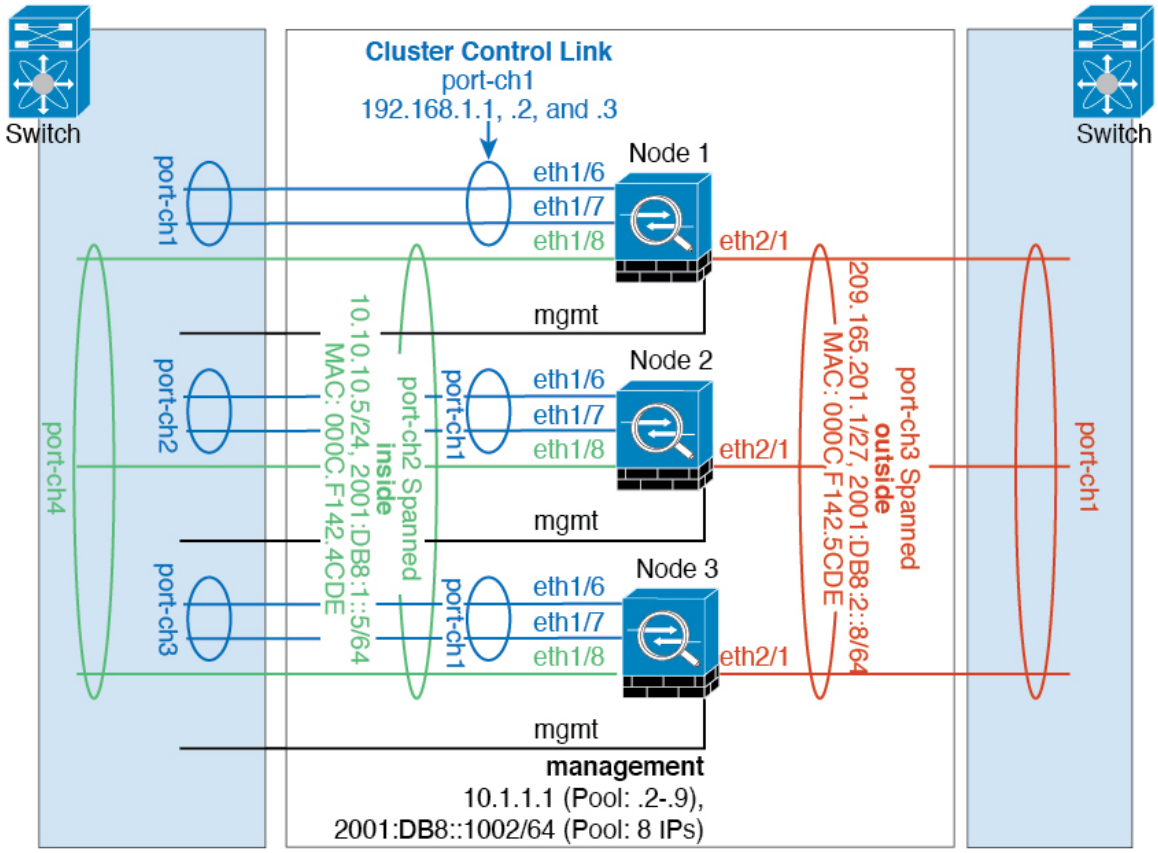
```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
```

```
enable as-slave
```

制御ユニットのインターフェイス設定

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface ethernet1/1
channel-group 1 mode active
no shutdown

interface port-channel 1
port-channel span-cluster

interface port-channel 1.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ユニット 1 制御ユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL
```

```
cluster group cluster1
local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ユニット 2 データユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL

cluster group cluster1
local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ユニット 3 データユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL

cluster group cluster1
local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

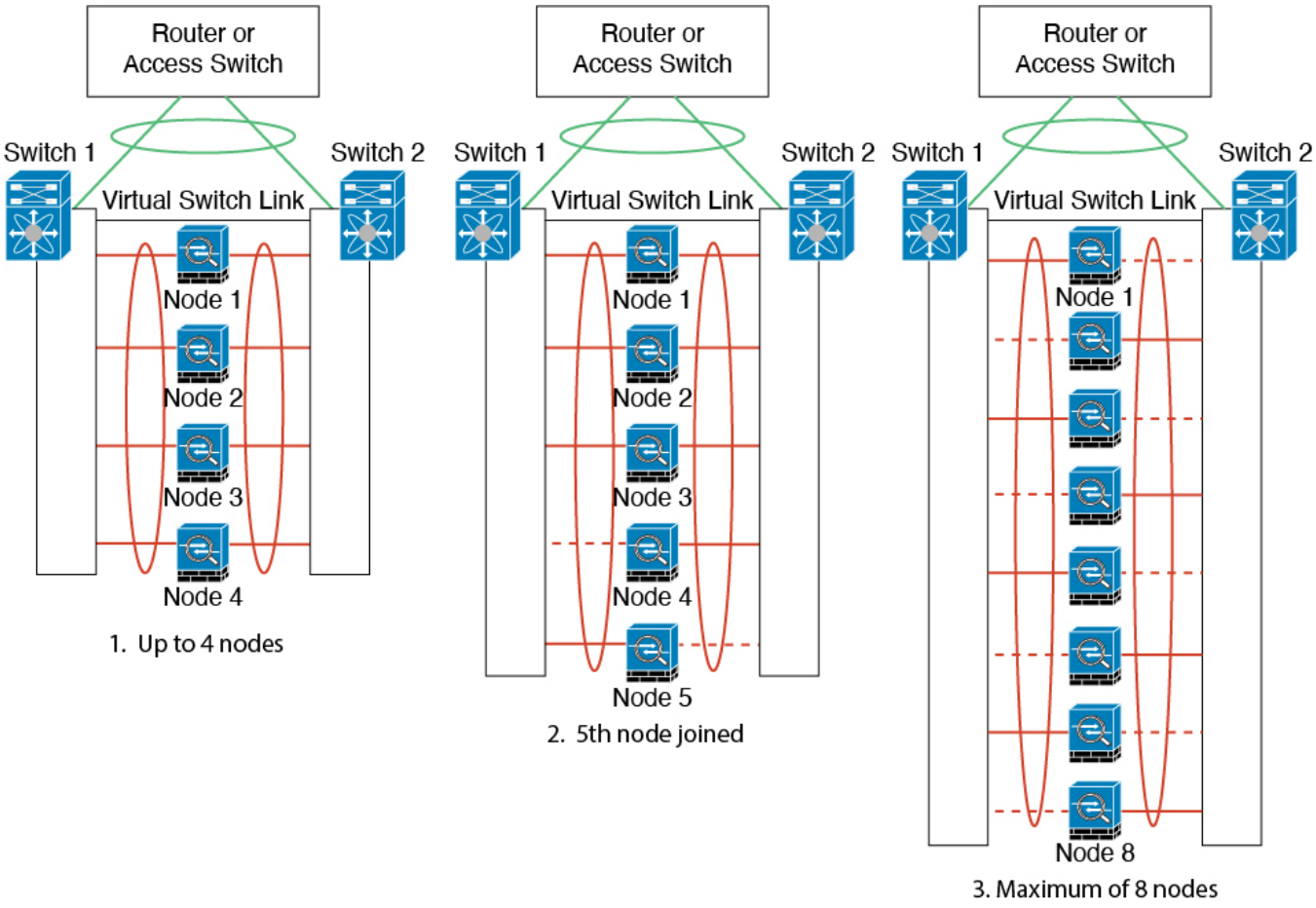
制御ユニットのインターフェイス設定

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
```

```
security-level 100
management-only
no shutdown

interface ethernet 1/8
channel-group 2 mode active
no shutdown

interface port-channel 2
port-channel span-cluster
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface ethernet 2/1
channel-group 3 mode active
no shutdown

interface port-channel 3
port-channel span-cluster
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

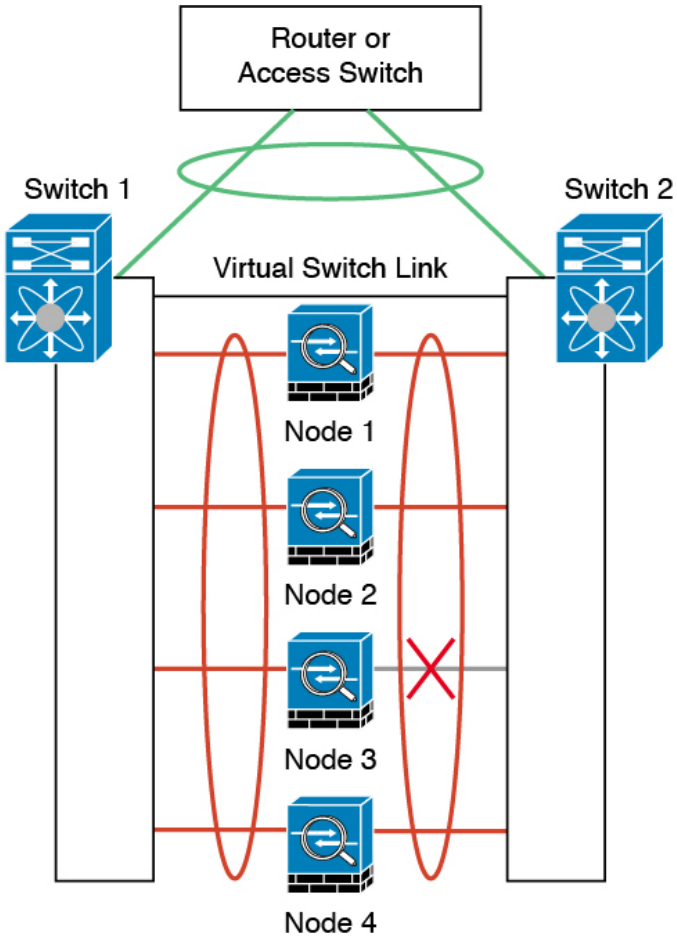
スパンド EtherChannel とバックアップ リンク（従来の 8 アクティブ/8 スタンバイ）

従来の EtherChannel のアクティブ ポートの最大数は、スイッチ側からの 8 に制限されます。8 ユニットから成るクラスタがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイ モードにする必要があります。ASA は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。VSS または vPC を使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASA では、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「制御」ポートとなり（たとえば Ethernet 1/1）、他方が「データ」ポートとなります（たとえば Ethernet 1/2）。ハードウェア接続の対称性を保証する必要があります。つまり、すべての制御リンクは 1 台のスイッチが終端となり、すべてのデータリンクは別のスイッチが終端となっている必要があります（VSS/vPC が使用されている場合）。次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。

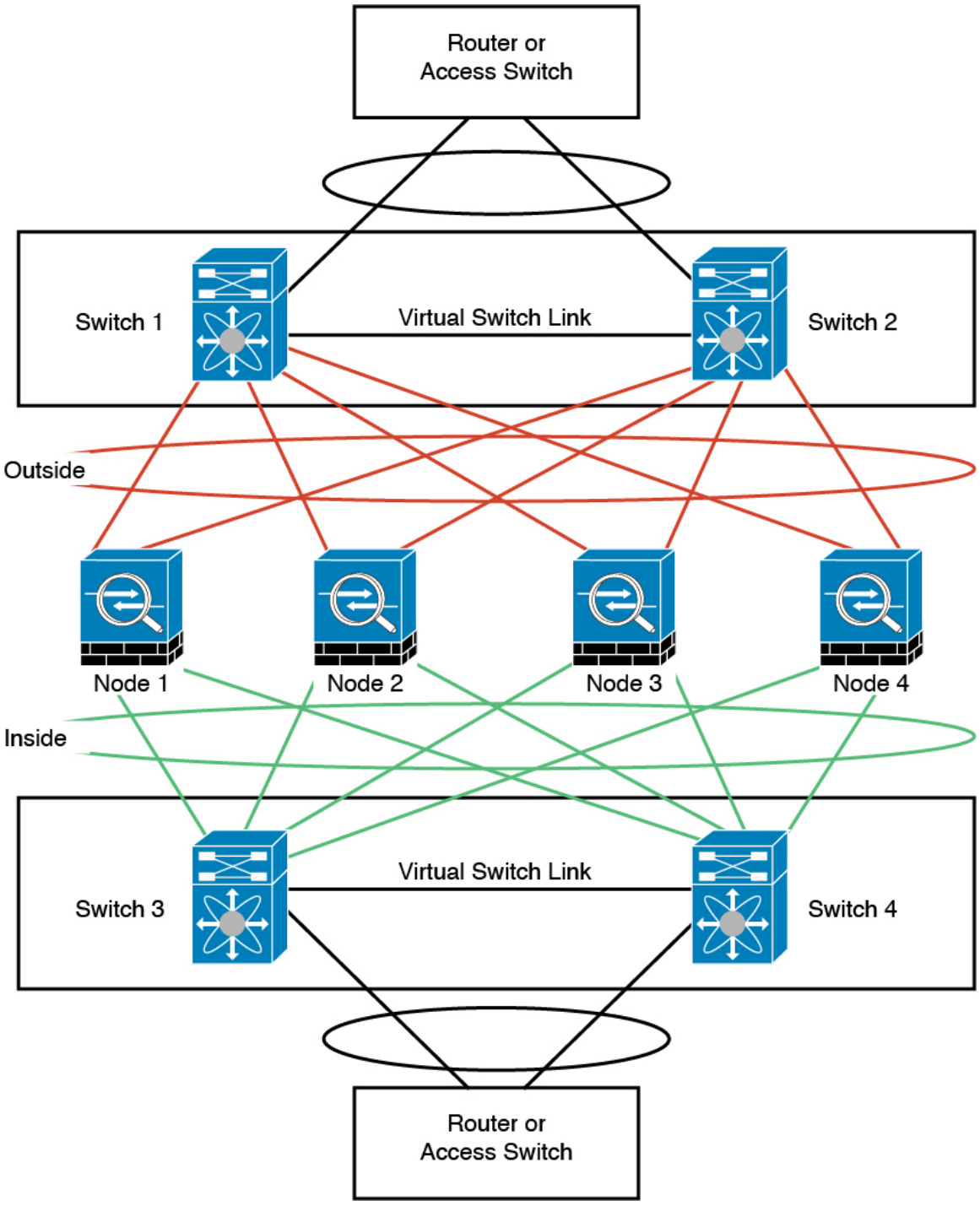


原則として、初めにチャネル内のアクティブポート数を最大化し、そのうえで、アクティブな制御ポートとアクティブなデータポートの数のバランスを保ちます。5 番目のユニットがクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

リンクまたはデバイスの障害が発生したときも、同じ原則で処理されます。その結果、ロードバランシングが理想的な状態にはならないこともあります。次の図は、4 ユニットのクラスタを示しています。このユニットの 1 つで、単一リンク障害が発生しています。



ネットワーク内に複数の EtherChannel を設定することも考えられます。次の図では、EtherChannel が内部に 1 つ、外部に 1 つあります。ASA は、一方の EtherChannel で制御とデータの両方のリンクが障害状態になった場合にクラスタから削除されます。これは、その ASA がすでに内部ネットワークへの接続を失っているにもかかわらず、外部ネットワークからトラフィックを受信するのを防ぐためです。



各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ユニット 1 制御ユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface ethernet 1/8
channel-group 1 mode on
no shutdown

interface ethernet 2/1
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL

cluster group cluster1
local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ユニット 2 データユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface ethernet 1/8
channel-group 1 mode on
no shutdown

interface ethernet 2/1
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL

cluster group cluster1
local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ユニット 3 データユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface ethernet 1/8
channel-group 1 mode on
no shutdown

interface ethernet 2/1
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL

cluster group cluster1
local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

ユニット 4 データユニットのブートストラップ設定

```
interface ethernet 1/6
channel-group 1 mode on
no shutdown

interface ethernet 1/7
channel-group 1 mode on
no shutdown

interface ethernet 1/8
channel-group 1 mode on
no shutdown

interface ethernet 2/1
channel-group 1 mode on
no shutdown

interface port-channel 1
description CCL

cluster group cluster1
local-unit asa4
cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
priority 4
key chuntheunavoidable
enable as-slave
```

制御ユニットのインターフェイス設定

```
ip local pool mgmt 10.1.1.2-10.1.1.9

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
security-level 100
management-only

interface ethernet 2/6
channel-group 3 mode active vss-id 1
no shutdown

interface ethernet 2/7
channel-group 3 mode active vss-id 2
no shutdown

interface port-channel 3
port-channel span-cluster vss-load-balance
nameif inside
ip address 10.10.10.5 255.255.255.0
mac-address 000C.F142.4CDE

interface ethernet 2/8
channel-group 4 mode active vss-id 1
no shutdown

interface ethernet 2/9
channel-group 4 mode active vss-id 2
no shutdown

interface port-channel 4
port-channel span-cluster vss-load-balance
nameif outside
ip address 209.165.201.1 255.255.255.224
mac-address 000C.F142.5CDE
```

ルーテッド モード サイト間クラスタリングの OTV 設定

スパンド EtherChannel を使用したルーテッド モードに対するサイト間クラスタリングの成功は、OTV の適切な設定とモニタリングによって異なります。OTV は、DCI 全体にパケットを転送することで、重要な役割を果たします。OTV は、転送テーブルに MAC アドレスを学習するときにのみ、DCI 全体にユニキャスト パケットを転送します。MAC アドレスが OTV 転送テーブルに学習されていない場合、ユニキャスト パケットはドロップされます。

OTV 設定の例

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
```

```
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
```

```
otv flood mac 0050.56A8.3D22 vlan 3151
```

サイト障害のために必要な OTV フィルタの変更

サイトがダウンした場合は、グローバル MAC アドレスをそれ以上ブロックしなくて済むように、フィルタを OTV から削除する必要があります。必要ないくつかの追加設定があります。

機能しているサイトで OTV スイッチ上の ASA グローバル MAC アドレスに対するスタティック エントリを追加する必要があります。このエントリによって、反対側の OTV はオーバーレイ インターフェイスにこれらのエントリを追加できます。サーバとクライアントに ASA 用の ARP エントリがすでにある場合（これは既存の接続の場合です）、ARP は再送信されないので、この手順が必要になります。したがって、OTV は転送テーブルに ASA グローバル MAC アドレスを学習する機会はありません。OTV には転送テーブル内にグローバル MAC アドレスがなく、OTV の設計ごとに OTV はオーバーレイ インターフェイスを介してユニキャスト パケットをフラッディングしないので、ユニキャスト パケットはサーバからのグローバル MAC アドレスにドロップされ、既存の接続は切断されます。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

他のサイトが復元した場合は、フィルタを再度追加して、OTV でこのスタティック エントリを削除する必要があります。グローバル MAC アドレスのオーバーレイ エントリをクリアするには、両方の OTV でダイナミック MAC アドレス テーブルをクリアすることが非常に重要です。

MAC アドレス テーブルのクリア

サイトがダウンし、グローバル MAC アドレスへのスタティック エントリが OTV に追加される場合は、他の OTV がオーバーレイ インターフェイスのグローバル MAC アドレスを学習できるようにする必要があります。他のサイトが起動したら、これらのエントリをクリアする必要があります。OTV の転送テーブルにこれらのエントリがないことを確認するために、MAC アドレス テーブルを必ず消去してください。

```
cluster-N7k6-OTV# show mac address-table
```

```
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP キャッシュのモニタリング

OTV は、OTV インターフェイス全体で学習した IP アドレスに対するプロキシ ARP への ARP キャッシュを維持します。

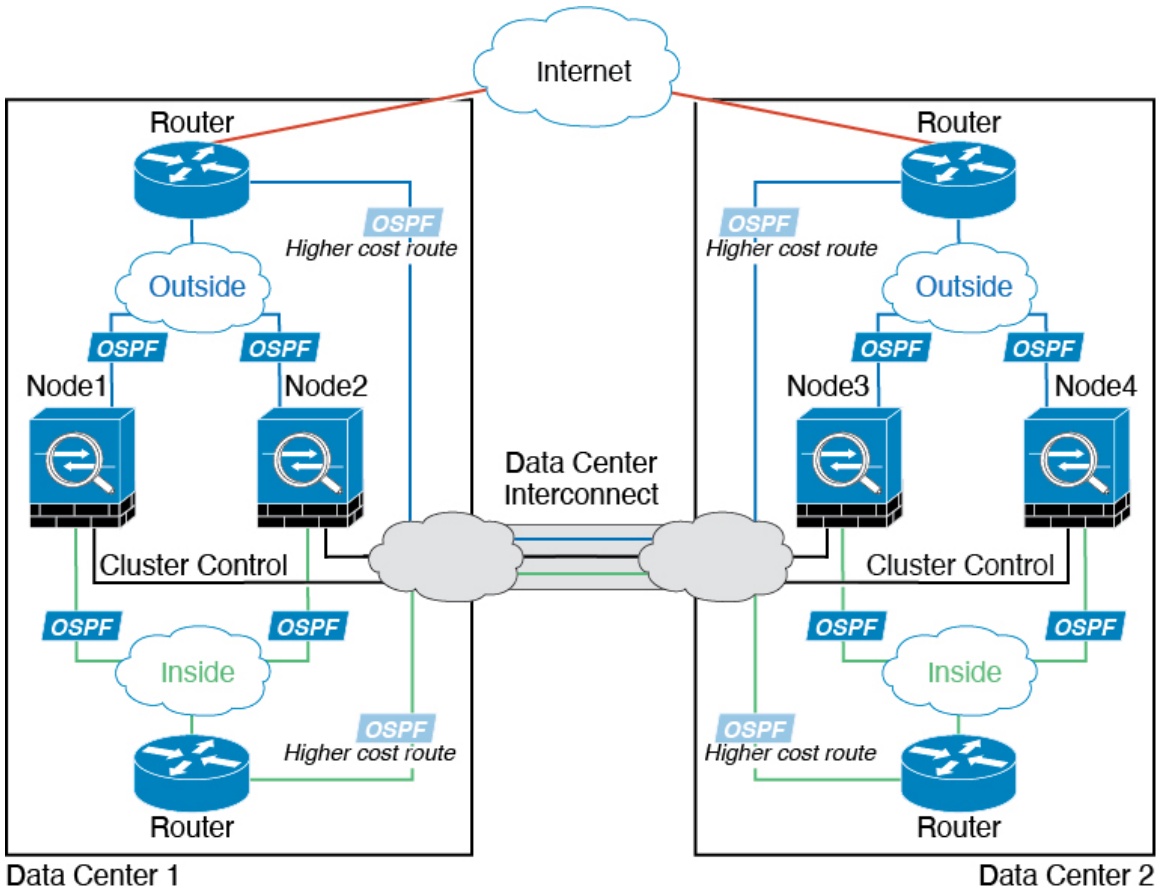
```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

個別インターフェイス ルーテッド モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つの ASA クラスタノードがある場合を示します。クラスタノードは、DCI 経由のクラスタ制御リンクによって接続されています。各データセンターの内部ルータと外部ルータは、OSPF と PBR または ECMP を使用してクラスタ メンバ間でトラフィックをロードバランスします。DCI に高コストルートを割り当てることにより、特定のサイトのすべての ASA クラスタノードがダウンしない限り、トラフィックは各データセンター内に維持されます。1 つのサイトのすべてのクラスタノードに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトの ASA クラスタノードに送られます。



サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド EtherChannel ルーテッド モードの例

次の例では、各サイトのゲートウェイ ルータと内部ネットワーク間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部両方のネットワークに対しスパンド EtherChannel を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

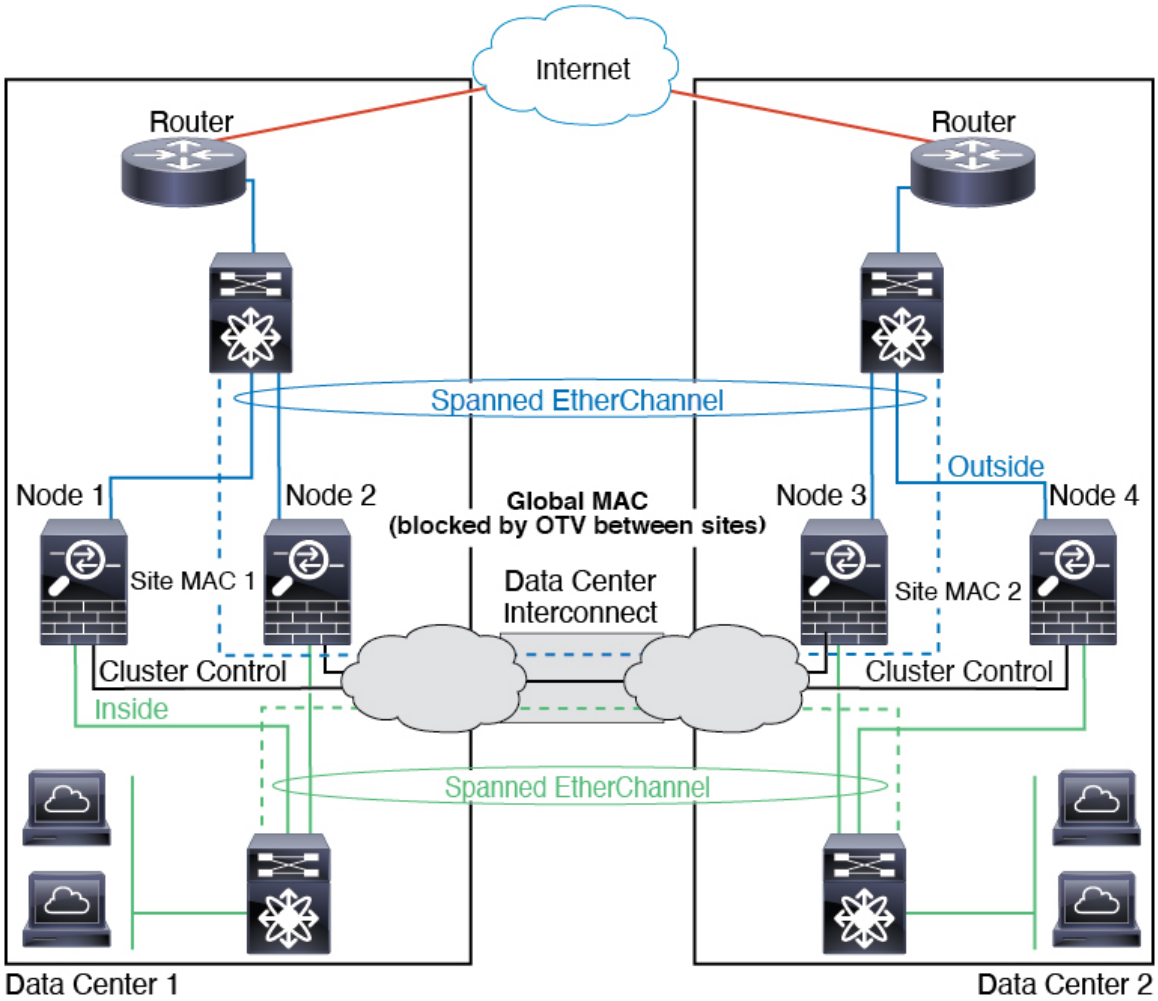
データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロックするフィルタを追加する必要があります。1 つのサイトのクラスタ ノードが到達不能になった場合、トラフィックが他のサイトのクラスタ ノードに送信されるようにフィルタを削除する必要があります。Vacl を使用して、グローバルの MAC アドレスのフィルタ リングする必要があります。F3 シリーズライン カードが搭載された Nexus などの一部のスイッチでは、グローバル MAC アドレスからの ARP パケットをブロックするために ARP インスペクションも使用する必要があります。ARP インスペクションでは、ASA でサイトの MAC アドレスとサイトの

IP アドレスの両方を設定する必要があります。サイトの MAC アドレスのみを設定する場合は必ず ARP インスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタノード間で共有されるグローバルな仮想 MAC は、パケットを受信するためだけに使用されます。発信パケットは、各 DC クラスタからのサイト固有の MAC アドレスを使用します。この機能により、スイッチが 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。

この場合のシナリオは次のとおりです。

- クラスタから送信されるすべての出力パケットは、サイトの MAC アドレスを使用し、データセンターでローカライズされます。
- クラスタへのすべての入力パケットは、グローバル MAC アドレスを使用して送信されるため、両方のサイトにある任意のノードで受信できます。OTV のフィルタによって、データセンター内のトラフィックがローカライズされます。



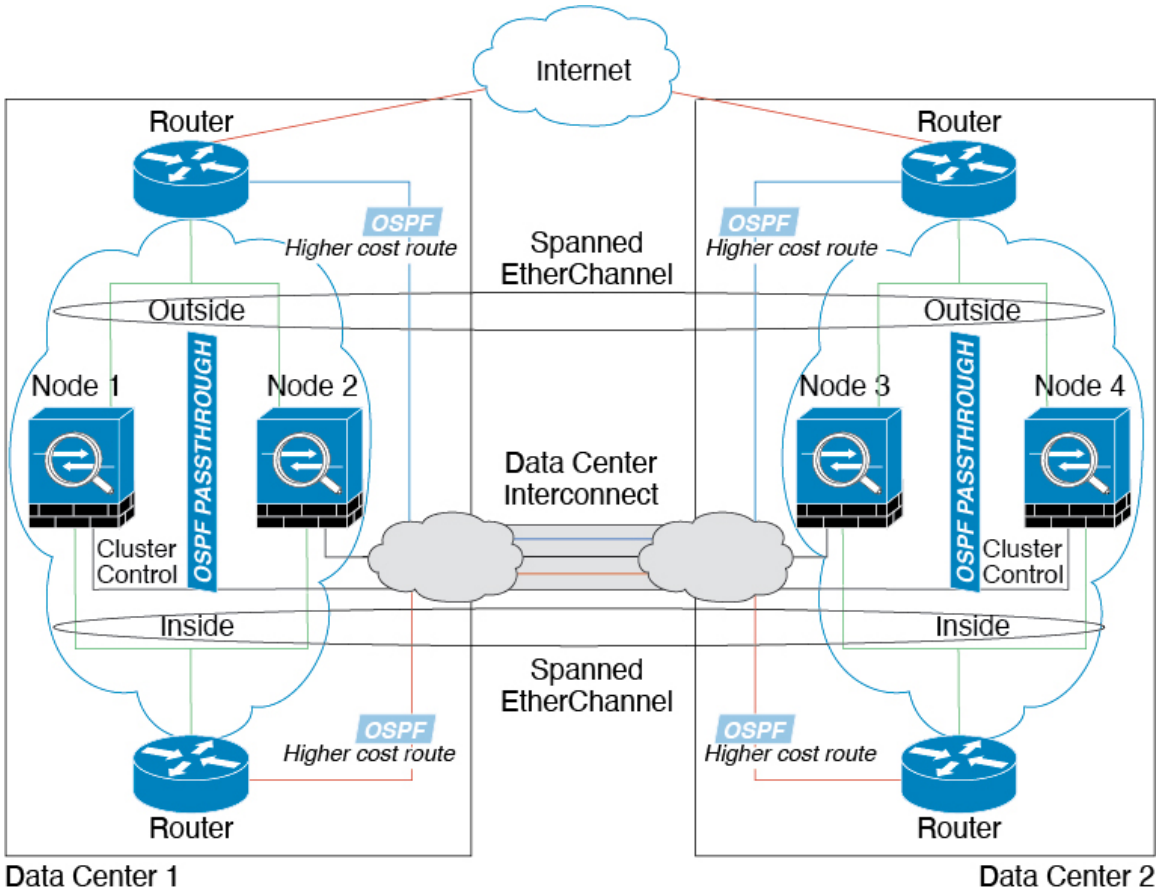
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コストルートを割り当てることにより、特定のサイトですべてのクラスタ メンバーがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1 つのサイトのすべてのクラスタ メンバーに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタ メンバーに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS/vPC：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、VSS/vPC トラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCI が余分なトラフィックを処理できる場合、必要に応じて、各ノードを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS/vPC：スイッチの冗長性を高めるには、各サイトに 2 つの異なる VSS/vPC ペアをインストールできます。この場合、クラスタノードは、両方のローカルスイッチだけに接続されたデータセンター 1 のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター 2 のシャーシではスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。

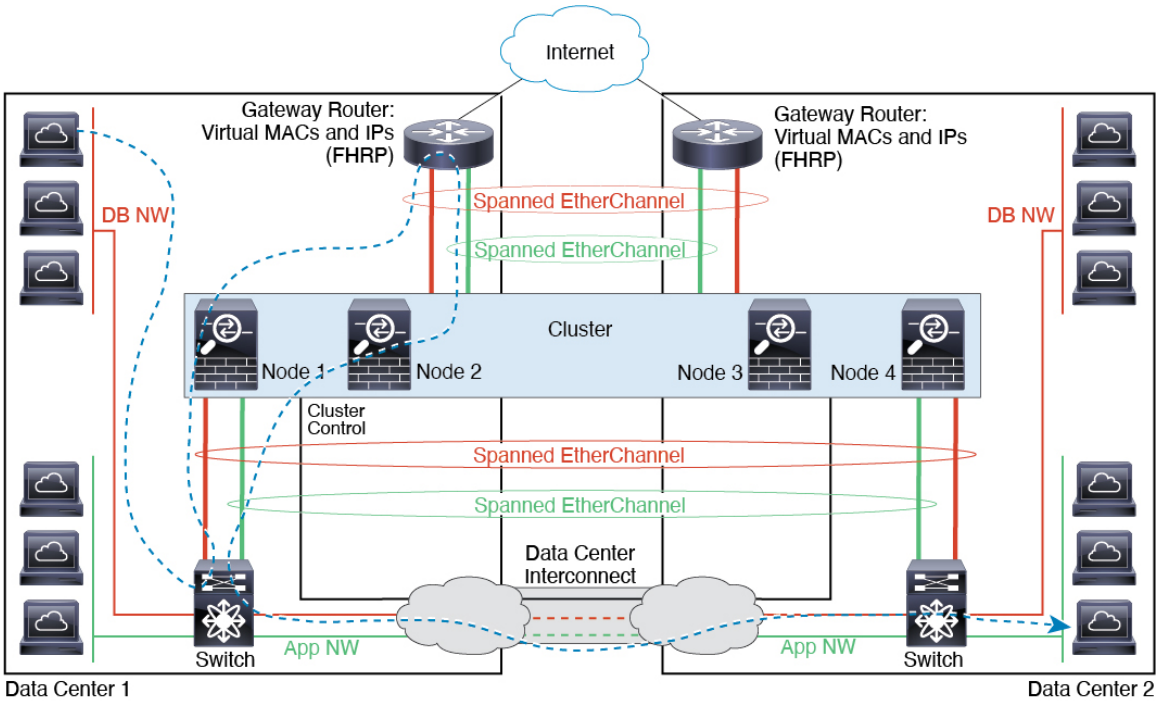


スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイ ルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレス と IP アドレスを提供します。MAC アドレスの予期せぬフラッピングを避けるため、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト 1 のゲートウェイがサイト 2 のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト 2 に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイ ルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1 つ

のサイトのゲートウェイ ルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- 次のアプリケーション インスペクション：
  - CTIQBE

- H323、H225、および RAS
- IPsec パススルー
- MGCP
- MMP
- RTSP
- SCCP（Skinny）
- WAAS
- WCCP

- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- VPN ロード バランシング
- フェールオーバー
- 統合ルーティングおよびブリッジング
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。たとえば、8 つのノードのクラスタがあるとします。Other VPN ライセンスでは、1 台の ASA に対して許可されるサイト間 IPsec トンネルの最大数は 10,000 です。8 ノードクラスタ全体で使用できるトンネル数は 10,000 までです。この機能はスケーリングしません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

- サイト間 VPN
- 次のアプリケーション インスペクション：

- DCERPC
- ESMTP
- IM
- NetBIOS
- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- スタティック ルート トラッキング
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス
- ダイナミックルーティング（スパンド EtherChannel モードのみ）

個々のノードに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。

- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

- ASA FirePOWER モジュール：ASA Firepower モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。Firepower Management Center を使用して、クラスタ内の ASA Firepower モジュールで一貫したポリシーを保持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイスベースのゾーン定義を使用しないでください。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証と許可は、クラスタリング制御ノード上で中央集中型機能として実装されており、データ構造がクラスタデータノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザーおよびユーザーに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザー認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるため、フローに対するアカウンティングが設定されている場合、そのフローを所有するクラスタノードがアカウンティング開始と停止のメッセージを AAA サーバーに送信します。

接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます（**[構成（Configuration）] > [ファイアウォール（Firewall）] > [サービスポリシー（Service Policy）]** ページを参照）。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

FTP とクラスタリング

- FTP D チャネルとコントロールチャネルのフローがそれぞれ別のクラスタ メンバーによって所有されている場合は、D チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。

- FTP アクセスに AAA を使用する場合、制御チャネルのフローは制御ノードに集中されます。

ICMP インスペクションとクラスタリング

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインスペクションが有効かどうかによって異なります。ICMPインスペクションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インスペクションを使用する場合、ICMP フローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットのディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

マルチキャスト ルーティングとクラスタリング

マルチキャスト ルーティングは、インターフェイス モードによって動作が異なります。

スパンド EtherChannel モードでのマルチキャスト ルーティング

スパンドEtherChannelモードでは、ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを処理します。接続が確立された後は、各データユニットがマルチキャスト データ パケットを転送できます。

個別インターフェイス モードでのマルチキャスト ルーティング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべて制御ユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NATが使用されるときは、インバウンドとアウトバウンドとで、パケットのIPアドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。これは、スパンドEtherChannelの問題ではありません。クラスタ インターフェイスには関連付けられた IP アドレスが 1 つしかないためです。

- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。

- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT IP アドレスのオーナーがダウンすると、バックアップノードは PAT の IP アドレス、対応するポートブロック、および xlate を所有します。通常の PAT アドレスでポートが不足している場合、新しい要求を処理するために引き継いだアドレスを使用できます。接続が最終的にタイムアウトすると、ブロックは解放されます。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。

- ダイナミック PAT 用 NAT プールアドレス分散：制御ノードは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信し、アドレスが割り当てられていない場合、その接続は PAT の制御ノードに転送されます。クラスタメンバが（障害により）クラスタから離脱した場合、バックアップメンバは PAT IP アドレスを取得し、バックアップで通常の PAT IP アドレスが使い果たされると、新しいアドレスを使用できるようになります。各ノードがアドレスを受信し、アドレスを引き継いだメンバーが古いアドレスを使用している場合に障害が発生したノードが新しいアドレスを取得できるようにするには、少なくともクラスタ内のノードと同じ数の NAT アドレスに加えて、少なくとも 1 つの追加アドレスが含まれていることを確認してください。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。

- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。

- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。

- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlates：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、ファイアウォールの設定ガイドを参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

ダイナミック ルーティングおよびクラスタリング

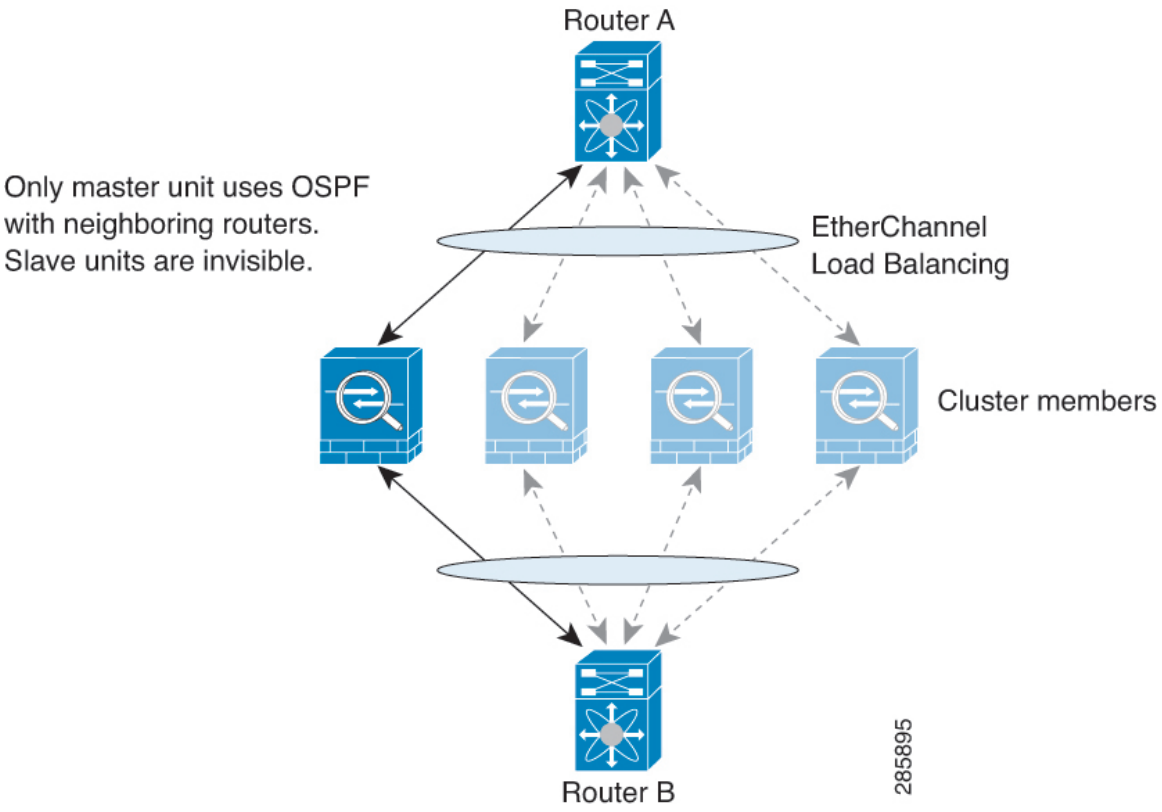
ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

（注） IS-IS は、スパンド EtherChannel モードではサポートされていません。

スパンドEtherChannelモード：ルーティングプロセスは制御ノードでのみ実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *55 :* スパンド *EtherChannel* モードでのダイナミック ルーティング



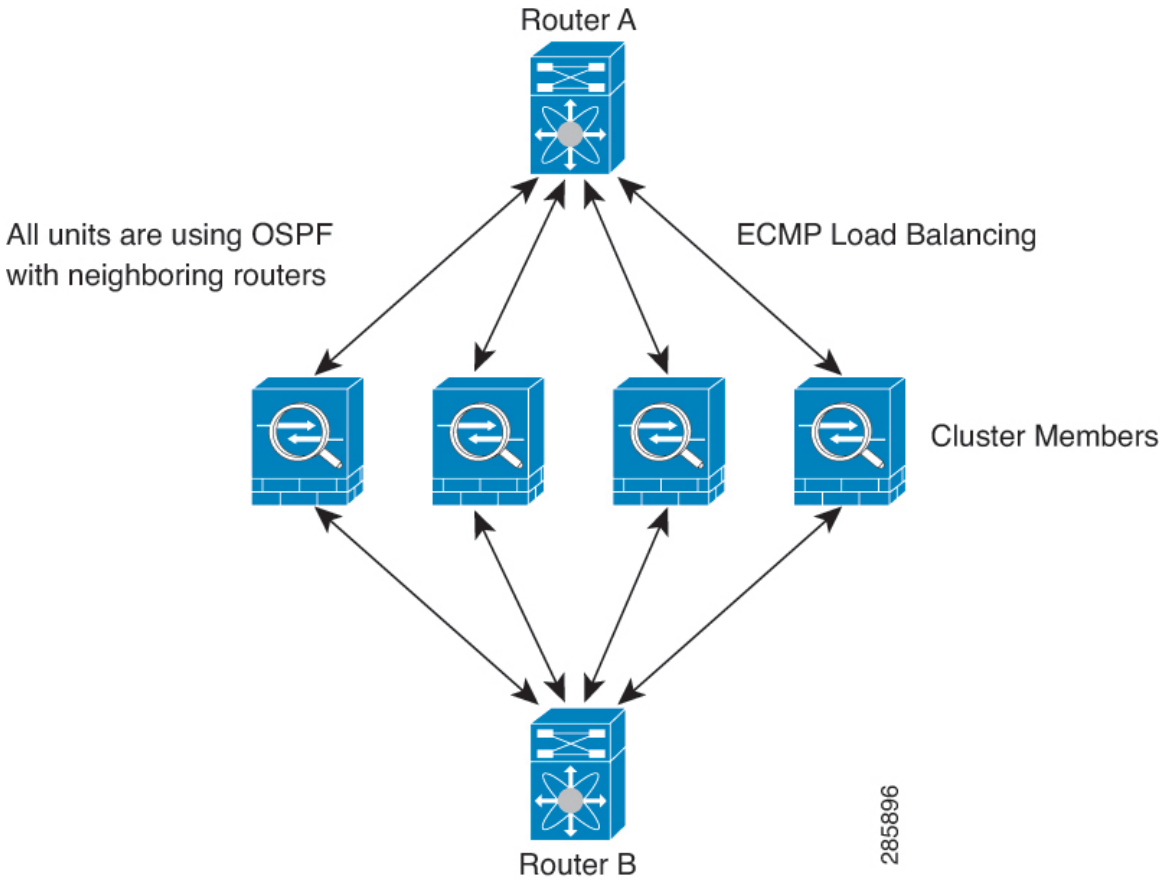
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータIDがクラスタ全体で使用されるようになります。割り込みを解決するには、OSPFノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *56*：個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コスト パスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタプールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性確保のためにクラスタが同一ルータに対して複数の隣接関係を持つ場合、非対称ルーティングが原因で許容できないトラフィック損失が発生する場合があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべての ASA インターフェイスをまとめます。トラフィック ゾーンの設定 （739 ページ）を参照してください。

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、その 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザーは新しいノードに複製されません。SNMPv3ユーザーは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、STUNインスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN要求の受信後にノードに障害が発生し、別のノードがSTUN応答を受信した場合、STUN応答はドロップされます。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。
- NetFlow：クラスタの各ノードは自身のNetFlowストリームを生成します。NetFlowコレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。分散型サイト間 VPN クラスタリングがサポートされています。詳細については、この pdf のハイアベイラビリティ オプションを検索してください。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンド EtherChannel アドレスに接続すると、接続が自動的に制御ノードに転送されます。 PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットを結合して 1 つのクラスタとしたときに、期待できるパフォーマンスの概算値は次のようになります。

- 合計スループットの 70 %
- 最大接続数の 60 %
- 接続数/秒の 50 %

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。

3. 45秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

注　最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。

5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注）　ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

ASA クラスタ内のハイアベイラビリティ

ASA クラスタリングは、ノードとインターフェイスの正常性を監視し、ノード間で接続状態を複製することにより、ハイアベイラビリティを提供します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション 2 のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

詳細については、制御ノードの選定 （491 ページ）を参照してください。

インターフェイス モニターリング

各ノードは、使用中のすべての指名されたハードウェアインターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

- スパンド EtherChannel：クラスタ Link Aggregation Control Protocol（cLACP）を使用します。各ノードは、リンクステータスおよび cLACP プロトコルメッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスが制御ノードに報告されます。
- 個別インターフェイス（ルーテッドモードのみ）：各ノードが自身のインターフェイスを自己モニタし、インターフェイスのステータスを制御ノードに報告します。

ヘルスモニタリングをイネーブルにすると、すべての物理インターフェイス（主要な EtherChannel インターフェイスおよび冗長インターフェイスのタイプを含む）がデフォルトでモニタされるため、オプションでインターフェイスごとのモニタリングをディセーブルにすることができます。指名されたインターフェイスのみモニターできます。たとえば、指名された EtherChannel に障害が発生したと判断される必要がある場合、つまり、EtherChannel のすべてのメンバーポートはクラスタ削除をトリガーすることに失敗する必要があります（最小ポートバンドリング設定に応じて）。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパニングかどうかを問わない）は、確立済みメンバーのインターフェイスがダウン状態のときに、ASA はそのメンバーを 9 秒後に削除します。ASA は、ノードがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。非 EtherChannel の場合は、メンバー状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASA が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでノードがまだ非アクティブになっていると、管理インターフェイスは無効になります。さらに設定を行う場合は、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタノードがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：（最初の参加時）クラスタ制御リンクの問題を解決した後、。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASAは、無限に5分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASAは自動的に最初は5分後、次に10分後、最終的に20分後に再参加を試みます。20分後に参加できない場合、ASAはクラスタリングをディセーブルにします。データインターフェイスの問題を解決した後、。この動作は設定可能です。
- ASA FirePOWEソフトウェアモジュールの障害：モジュールの問題を解決した後、手動でクラスタリングをイネーブルにする必要があります。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングがまだイネーブルになっているなら、ノードは再起動するとクラスタに再参加することを意味します。ASAは5秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。ノードは、5分、10分、20分の間隔で自動的にクラスタに再参加しようとします。この動作は設定可能です。

ASA クラスタの基本パラメータの設定 （438 ページ） を参照してください。

データ パス接続状態の複製

どの接続にも、1つのオーナーおよび少なくとも1つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDPのステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCPまたはUDPレイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *22:* クラスタ全体で複製される機能

トラフィック	状態のサポート	注記（Notes）
アップ タイム	○	システム アップ タイムをトラッキングします。
ARP テーブル	あり	—

トラフィック	状態のサポート	注記（Notes）
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	○	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	対応	—
ダイナミック ルーティング	対応	—
SNMP エンジン ID	なし	—
Firepower 4100/9300 用の分散型 VPN（サイト間）	Yes	バックアップ セッションがアクティブ セッションになると、新しいバックアップ セッションが作成されます。

ASA クラスタが接続を管理する方法

接続をクラスタの複数のメンバーにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信した TCP/UDP ステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタ ノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカル バックアップとグローバル バックアップの2つのバックアップ オーナー権限があります。オーナーは、常に同じサイトのローカル バックアップをオーナー自身として選択します（サイト ID に基づいて）。グローバル バックアップはどのサイトにも配置でき、ローカル バックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

サイトの冗長性が有効になっており、バックアップ オーナーがオーナーと同じサイトに配置されている場合は、サイトの障害からフローを保護するために、別のサイトから追加のバックアップ オーナーが選択されます。シャーシ バックアップとサイト バックアップは独立しているため、フローにはシャーシ バックアップとサイト バックアップの両方が含まれている場合があります。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルディレクタとグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（Site Id に基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにも配置でき、ローカルディレクタと同一ノードとすることもできます。最初のオーナーに障害が発生すると、ローカルディレクタは、同じサイトの新しい接続オーナーを選択します。

  ICMP/ICMPv6 ハッシュの詳細：

  - エコーパケットの場合、送信元ポートは ICMP 識別子で、宛先ポートは 0 です。
  - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
  - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタ ローカリゼーションを有効にすると、フォワーダは常にローカル ディレクタに問い合わせを行います。フォワーダがグローバル ディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタ メンバーが受信する場合などです。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN

クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化をディセーブルにした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

(注) クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを決定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。これが既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続の所有者はすべてのフラグメントを再構築します。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

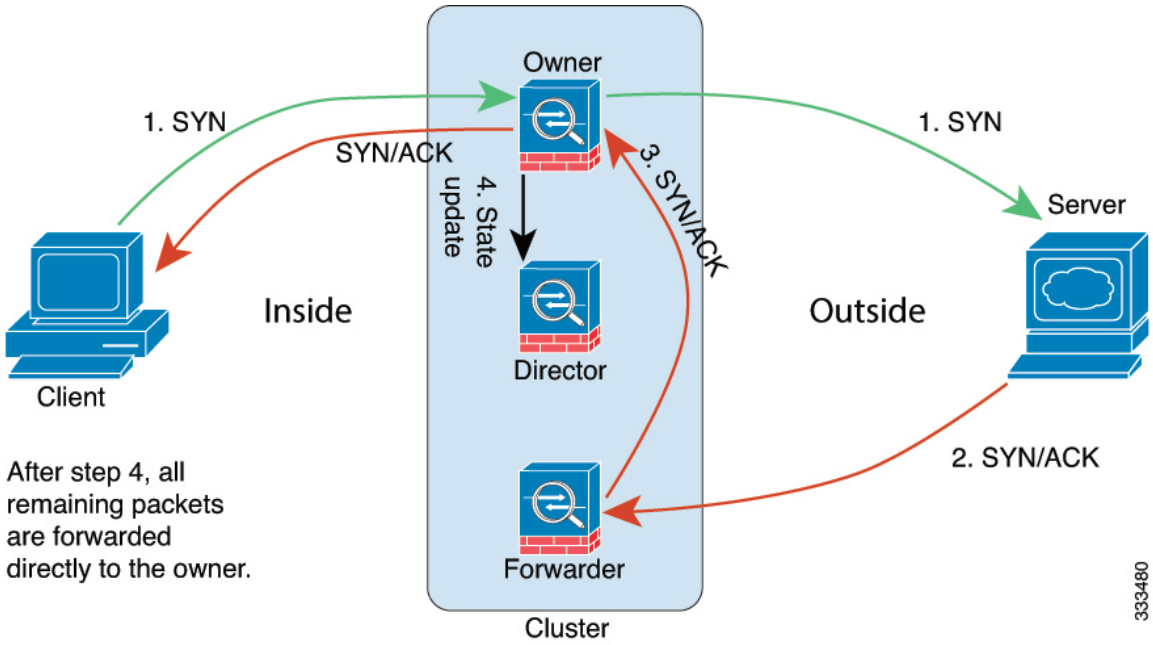
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1つのフローの両方向が同じノードに到着するとともに、フローがノード間に均等に分散されるようにするためです。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。



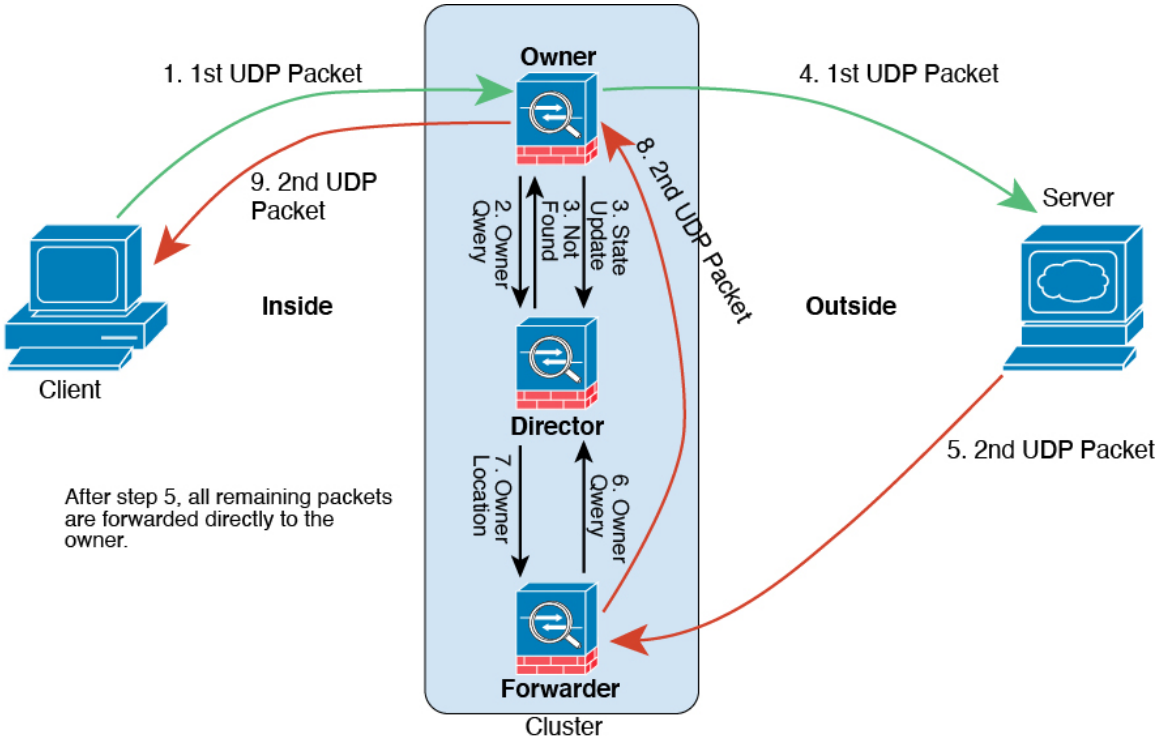
1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP 状態情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。

6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

1. 図 *57 : ICMP* および *UDP* データフロー



UDP パケットがクライアントから発信され、1 つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバーにパケットを転送します。

5. 2 番目の UDP パケットはサーバーから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

新しい TCP 接続のクラスタ全体での再分散

アップストリームまたはダウンストリームルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しい TCP フローを過負荷のノードから他のノードにリダイレクトするように設定できます。既存のフローは他のノードには移動されません。

ASA クラスタリングの履歴

機能名	バージョン	機能情報
データユニットとの設定の並列同期	9.14(1)	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable parallel configuration replicate]** チェックボックス
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 **show cluster history**	9.14(1)	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history** 新規/変更された画面：なし。
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新規/変更された画面：なし。

機能名	バージョン	機能情報
クラスタのトラフィック負荷のモニター	9.13(1)	クラスタ メンバのトラフィック負荷をモニターできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable Cluster Load Monitor]** チェックボックス • **[Monitoring]** > **[ASA Cluster]** > **[Cluster Load-Monitoring]**
クラスタ結合の高速化	9.13(1)	データユニットが制御ユニットと同じ設定の場合、設定の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。 （注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable config sync acceleration]** チェックボックス

機能名	バージョン	機能情報
サイトごとのクラスタリング用 Gratuitous ARP	9.12(1)	ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチング インフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Site Periodic GARP]**フィールド
クラスタインターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。	9.10(1)	インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで **health-check monitor-interface debounce-time** コマンドまたは ASDM **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタユニットの方がポートのバンドルが速いという理由だけで、クラスタユニット上でインターフェイスがエラー表示されるのを防ぐことができます。 変更された画面はありません。
内部障害発生後に自動的にクラスタに再参加する	9.9(2)	以前は、多くのエラー状態によりクラスタユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Auto Rejoin]**
クラスタの信頼性の高いトランスポートプロトコルメッセージのトランスポートに関連する統計情報の表示	9.9(2)	ユニットごとのクラスタの信頼性の高いトランスポート バッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**

機能名	バージョン	機能情報
ASA 5000-X シリーズに対してインターフェイスを障害としてマークするために設定可能なデバウンス時間	9.9(2)	ASA がインターフェイスを障害が発生していると見なし、ASA 5500-X シリーズ上のクラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。この機能は以前は Firepower 4100/9300 で使用できました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
クラスタリングのサイト間冗長性	9.9(1)	サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
クラスタ ユニット ヘルスチェック障害検出の改善	9.8(1)	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージング アクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビート メッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

機能名	バージョン	機能情報
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	9.7(1)	データ センターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]**
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	9.6(1)	スパンド EtherChannel のルーテッド モードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイ トランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次の画面を変更しました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add/Edit EtherChannel Interface]** > **[Advanced]**
ASA 5516-X でのクラスタリングのサポート	9.5(2)	ASA 5516-X が 2 ユニット クラスタをサポートするようになりました。基本ライセンスでは、2 ユニットのクラスタリングがデフォルトで有効化されています。 変更された ASDM 画面はありません。
サイト間フローモビリティの LISP インスペクション	9.5(2)	Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID をその場所から 2 つの異なるナンバリング スペースに分離し、サーバーの移行をクライアントに対して透過的にします。ASA は、場所変更の LISP トラフィックを検査し、その情報をシームレスなクラスタリング運用に活用できます。ASA クラスタ メンバーは、最初のホップ ルータと出力トンネル ルータまたは入力トンネル ルータの間の LISP トラフィックを検査し、フロー オーナーの所在場所を新規サイトに変更します。 次の画面が導入または変更されました。 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[LISP]** **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** > **[Protocol Inspection]** **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** > **[Cluster]** **[Monitoring]** > **[Routing]** > **[LISP-EID Table]**

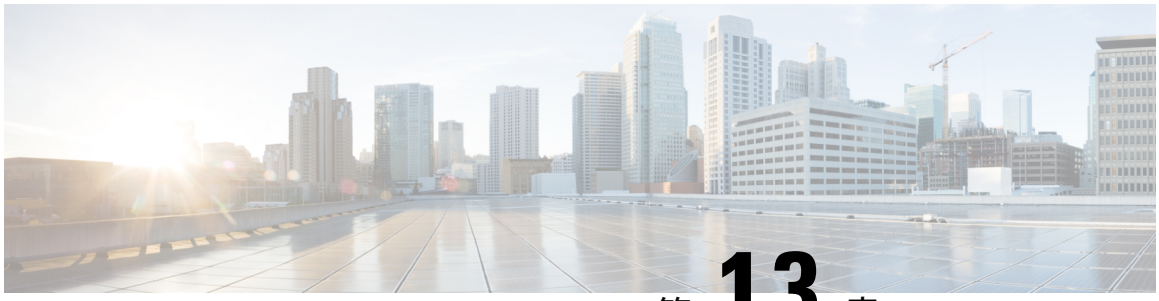
機能名	バージョン	機能情報
キャリア グレード NAT の強化がフェールオーバーおよび ASA クラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 変更された画面はありません。
クラスタリング トレース エントリの設定可能なレベル	9.5(2)	デフォルトで、すべてのレベル クラスタリング イベントは、多くの下位レベルのイベント以外に、トレース バッファに含まれます。より上位レベルのイベントへのトレースを制限するために、クラスタの最小トレース レベルを設定できます。 変更された画面はありません。
ルーテッド ファイア ウォール モードのスパンド EtherChannel のサイト間クラスタリング サポートのサイト別 MAC アドレス	9.5(1)	ルーテッド モードでは、スパンド EtherChannel サイト間クラスタリングを使用することができます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。 次の画面を変更しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]**
インターフェイスまたはクラスタ制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスタのカスタマイズ	9.5(1)	インターフェイスまたはクラスタ制御リンクが失敗した場合、auto-rejoin 動作をカスタマイズできます。 次の画面を導入しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Auto Rejoin]**
ASA クラスタは、GTPv1 と GTPv2 をサポートします	9.5(1)	ASA クラスタは、GTPv1 および GTPv2 インスペクションをサポートします。 変更された画面はありません。
ASA クラスタリングのハードウェア モジュールのヘルス モニターリングの無効化	9.5(1)	クラスタリング使用時、ASA はデフォルトで、設置されているハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニターリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニターリングをディセーブルにできます。 次の画面を変更しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]**
TCP 接続のクラスタ複製遅延	9.5(1)	この機能で、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。 次の画面を導入しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]**

機能名	バージョン	機能情報
インターフェイスごとの ASA クラスタのヘルスモニターリングの有効化またはディセーブル化	9.4(1)	ヘルスモニターリングは、インターフェイスごとにイネーブルまたはディセーブルにすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルスモニターリングがイネーブルになっています。ヘルス モニターリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニターリングは設定できません。このリンクは常にモニターされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニターリングをディセーブルにすることができます。 次の画面を導入しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]。
DHCP リレーの ASA クラスタリングのサポート	9.4(1)	ASA クラスタで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスタ メンバにロードバランスされます。DHCP クライアントおよびサーバー機能はサポートされていません。 変更された画面はありません。
ASA クラスタリングでの SIP インスペクションのサポート	9.4(1)	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 変更された画面はありません。
内部ネットワーク間に ASA クラスタ ファイアウォールを備えたトランスペアレントモードのサイト間導入	9.3(2)	各サイトの内部ネットワークとゲートウェイ ルータ間にトランスペアレント モードのクラスタを導入し（AKA イーストウェスト挿入）、サイト間に内部 VLAN を拡張できます。オーバーレイ トランスポート仮想化（OTV）の使用を推奨しますが、ゲートウェイ ルータの重複する MAC アドレスおよび IP アドレスがサイト間で漏えいしないようにする任意の方法を使用できます。HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、同じ仮想 MAC アドレスおよび IP アドレスをゲートウェイ ルータに提供します。
ASA クラスタリングに対する BGP のサポート	9.3(1)	ASA クラスタリングに対する BGP のサポートが追加されました。 次の画面を変更しました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]。
トランスペアレント モードでの異なる地理的位置にあるクラスタ メンバのサポート（サイト間）	9.2(1)	トランスペアレント ファイアウォール モードでスパンド EtherChannel モードを使用すると、クラスタ メンバを異なる地理的な場所に配置できるようになりました。ルーテッド ファイアウォール モードのスパンド EtherChannel での Inter-Site クラスタリングはサポートされません。 変更された ASDM 画面はありません。

機能名	バージョン	機能情報
クラスタリングに対するスタティック LACP ポートプライオリティのサポート	9.2(1)	一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティをディセーブルにすることで、スパンド EtherChannel との互換性を高めることができるようになりました。次の注意事項にも従う必要があります。 • クラスタ制御リンク パスのネットワーク エレメントでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。 • ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。 次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]。
スパンド EtherChannel での 32 個のアクティブ リンクのサポート	9.2(1)	ASA EtherChannels は最大 16 個のアクティブ リンクをサポートするようになりました。スパンド EtherChannel ではその機能が拡張されて、vPC の 2 台のスイッチで使用し、ダイナミック ポート プライオリティをディセーブルにした場合、クラスタ全体で最大 32 個のアクティブ リンクをサポートします。スイッチは、16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 8 個のアクティブ リンクをサポートする VSS または vPC のスイッチの場合は、スパンド EtherChannel に 16 個のアクティブ リンクを設定できます（各スイッチに接続された 8 個）。従来は、VSS/vPC で使用する場合であっても、スパンド EtherChannel は 8 個のアクティブ リンクと 8 個のスタンバイ リンクしかサポートしませんでした。 （注） スパンド EtherChannel で 8 個より多くのアクティブ リンクを使用する場合は、スタンバイ リンクも使用できません。9 ～ 32 個のアクティブ リンクをサポートするには、スタンバイ リンクの使用を可能にする cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。 次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。 変更された画面はありません。

機能名	バージョン	機能情報
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。 変更された ASDM 画面はありません。
ヘルス チェック モニターリングの VSS および vPC によるサポートの強化	9.1(4)	クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合、ヘルス チェック モニターリングによって安定性を高めることができます。一部のスイッチ（Cisco Nexus 5000 など）では、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続されている EtherChannel メンバー インターフェイスが ASA に対してアップと認識される場合がありますが、スイッチ側にはトラフィックが渡されていません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。VSS/vPC ヘルス チェック機能をイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。 次の画面を変更しました。[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]。
異なる地理的位置にあるクラスタ メンバのサポート（サイト間）。個別インターフェイス モードのみ	9.1(4)	個別インターフェイス モードを使用すると、クラスタ メンバを異なる地理的な場所に配置できるようになりました。 変更された ASDM 画面はありません。

機能名	バージョン	機能情報
ASA 5580 および 5585-X の ASA クラスタリング	9.0(1)	ASA クラスタリングを利用すると、最大で 8 の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASA クラスタリングは、ASA 5580 および ASA 5585-X でサポートされます。1 つのクラスタ内のすべてのユニットが同一モデル、同一ハードウェア仕様であることが必要です。クラスタリングがイネーブルのときにサポートされない機能のリストについては、コンフィギュレーション ガイドを参照してください。 次の画面が導入または変更されました。 **[Home] > [Device Dashboard] [Home] > [Cluster Dashboard] [Home] > [Cluster Firewall Dashboard] [Configuration] > [Device Management] > [Advanced] > [Address Pools] > [MAC Address Pools] [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] [Configuration] > [Device Management] > [Logging] > [Syslog Setup] > [Advanced] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [Advanced] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [IPv6] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced] [Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules] [Monitoring] > [ASA Cluster] [Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link] [Tools] > [Preferences] > [General] [Tools] > [System Reload] [Tools] > [Upgrade Software from Local Computer] [Wizards] > [High Availability and Scalability Wizard] [Wizards] > [Packet Capture Wizard] [Wizards] > [Startup Wizard]**



第 13 章

Firepower 4100/9300 の ASA クラスタ

クラスタリングを利用すると、複数のFirepower 4100/9300 シャーシ ASA をグループ化して、1 つの論理デバイスにすることができます。Firepower 4100/9300 シャーシ シリーズには、Firepower 9300 および Firepower 4100 シリーズ が含まれます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。クラスタリングでサポートされない機能 （580 ページ） を参照してください。

Firepower 4100/9300 シャーシのクラスタリングについて

Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポートチャネル 48）を作成します。

シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通信にFirepower 9300 バックプレーンを使用します。

シャーシ間クラスタリングでは、シャーシ間通信用にこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがシャーシスーパバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

  シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのようにEtherChannelに制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部でEtherChannelテクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。 シャーシ間クラスタリングでは、すべてのデータ インターフェイスでスパンド EtherChannel を使用します。

  注 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ブートストラップ コンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがFirepower 4100/9300シャーシスーパバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部はユーザーが設定できます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバーの1つが**制御**ユニットになります。制御ユニットは自動的に決定されます。他のすべてのメンバーは**データ**ユニットになります。

すべてのコンフィギュレーション作業は制御ユニット上でのみ実行する必要があります。コンフィギュレーションはその後、データユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能 （581 ページ）を参照してください。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポート チャネル 48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信のために、Firepower 4100/9300 シャーシ のこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

2 シャーシのシャーシ間クラスタの場合、シャーシと他のシャーシの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- 状態の複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- ネットワークアクセスに対する AAA は一元的な機能であるため、すべてのトラフィックが制御ユニットに転送されます。

- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

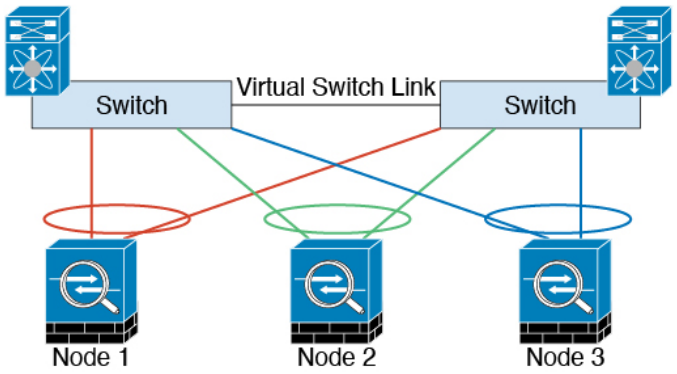
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンク冗長性

クラスタ制御リンクにはEtherChannelを使用することを推奨します。冗長性を実現しながら、EtherChannel内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとしてEtherChannelを使用する方法を示します。EtherChannelのすべてのリンクがアクティブです。スイッチがVSSまたはvPCの一部である場合は、同じEtherChannel内のファイアウォールインターフェイスをそれぞれ、VSSまたはvPC内の異なるスイッチに接続できます。スイッチインターフェイスは同じEtherChannelポートチャネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。このEtherChannelは、スパンドEtherChannelではなく、デバイスローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が20 ms未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタメンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクでpingを実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。クラスタを展開するときに、この IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。 サイト間トラフィックには、オーバーレイ トランスポート仮想化（OTV）を使用することをお勧めします。

クラスタ インターフェイス

シャーシ内クラスタリングでは、物理インターフェイスと EtherChannel（ポート チャネルとも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンド インターフェイスです。

シャーシ間クラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンド EtherChannel は、各シャーシの同じメンバー インターフェイスを含みます。上流に位置するスイッチでは、これらのインターフェイスはすべて単一の EtherChannel に含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

VSS または vPC への接続

インターフェイスの冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

ASA クラスタの管理

ASA クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ユニットに属します。アドレス範囲も設定して、現在の制御ユニットを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタの管理をシームレスに続行できます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の制御ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、制御ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバーに接続します。

制御ユニット管理とデータユニット管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。また、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。
- ノードごとの Syslog モニタリング（コンソールレプリケーションが有効な場合にコンソールに送信される Syslog を除く）。
- SNMP
- NetFlow

暗号キー複製

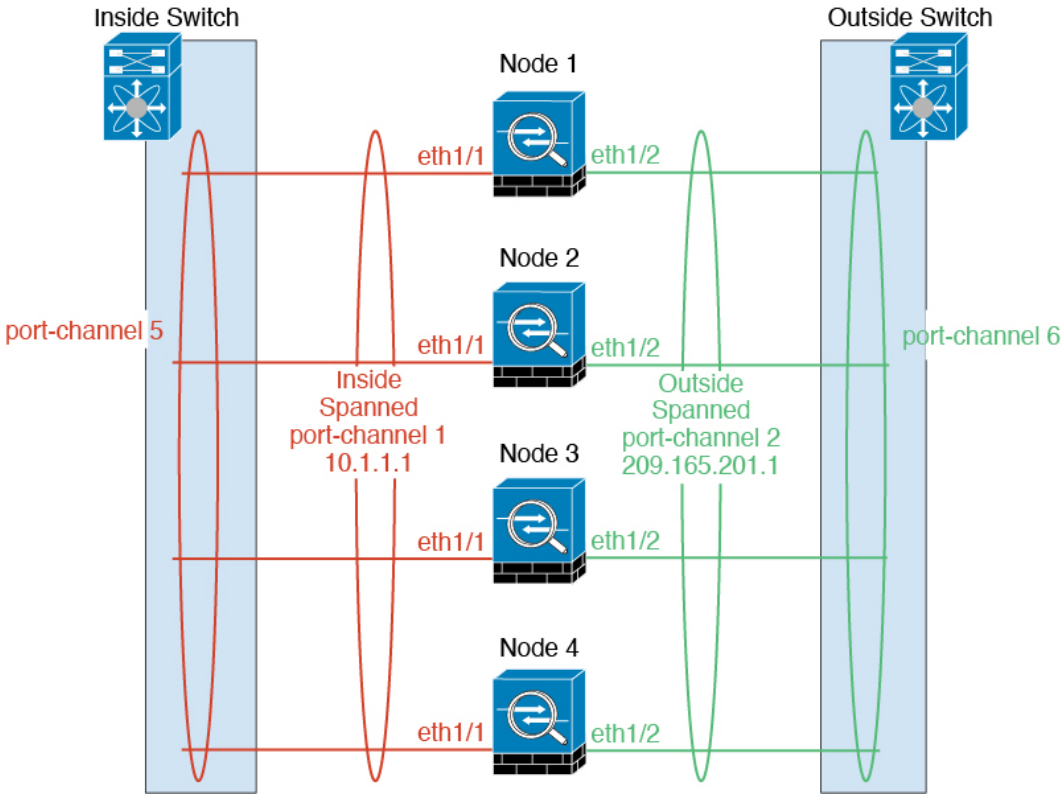
制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH 接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

スパンド EtherChannel（推奨）

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジ グループ メンバのインターフェイスではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト ID は、LISP インスペクションを使用するフロー モビリティ、データセンターのサイト間クラスタリングのパフォーマンスを向上し、ラウンドトリップ時間の遅延を減少させるためのディレクタ ローカリゼーション、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトにある接続のサイト冗長性を有効にするためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 （518 ページ）
- サイト間のガイドライン：クラスタリング ガイドラインと制限事項 （522 ページ）
- クラスタ フロー モビリティの設定：クラスタ フロー モビリティの設定 （547 ページ）
- ディレクタ ローカリゼーションの有効化：ASA クラスタの基本パラメータの設定 （540 ページ）
- サイト冗長性の有効化：ASA クラスタの基本パラメータの設定 （540 ページ）

Firepower4100/9300シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリング ユニット

- Firepower 4100：16 シャーシ
- Firepower 9300：16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。

インター シャーシ クラスタ化に関するハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower 4100 シリーズ：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。各シャーシに異なる数のセキュリティ モジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。
- イメージアップグレード時を除き、同じ FXOS ソフトウェアを実行する必要があります。
- 同じ管理インターフェイス、EtherChannel、アクティブ インターフェイス、速度、デュプレックスなど、クラスタに割り当てるインターフェイスについても同じインターフェイスの設定を含める必要があります。同じインターフェイス ID の容量が一致し、同じスパンド EtherChannel にインターフェイスを正常にバンドルできれば、シャーシに異なるネットワーク モジュール タイプを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイスモジュールの追加や削除、または EtherChannel の設定などにより）クラスタリングを有効にした後に FXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データ ノードから始めて、制御ノードで終わります）。FXOS でインターフェイスを削除した場合、必要な調整を行うことができるように、ASA 設定では関連するコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。古いインターフェイス設定は手動で削除することができます。
- 同じ NTP サーバを使用する必要があります。時間を手動で設定しないでください。
- ASA：各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。データ ノードは追加料金なしで使用できます。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firepower Threat Defense では、すべてのライセンスは Firepower Management Center で処理されます。

スイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチの特性については、『Cisco FXOS Compatibility』を参照してください。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect（DCI）に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCIの最小帯域幅は、1 つのメンバーに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバーの場合。
  - 合計 4 クラスタ メンバー
  - 各サイト 2 メンバー
  - メンバーあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。
- 3 サイトの 6 メンバーの場合、サイズは増加します。
  - 合計 6 クラスタ メンバー
  - サイト 1 は 3 メンバー、サイト 2 は 2 メンバー、サイト 3 は 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。
- 2 サイトの 2 メンバーの場合。
  - 合計 2 クラスタ メンバー
  - 各サイト 1 メンバー
  - メンバーあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

でのクラスタリングのライセンス Firepower 4100/9300 シャーシ

通常またはサテライト スマート ライセンシング

クラスタリング機能自体にライセンスは必要ありません。高度暗号化およびその他のオプションライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシが License Authority またはサテライトサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASAライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます:

- 標準：制御ユニットのみがサーバから標準ライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトで標準ライセンスは 10 のコンテキストを含み、すべてのクラスタ メンバー上に存在します。各ユニットの標準ライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタに 6 台の Firepower9300 モジュールがある場合を考えます。標準ライセンスは 10 のコンテキストを含みます。6 つユニットの場合、合計で 60 のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 80 のコンテキストを含みます。モジュールごとのプラットフォーム制限は250であるため、統合されたライセンスに最大 250 のコンテキストが許容されます。80 のコンテキストは制限範囲内です。したがって、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して80コンテキストを持つことになります。
  - クラスタに Firepower4110 が 3 台あるとします。標準ライセンスは 10 のコンテキストを含みます。3つユニットの場合、合計で30のコンテキストが加算されます。制御ユニット上で追加の250コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 280 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大250のコンテキストが許容されます。280コンテキストは制限を超えています。したがって、制御ユニット上で最大250のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して250のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして220のコンテキストのみを設定する必要があります。
- キャリア：分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager サテライト展開用、または管理目的用）—このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、

データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

分散型 S2S VPN のライセンス

キャリア ライセンスは、クラスタの各メンバーで、分散型 S2S VPN に必要です。

各 VPN 接続には、2 つの *Other VPN* ライセンス済みセッションが必要です（*Other VPN* ライセンスは基本ライセンスの一部です）。1 つはアクティブ セッション用、もう 1 つはバックアップ セッション用です。クラスタの最大 VPN セッション容量は、セッションごとに 2 つのライセンスを使用するため、ライセンス済み容量の半分以下にすることができます。

クラスタリング ガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンクインターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンクインターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。

- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシング アルゴリズムは変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannelインターフェイスは一時的にトラフィックの転送を停止し、スパニングツリープロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効化することで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

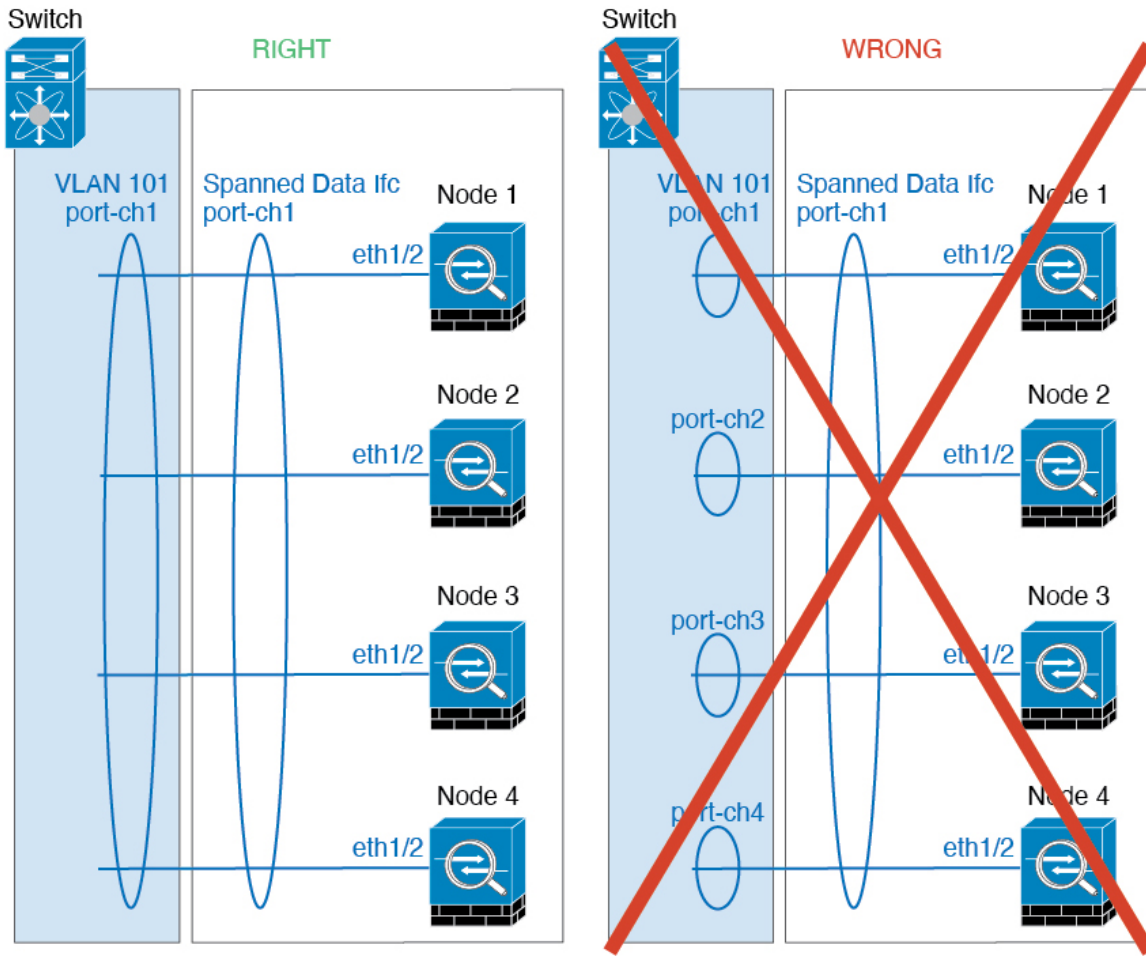
- ASA ハードウェアクラスタとは異なり、Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、Firepower プラットフォームでは、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際にLACP高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。

シャーシ間クラスタリングの EtherChannel

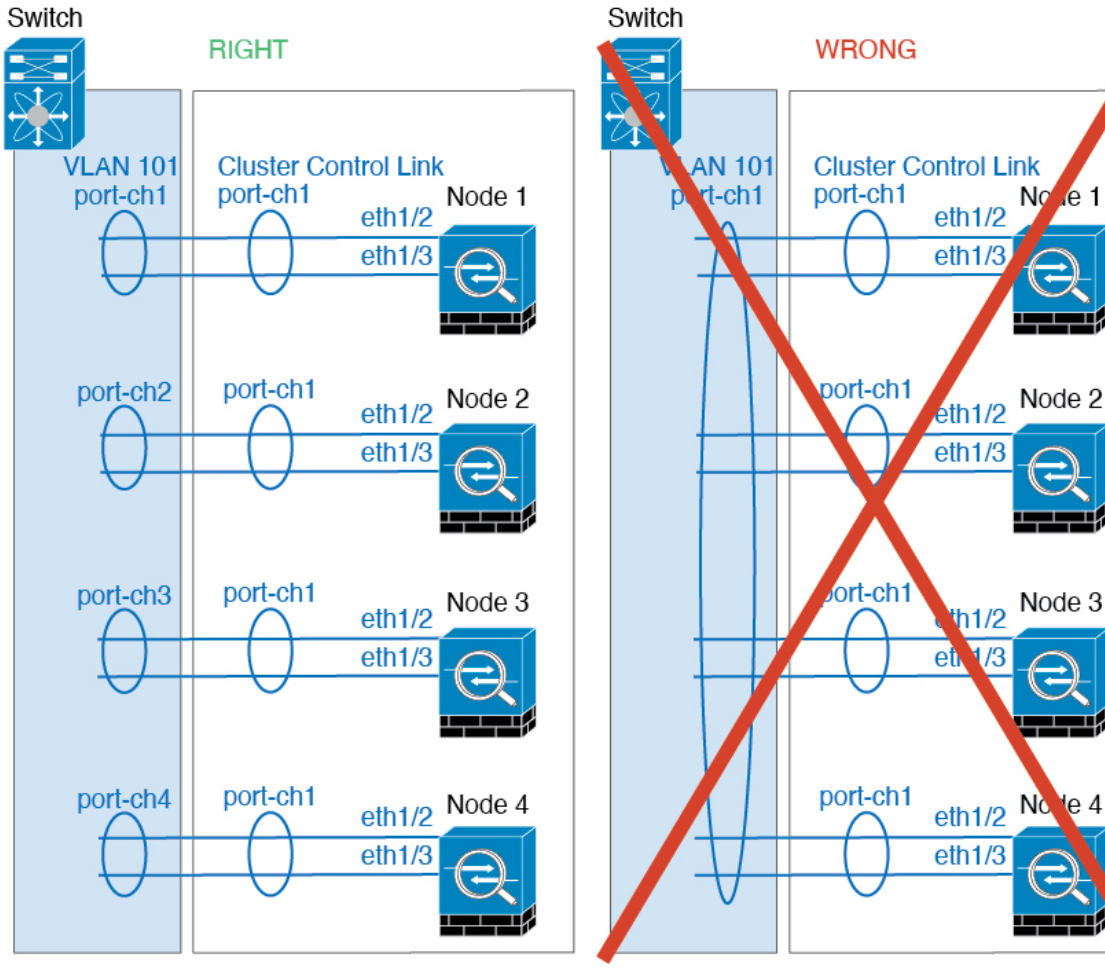
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでし

た。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



  - デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- ASA は専用リンクであるため、データセンター相互接続（DCI）で使用されている場合でも、クラスタ制御リンクで転送されるデータトラフィックを暗号化しません。オーバーレイトランスポート仮想化（OTV）を使用する場合、またはローカル管理ドメインの外部でクラスタ制御リンクを拡張する場合は、OTE を介した 802.1AE MacSec などの境界ルータで暗号化を設定できます。

- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタ ローカリゼーションを有効にすると、ローカル ディレクタのロールは（サイト ID に従って）常に接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。

- ディレクタ ローカリゼーションでは、次のトラフィック タイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション クエリ。

- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じMACアドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバーがサイト 2 のメンバーに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。

- トランスペアレントモードの場合、内部ネットワーク間のファイアウォール用に各サイトのデータ ネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。

- トランスペアレントモードでは、クラスタが HSRP ルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして ASA に追加する必要があります（ブリッジ グループのスタティック MAC アドレスの追加 （830 ページ）を参照）。隣接ルータで HSRP が使用される場合、HSRP IP アドレス宛てのトラフィックは HSRP MAC アドレスに送信されますが、リターントラフィックは特定のルータのインターフェイスの MAC アドレスから HSRP ペアで送信されます。したがって、ASA MACアドレステーブルは通常、HSRP IPアドレスの ASA ARP テーブルエントリが期限切れになり、ASA が ARP 要求を送信して応答を受信した場合にのみ更新されます。ASA の ARP テーブルエントリはデフォルトで 14400 秒後に期限切れになりますが、MAC アドレステーブルエントリはデフォルトで 300 秒後に期限切れになるため、MAC アドレステーブルの期限切れトラフィックのドロップを回避するために静的 MAC アドレスエントリが必要です。

- スパンド EtherChannel を使用したルーテッド モードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないよ

うにするには、フィルタを作成する必要があります。クラスタが1つのサイトで到達不能になった場合、トラフィックが他のサイトのクラスタノードに正常に到達できるようにフィルタを削除する必要があります。ダイナミックルーティングは、サイト間クラスタが拡張セグメントのファースト ホップ ルータとして機能する場合はサポートされません。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannelインターフェイスの追加または削除、Firepower4100/9300シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイス モニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。
- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5 分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

でのクラスタリングの設定 Firepower 4100/9300 シャーシ

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタ メンバーを管理する方法についても説明します。クラスタ メンバーシップは Firepower 4100/9300 シャーシからも管理できます。詳細については、Firepower 4100/9300 シャーシ のマニュアルを参照してください。

手順

ステップ 1 FXOS：ASA クラスタの追加 （528 ページ）
ステップ 2 ASA：ファイアウォール モードとコンテキスト モードの変更 （537 ページ）
ステップ 3 ASA：データ インターフェイスの設定 （538 ページ）
ステップ 4 ASA：クラスタ設定のカスタマイズ （540 ページ）
ステップ 5 ASA：クラスタ メンバの管理 （559 ページ）

FXOS：ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、導入を簡単にするため、ブートストラップ設定を最初のシャーシから次のシャーシにコピーし、

ASA クラスタの作成

範囲をイメージバージョンに設定します。

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

シャーシ間クラスタリングでは、各シャーシを別々に設定します。導入を容易にするために、1 つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3 つのすべてのモジュールでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

クラスタを導入すると、Firepower 4100/9300 シャーシ スーパバイザが次のブートストラップ コンフィギュレーションで各 ASA アプライアンスを設定します。ブートストラップ コンフィギュレーションの一部（**太字**のテキストで示されている部分）は、後から必要に応じて ASA から変更できます。

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

（注） **local-unit** 名は、クラスタリングを無効化した場合にのみ変更できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレスおよびネットワークマスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 インターフェイスを設定します。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。EtherChannel（ポート チャネル）の追加（232 ページ）または物理インターフェイスの設定 （231 ページ）を参照してください。

シャーシ間クラスタリングの場合は、すべてのデータインターフェイスが、少なくとも 1 つのメンバーインターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタユニットからメンバーインターフェイスを 1 つの EtherChannel へと結合します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （522 ページ） を参照してください。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポートチャネル）の追加 （232 ページ）または物理インターフェイスの設定 （231 ページ）を参照してください。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

シャーシ間クラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

c) シャーシ間クラスタリングでは、メンバーインターフェイスをクラスタ制御リンクの EtherChannel（デフォルトではポートチャネル 48）に追加します。EtherChannel（ポートチャネル）の追加 （232 ページ） を参照してください。

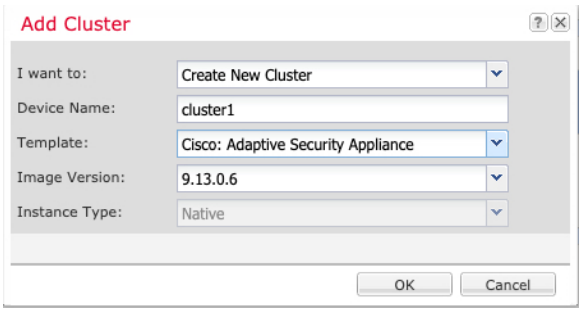
シャーシ内クラスタリングのメンバー インターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタがシャーシ間であると見なし、例えばスパンド Etherchannel のみを使用できるようになります。

[インターフェイス（Interfaces）] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバ インターフェイスが含まれていない場合は、[動作状態（Operation State）] を [失敗（failed）] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバ インターフェイスを必要としないため、この動作状態は無視して構いません。

各シャーシに同じメンバインターフェイスを追加します。クラスタ制御リンクは、各シャーシのデバイスローカル EtherChannel です。デバイスごとにスイッチで個別の EtherChannel を使用します。シャーシ間クラスタリングの EtherChannel についての詳細は、クラスタリング ガイドラインと制限事項 （522 ページ） を参照してください。

ステップ 2 [論理デバイス（Logical Devices）] を選択します。

ステップ 3 **[追加（Add）] > [クラスタ（Cluster）]** をクリックし、次のパラメータを設定します。



a) **[必要な操作（I want to:）]** > **[新しいクラスタの作成（Create New Cluster）]** を選択します。
b) **デバイス名**を入力します。

この名前は、シャーシスーパバイザが管理設定を行ってインターフェイスを割り当てるために内部で使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

c) [テンプレート（Template）] には、[Cisco 適応型セキュリティ アプライアンス（Cisco Adaptive Security Appliance）] を選択します。
d) [Image Version] を選択します。
e) [Instance Type] では、[Native] タイプのみがサポートされます。
f) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

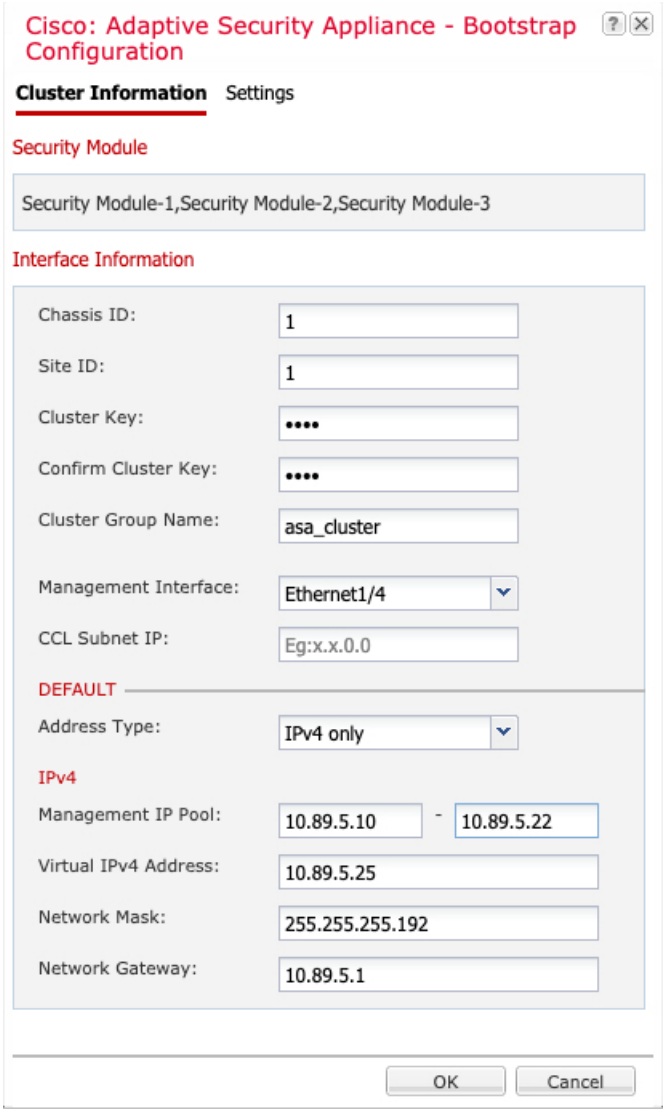
ステップ 4 このクラスタに割り当てるインターフェイスを選択します。

デフォルトでは、すべての有効なインターフェイスが割り当てられています。マルチクラスタタイプのインターフェイスを定義した場合は、すべての選択を解除し、1 つのみ選択します。

ステップ 5 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 6 [クラスタ情報（Cluster Information）] ページで、次の手順を実行します。



a) シャーシ間クラスタリングでは、**シャーシ ID** フィールドに、シャーシ ID を入力します。クラスタの各シャーシに固有の ID を使用する必要があります。

このフィールドは、クラスタ制御リンク Port-Channel 48 にメンバー インターフェイスを追加した場合にのみ表示されます。

b) サイト間クラスタリングの場合、[サイト ID（Site ID）] フィールドに、このシャーシのサイト ID を 1 ～ 8 の範囲で入力します。

c) [Cluster Key] フィールドで、クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

d) [クラスタ グループ名（Cluster Group Name）] を設定します。これは、論理デバイス設定のクラスタ グループ名です。

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

e) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

f) 管理インターフェイスの [アドレスタイプ（Address Type）] を選択します。

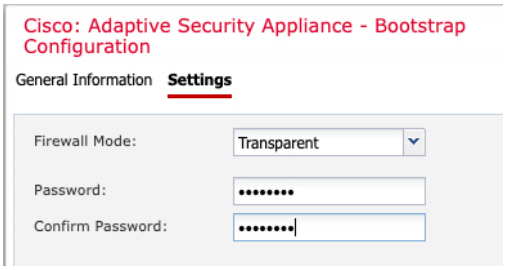
この情報は、ASA 設定で管理インターフェイスを設定するために使用されます。次の情報を設定します。

- [管理IPプール（Management IP Pool）]：開始アドレスと終了アドレスをハイフンで区切って入力し、ローカル IP アドレスのプールを設定します。このうちの 1 つがインターフェイス用に各クラスタユニットに割り当てられます。

  最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在の制御ユニットに属する仮想 IP アドレス（メインクラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

- **ネットワークマスク**または**プレフィックス長**
- **ネットワークゲートウェイ**
- [仮想IPアドレス（Virtual IP address）]：現在の制御ユニットの管理 IP アドレスを設定します。この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

ステップ 7 [Settings] ページで、以下を実行します。



a) [ファイアウォール モード（Firewall Mode）] ドロップダウン リストから、[トランスペアレント（Transparent）] または [ルーテッド（Routed）] を選択します。

ルーテッドモードでは、FTDはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレ

ント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

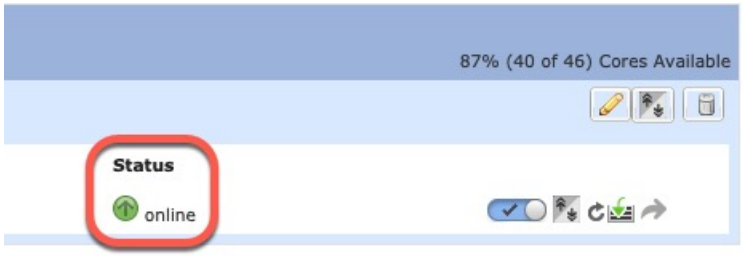
b) 管理者ユーザの [Password] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されている場合、残りのクラスタシャーシを追加するか、シャーシ内クラスタリングでアプリケーションのクラスタの設定を開始できます。このプロセスの一環として、[セキュリティ モジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 10 シャーシ間クラスタリングでは、クラスタに次のシャーシを追加します。

a) 最初のシャーシの Firepower Chassis Manager で、右上の [設定の表示（Show Configuration）] アイコンをクリックして、表示されるクラスタ設定をコピーします。

b) 次のシャーシの Firepower Chassis Manager に接続し、この手順に従って論理デバイスを追加します。

c) [必要な操作（I want to:）] > [既存のクラスタへの参加（Join an Existing Cluster）] を選択します。

d) **[OK]** をクリックします。

e) [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

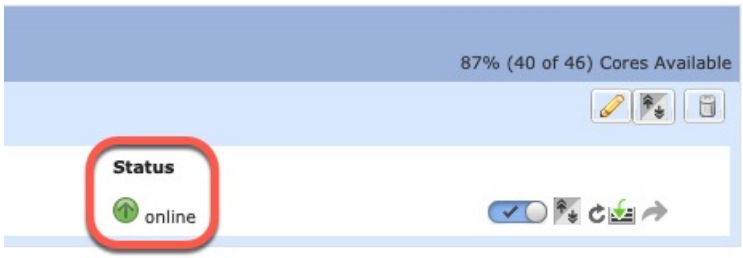
f) 画面中央のデバイスアイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **サイト ID（Site ID）**：正しいサイト ID を入力します。
- **クラスタ キー（Cluster Key）**：（事前に入力されていない）同じクラスタ キーを入力します。

[OK] をクリックします。

g) [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバーの [論理デバイス（Logical Devices）] ページで、新しい論理デバイスのステータスを確認します。各クラスタメンバーの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ステップ 11 制御ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

クラスタ メンバの追加

ASA クラスタ メンバを追加または置き換えます。

（注） この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

始める前に

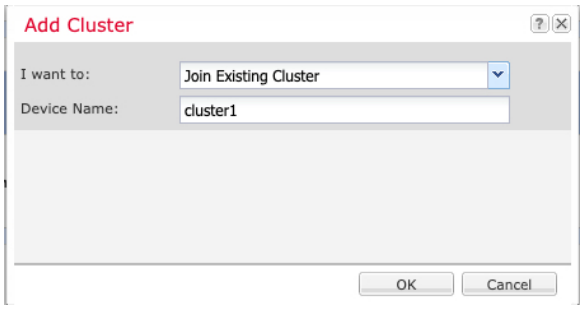
- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタ ブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。
- マルチ コンテキスト モードでは、最初のクラスタ メンバの ASA アプリケーションでマルチ コンテキスト モードを有効にします。追加のクラスタ メンバはマルチ コンテキスト モード設定を自動的に継承します。

手順

ステップ 1 既存のクラスタ シャーシ Firepower Chassis Manager で、[Logical Devices] を選択して [Logical Devices] ページを開きます。

ステップ 2 右上の [設定を表示（Show Configuration）] アイコン（  ）をクリックして、表示されるクラスタの設定をコピーします。

ステップ 3 新しいシャーシの Firepower Chassis Manager に接続して、**[追加（Add）]**>**[クラスタ（Cluster）]** をクリックします。



ステップ 4 **[I want to:]** > **[Join an Existing Cluster]**を選択します。

ステップ 5 [Device Name] に論理デバイスの名前を入力します。

ステップ 6 [OK] をクリックします。

ステップ 7 [クラスタ詳細のコピー（Copy Cluster Details）] ボックスに、最初のシャーシのクラスタ設定を貼り付け、[OK] をクリックします。

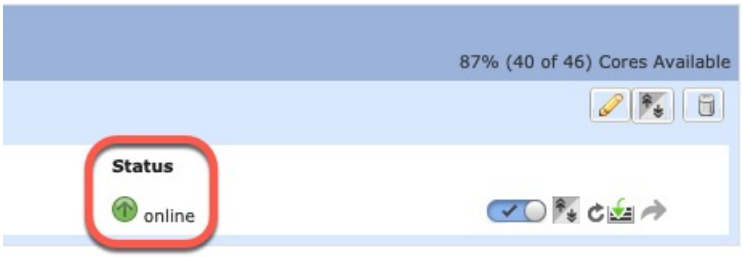
ステップ 8 画面中央のデバイス アイコンをクリックします。クラスタ情報は大半は事前に入力済みですが、次の設定は変更する必要があります。

- [シャーシ ID（Chassis ID）]：一意のシャーシ ID を入力します。
- **サイト ID（Site ID）**：正しいサイト ID を入力します。
- **クラスタ キー（Cluster Key）**：（事前に入力されていない）同じクラスタ キーを入力します。

[OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。各クラスタメンバーの [論理デバイス（Logical Devices）] ページで、新しい論理デバイスのステータスを確認します。各クラスタメンバーの論理デバイスの [ステータス（Status）] に [オンライン（Online）] と表示されたら、アプリケーションでクラスタの設定を開始できます。このプロセスの一環として、[セキュリティモジュールが応答していません（Security module not responding）] というステータスが表示されることがあります。このステータスは正常であり、一時的な状態です。



ASA：ファイアウォール モードとコンテキスト モードの変更

デフォルトでは、FXOS シャーシはルーテッド ファイアウォール モード、およびシングル コンテキスト モードでクラスタを展開します。

- ファイアウォールモードの変更：展開後にモードを変更するには、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。を参照してください。ファイアウォール モード（シングル モード）の設定（258 ページ）マルチ コンテキスト モードでは、コンテキストごとにファイアウォール

モードを設定します。セキュリティ コンテキストの設定（308 ページ）を参照してください。

- マルチコンテキストモードに変更：展開後にマルチコンテキストモードに変更するには、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。マルチ コンテキスト モードの有効化（301 ページ）を参照してください。

ASA：データ インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。

（注） 管理インターフェイスは、クラスタを展開したときに事前設定されました。ASA で管理インターフェイス パラメータを変更することもできますが、この手順はデータ インターフェイスに焦点を当てています。管理インターフェイスは、スパンドインターフェイスとは対照的に、個別のインターフェイスです。詳細については、「管理インターフェイス（516 ページ）」を参照してください。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。ブリッジ仮想インターフェイス（BVI）の設定（685 ページ）を参照してください。
- シャーシ間クラスタリングにスパンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 3 次の設定を行います。

- （EtherChannel の場合）[MIO Port-channel ID]：FXOS で使用されるのと同じ ID を入力します。
- [**Enable Interface**]（デフォルトでオンになります）

この画面の残りのフィールドは、この手順の後半で説明します。

ステップ 4 MAC アドレスおよびオプション パラメータを設定するには、[Advanced] タブをクリックします。

- [MAC Address Cloning] 領域で、EtherChannel の手動グローバル MAC アドレスを設定します。スタンバイ MAC アドレスを設定しないでください。無視されます。潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel にはグローバル MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在の制御ユニットに留まります。MAC アドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

  マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

- サイト間クラスタリングの場合、[ASA Cluster] 領域で、**サイト固有の MAC アドレスを、**ルーテッド モードの場合は IP アドレスを設定するために、[Add] をクリックして、サイト ID（1 ～ 8）の MAC アドレスおよび IP アドレスを指定します。最大 8 つのサイトで上記の手順を繰り返します。サイト固有の IP アドレスは、グローバル IP アドレスと同じサブネット上にある必要があります。ユニットで使用するサイト固有の MAC アドレスおよび IP アドレスは、各ユニットのブートストラップ コンフィギュレーションに指定したサイト ID によって異なります。

ステップ 5 （オプション）この EtherChannel に VLAN サブインターフェイスを設定します。この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 6 （マルチ コンテキスト モード）この手順を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

a) [OK] をクリックして変更内容を確定します。
b) インターフェイスを割り当てます。
c) ユーザーが設定するコンテキストを変更します。[Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
d) [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択し、カスタマイズするポートチャネル インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 7 [General] タブをクリックします。

ステップ 8 （トランスペアレント モード）[Bridge Group] ドロップダウン リストから、このインターフェイスを割り当てるブリッジ グループを選択します。

ステップ 9 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 10 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

ステップ 11 （ルーテッド モード）IPv4 アドレスに対して [Use Static IP] オプション ボタンをクリックし、IP およびマスクを入力します。DHCP と PPPoE はサポートされません。ポイントツーポイント接続の場合、31 ビットのサブネット マスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。トランスペアレント モードの場合は、EtherChannel インターフェイスではなく、ブリッジ グループ インターフェイスの IP アドレスを設定します。

ステップ 12 （ルーテッド モード）IPv6 アドレスを設定するには、[IPv6] タブをクリックします。

トランスペアレント モードの場合は、EtherChannel インターフェイスではなく、ブリッジ グループ インターフェイスの IP アドレスを設定します。

a) [Enable IPv6] チェックボックスをオンにします。
b) [Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

（注） [Enable address autoconfiguration] オプションはサポートされません。

c) [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、2001:DB8::BA98:0:3210/64。
d) （オプション）ホスト アドレスとして Modified EUI-64 インターフェイス ID を使用するには、[EUI-64] チェックボックスをオンにします。この場合は、単に [Address/Prefix Length] フィールドにプレフィックスを入力します。
e) [OK] をクリックします。

ステップ 13 [OK] をクリックして、[Interfaces] 画面に戻ります。

ステップ 14 [Apply] をクリックします。

ASA：クラスタ設定のカスタマイズ

クラスタを展開した後にブートストラップ設定を変更する場合や、クラスタリング ヘルス モニターリング、TCP 接続複製の遅延、フロー モビリティ、およびその他の最適化など、追加のオプションを設定する場合は、制御ユニットで行うことができます。

ASA クラスタの基本パラメータの設定

制御ユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチコンテキストモードでは、制御ユニット上のシステム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- local-unit **Member Name** およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合に ASA でのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** の順に選択します。

ステップ 2 （任意） 次のオプション パラメータを設定します。

- **Site Periodic GARP**—The ASA generates gratuitous ARP（GARP）packets to keep the switching infrastructure up to date: the highest priority member at each site periodically generates GARP traffic for the global MAC/IP addresses. 各スパンド EtherChannel のユニットと、サイト MAC および IP アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。GARP 間隔を 1 ～ 1000000 秒に設定します。デフォルトは 290 秒です。

  クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチング インフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

- [Enable connection rebalancing for TCP traffic across all the ASAs in the cluster]：接続の再分散をイネーブルにします。このパラメータはデフォルトではディセーブルになっています。イネーブルの場合は、クラスタの ASA は定期的に負荷情報を交換し、負荷のかかっているデバイスから負荷の少ないデバイスに新しい接続をオフロードします。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、制御ユニットからデータユニットに複製されます。

- [Enable cluster load monitor]：クラスタメンバのトラフィック負荷をモニターできるようになりました。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティモジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティモジュールがクラスタを離れると、

そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ユニットでクラスタリングを手動で無効にすることを選択できます。

次の値を設定します。

- [**Time Interval**]: モニターリングメッセージ間の時間を、10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。
- [**Number Of interval**]: ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

トラフィック負荷を表示するには、**[Monitoring] > [ASA Cluster] > [Cluster Load-Monitoring]** を参照してください。

- [Enable health monitoring of this device within the cluster]：クラスタユニットのヘルスチェック機能を有効にして、ユニット ハートビート ステータス メッセージ間の間隔を .3 から 45 秒の間で設定します。デフォルトは 3 秒です。**注**：新しいユニットをクラスタに追加していて、ASA またはスイッチのトポロジが変更される場合、クラスタが完成するまでこの機能を一時的にディセーブルにし、ディセーブルにされたインターフェイスのインターフェイス モニターリングもディセーブルにする必要があります（**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Interface Health Monitoring]**）。クラスタとトポロジの変更が完了したら、この機能を再度イネーブルにすることができます。ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにハートビート メッセージを送信します。ユニットが保留時間内にピアユニットからハートビートメッセージを受信しない場合は、そのピアユニットは応答不能またはデッド状態と見なされます。

- [Debounce Time]：ASA がインターフェイスに障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定します。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。 ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタユニットの方がポートのバンドルが速いという理由だけで、クラスタユニット上でインターフェイスがエラー表示されるのを防ぐことができます。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。

- [Replicate console output]：データユニットから制御ユニットへのコンソール複製を有効にします。この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力する場合があります。コンソール複製をイネーブルにすると、データユニットから制御ユニットにコンソールメッセージが送信されるので、モニターが必要になるのはクラスタのコンソールポート 1 つだけとなります。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、制御ユニットからデータユニットに複製されます。

- **クラスタリング フロー モビリティを有効にします。**LISP インスペクションの設定 （549 ページ）を参照してください。

- [Enable Director Localization for inter-DC cluster]：データセンターのサイト間クラスタリングでパフォーマンスを向上させてラウンドトリップ時間の遅延を短縮するには、ディレクタ ローカリゼーションを有効にします。通常、新しい接続はロード バランスされて、特定のサイト内のクラスタ メンバーにより所有されます。ただし、ASA はディレクタの役割を任意のサイトでメンバーに割り当てます。ディレクタ ローカリゼーションにより、追加のディレクタ役割がイネーブルになります。これは、所有者と同じサイトに存在するローカル ディレクタと、任意のサイトに配置できるグローバル ディレクタです。所有者とディレクタを同じサイトに配置することで、パフォーマンスが向上します。また、元の所有者で障害が発生した場合、ローカルディレクタは、同じサイトで新しい接続所有者を選択します。クラスタ メンバーが別のサイトで所有されている接続のパケットを受信する場合は、グローバル ディレクタが使用されます。

- [Site Redundancy]：サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。ディレクタ ローカリゼーションとサイトの冗長性は別々の機能です。そのうちの 1 つまたは両方を設定することができます。

- [Enable config sync acceleration]：データユニットが制御ユニットと同じ構成の場合、構成の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。

  （注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。

- [Enable parallel configuration replicate]：データユニットと並行して設定変更が同期化されるように、制御ユニットを有効にします。そうしないと、同期が順番に実行され、多くの時間がかかることがあります。

ステップ 3 [Cluster Control Link] 領域で、クラスタ制御リンクの MTU を設定できます。この領域のその他のオプションは、ASA では設定できません。

- [MTU]：クラスタ制御リンクインターフェイスの最大伝送ユニットを指定します。データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。MTU の最大値を 9184 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。

  たとえば、最大 MTU は 9184 バイトであるため、データインターフェイスの最大 MTU は 9084 になり、クラスタ制御リンクは 9184 に設定できます。

ステップ 4 （任意） [Cluster LACP] 領域で、スタティック ポートの優先順位を有効にできます。ASA は cLACP を使用して、EtherChannel とネイバー スイッチのネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの（仮想）デバイスであるかのように見えます。この領域のその他のオプションは、クラスタリングを無効化せずに、ASA では設定できません。

- [Enable static port priority]：LACP のダイナミック ポート プライオリティをディセーブルにします。一部のスイッチはダイナミック ポート プライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。さらに、8 個より多くのアクティブなスパンド EtherChannel メンバのサポートがイネーブルになります（最大 32 メンバ）。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ コンフィギュレーションの一部ではなく、制御ユニットからデータユニットに複製されます。

ステップ 5 （任意） （Firepower 9300 のみ）[Parallel Join of Units Per Chassis] 領域で、シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されていることを確認できます。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。

- **num_of_units**：モジュールがクラスタに参加する前に準備する必要がある同じシャーシ内のモジュールの最小数（1 ～ 3）を指定します。デフォルトは 1 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。たとえば、値を 3 に設定した場合、各モジュールは最大遅延時間の間、または 3 つすべてのモジュールの準備が完了するまで待機してからクラスタに参加します。3つすべてのモジュールがほぼ同時にクラスタの参加を要求し、同時期にトラフィックの受信を開始します。
- [Maximum Join Delay]：最大遅延時間を分単位（0 ～ 30 分）で指定します。この時間が経過すると、モジュールは他のモジュールの準備が完了するのを待つことをやめて、クラスタに参加します。デフォルトは 0 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。最小単位を 1 に設定した場合、この値は 0 にする必要があります。最小単位を 2 または 3 に設定した場合、この値は 1 以上にする必要があります。このタイマーはモジュールごとのタイマーですが、最初のモジュールがクラスタに参加すると、その他すべてのモジュールのタイマーが終了し、残りのモジュールがクラスタに参加します。

たとえば、最小単位を 3、最大遅延を 5 分を設定します。モジュール 1 が起動すると、その 5 分間のタイマーが開始されます。モジュール 2 が 2 分後に起動すると、その 5 分間のタイマーが開始されます。モジュール 3 が 1 分後に起動し、すべてのモジュールが 4 分符号でクラスタに参加します。モジュールはタイマーが完了するまで待機しません。モジュール 3 が起動しない場合、モジュール 1 は 5 分間タイマーの終了時にクラスタに参加し、モジュール 2 も参加します。モジュール 2 はタイマーがまだ 2 分残っていますが、タイマーが完了するまで待機しません。

ステップ 6 [Apply] をクリックします。

インターフェイスのヘルス モニターリングおよび自動再結合の設定

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニターリングをディセーブルにすることができます。ポートチャネル ID、または単一の物理インターフェイス ID をモニターできます。ヘルス モニターリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニターリングは設定できません。このリンクは常にモニターされています。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Interface Health Monitoring]** の順に選択します。

ステップ 2 [Monitored Interfaces] ボックスでインターフェイスを選択し、[Add] をクリックしてそのインターフェイスを [Unmonitored Interfaces] ボックスに移動します。

インターフェイス ステータス メッセージによって、リンク障害が検出されます。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブ ポートがある場合、そのユニットはクラスタから削除されます。ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルス チェックはすべてのインターフェイスでイネーブルになっています。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニターリングをディセーブルにすることができます。ポートチャネル ID、または単一の物理インターフェイス ID を指定できます。ヘルス モニターリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニターリングは設定できません。このリンクは常にモニターされています。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 4100/9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし（**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**）、無効化したインターフェイスのモニターリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。

ステップ 3 インターフェイス、システム、またはクラスタ制御リンクに障害が発生した場合の自動再結合の設定をカスタマイズするには、[Auto Rejoin] タブをクリックします。各タイプに関して **[Edit]** をクリックして次の設定を行います。

- [Maximum Rejoin Attempts]：クラスタへの再結合の試行回数を定義するために、[Unlimited] または 0 ～ 65535 の範囲で値を設定します。**0** は自動再結合をディセーブルにします。デ

フォルト値は、クラスタ インターフェイスの場合は [Unlimited]、データ インターフェイスおよびシステムの場合は [3] です。

- [Rejoin Interval]：再結合試行間隔の時間を定義するために、2 ～ 60 の範囲で間隔を設定します。デフォルト値は**5**分です。クラスタへの再結合をユニットが試行する最大合計時間は、最後の失敗から 14,400 分に限られています。
- [Interval Variation]：1 ～ 3 の範囲で設定して、間隔を増加させるかどうかを定義します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタ インターフェイスの場合は [1]、データ インターフェイスおよびシステムの場合は [2] です。

デフォルト設定に戻すには、[Restore Defaults] をクリックします。

ステップ 4 [Apply] をクリックします。

クラスタ TCP 複製の遅延の設定

TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップフローが作成される前にユニットが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のユニットに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster Replication]**.の順に選択します。

ステップ 2 [Add] をクリックして次の値を設定します。

- [Replication delay]：1 ～ 15 の範囲で秒数を設定します。
- [HTTP]：すべての HTTP トラフィックの遅延を設定します。デフォルトでは、この設定は 5 秒間で有効化されています。
- **[Source Criteria]**
  - [Source]：送信元 IP アドレスを設定します。
  - [Service]：（オプション）送信元ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。
- **[Destination Criteria]**
  - [Source]：宛先 IP アドレスを設定します。

- [Service]：（オプション）宛先ポートを設定します。通常は、送信元または宛先ポートのいずれかを設定するか、両方ともに設定しません。

ステップ 3 [OK] をクリックします。

ステップ 4 [Apply] をクリックします。

サイト間機能の設定

サイト間クラスタリングの場合、冗長性と安定性を高めるために、設定をカスタマイズできます。

クラスタ フロー モビリティの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

LISP インスペクションについて

LISP トラフィックを検査することで、サイト間のフローのモビリティを有効にできます。

LISP について

VMware vMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンター サーバ モビリティをサポートするには、サーバの移動時にサーバへの入力ルートをルータが更新できる必要があります。Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID、つまりエンドポイント ID（EID）をその場所、つまりルーティング ロケータ（RLOC）から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

LISP では、LISP の出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、ファースト ホップ ルータ、マップ リゾルバ（MR）、およびマップ サーバ（MS）などのある一定のロールにおいてルータとサーバが必要です。サーバが別のルータに接続されていることをサーバのファースト ホップ ルータが感知すると、そのルータは他のすべてのルータとデータベースを更新し、クライアントに接続されている ITR がトラフィックを代行受信してカプセル化し、新しいサーバの場所に送信できるようにします。

ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISP の統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフロー オーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーニング」または「ヘアピニング」と呼ばれます。

LISP 統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR 間でやり取りされる LISP トラフィックを検査し、フローの所有者を新しいサイトに変更できます。

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。
- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々のノードに属しているフローは新しいオーナーには移動されません。半分散されたフローには SIP などのアプリケーションが含まれており、親フローとそのすべての子フローが同じ ASA によって所有されます。
- クラスタはレイヤ 3 および 4 のフロー状態を移動させるだけです。一部のアプリケーション データが失われる可能性があります。
- 短時間のフローまたはビジネスに不可欠でないフローの場合、オーナーの移動は有用でない可能性があります。インスペクションポリシーを設定するときに、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

ASA LISP の実装

この機能には、複数の相互に関係する設定が含まれています（それらについてはすべてこの章で説明します）。

1. （任意）ホストまたはサーバ IP アドレスに基づく検査対象 EID の制限：ファースト ホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。
2. LISP トラフィック インスペクション：ASA は、ファーストホップルータと ITR または ETR の間で送信される EID 通知メッセージにおいて、UDP ポート 4342 上の LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。LISP トラフィックにはディレクタが割り当てられておらず、LISP トラフィック自体はクラスタ状態の共有に参加しないことに注意してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。
4. サイト ID：ASA は、各クラスタノードのサイト ID を使用して新しいオーナーを特定します。

5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP インスペクションの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

始める前に

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。
- LISP のトラフィックはデフォルト インスペクション トラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

手順

ステップ 1 （任意） LISP インスペクション マップを設定して、IP アドレスに基づいて検査済みの EID を制限し、LISP の事前共有キーを設定します。

a) **[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[LISP]** を選択します。
b) [Add] をクリックして、新しいマップを追加します。
c) 名前（最大 40 文字）と説明を入力します。
d) **Allowed-EID access-list** については、[Manage] をクリックします。

[ACL Manager] が開きます。

ファースト ホップ ルータまたは ITR/ETR は、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信することがあります。このため、クラスタに関連するサーバーまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

e) ファイアウォールの設定ガイドに従って、少なくとも 1 つの ACE で ACL を追加します。
f) 必要に応じて、**検証キー**を入力します。

暗号化キーをコピーした場合は、[Encrypted]オプション ボタンをクリックします。

g) [OK] をクリックします。

ステップ 2 サービス ポリシー ルールを追加して LISP インスペクションを設定します。

a) **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** の順に選択します。
b) [Add] をクリックします。
c) [Service Policy] ページで、インターフェイスへのルールまたはグローバルなルールを適用します。

既存のサービス ポリシーで使用するものがあれば、そのポリシーにルールを追加します。デフォルトで、ASA には **global_policy** と呼ばれるグローバル ポリシーが含まれます。ポリシーをグローバルに適用しない場合は、インターフェイスごとに 1 つのサービス ポリシーを作成することもできます。LISP インスペクションは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービス ポリシーを適用する必要はありません。トラフィックが両方向のクラスに一致する場合、ルールを適用するインターフェイスに出入りするトラフィックのすべてが影響を受けます。

d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)]をオンにします。
e) [Next] をクリックします。
f) インスペクションを行うトラフィックを指定します。ファースト ホップ ルータと UDP ポート 4342 の ITR または ETR の間のトラフィックを指定します。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
g) [Next] をクリックします。
h) [Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。
i) [LISP] チェックボックスをオンにします。
j) （オプション）[Configure] をクリックして、作成したインスペクション マップを選択します。
k) [Finish] をクリックして、サービス ポリシー ルールを保存します。

ステップ 3 サービス ポリシー ルールを追加して、重要なトラフィックのフロー モビリティを有効化します。

a) **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** の順に選択します。
b) [Add] をクリックします。
c) [Service Policy] ページで、LISP インスペクションに使用する同じサービス ポリシーを選択します。
d) [Traffic Classification Criteria] ページで、[Create a new traffic class] をクリックし、[Traffic Match Criteria] の下部の [Source and Destination IP Address (uses ACL)]をオンにします。
e) [Next] をクリックします。
f) サーバーがサイトを変更するときに最適なサイトに再割り当てする、ビジネス クリティカルなトラフィックを指定します。たとえば、フロー モビリティを HTTPS トラフィックおよび/または特定のサーバーへのトラフィックのみに制限できます。IPv4 ACL および IPv6 ACL のどちらにも対応しています。
g) [Next] をクリックします。
h) [Rule Actions] ウィザード ページまたはタブで、[Cluster] タブを選択します。
i) [Enable Cluster flow-mobility triggered by LISP EID messages] チェックボックスをオンにします。
j) [Finish] をクリックして、サービス ポリシー ルールを保存します。

ステップ 4 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** の順に選択し、**[Enable Clustering flow mobility]** チェックボックスをオンにします。

ステップ 5 [適用（Apply）] をクリックします。

分散型サイト間 VPN の設定

デフォルトでは、ASA クラスタは集中型サイト間 VPN モードを使用します。クラスタリングの拡張性を活用するために、分散型サイト間VPNモードを有効にできます。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

分散型サイト間 VPN について

分散型 VPN 接続の役割

分散型 VPN モードで実行すると、次の役割がクラスタ メンバーに割り当てられます。

- アクティブ セッション オーナー：最初に接続を受信したユニット、またはバックアップ セッションをアクティブ セッションに移行したユニット。オーナーは、IKE と IPsec トンネル、およびそれらに関連付けられたすべてのトラフィックを含む、完全なセッションの状態を維持し、パケットを処理します。
- バックアップ セッション オーナー：既存のアクティブ セッションのバックアップ セッションを処理しているユニット。選択されたバックアップ戦略によっては、アクティブ セッション オーナーと同じシャーシ内のユニット、または別のシャーシ内のユニットである可能性があります。アクティブ セッション オーナーに障害が発生すると、バックアップ セッション オーナーがアクティブ セッション オーナーになり、新しいバックアップ セッションが別のユニットで確立されます。
- フォワーダ：VPN セッションに関連付けられたトラフィックが VPN セッションを所有していないユニットに送信された場合、そのユニットは VPN セッションを所有しているメンバーにトラフィックを転送するために Cluster Control Link（CCL）を使用します。
- オーケストレータ：オーケストレータ（常にクラスタの制御ユニット）は、アクティブ セッションの再配布（ASR）を実行する際に、移動するセッションとその移動先を計算する役割があります。オーケストレータは、オーナー メンバーXにNセッションをメンバーYに移動する要求を送信します。メンバーXは、完了時に移動できたセッション数を指定して、オーケストレータに応答を返します。

分散型 VPN セッションの特性

分散型 S2S VPN セッションには、次の特性があります。それ以外の場合、VPN 接続は、ASA クラスタ上にない場合に通常動作するように動作します。

- VPN セッションは、セッション レベルでクラスタ全体に分散されます。つまり、1 つの VPN 接続に対し、同じクラスタ メンバーが IKE および IPsec トンネルと、そのすべてのトラフィックを処理します。VPN セッション トラフィックが、その VPN セッションを所

有していないクラスタ メンバーに送信された場合、トラフィックは VPN セッションを所有しているクラスタ メンバーに転送されます。

- VPN セッションには、クラスタ全体で一意のセッション ID があります。セッション ID を使用して、トラフィックが検証され、転送の決定が行われ、IKE ネゴシエーションが完了します。
- S2S VPN ハブ アンド スポーク構成では、クライアントが ASA クラスタを介して接続する場合（ヘアピニングと呼ばれる）、流入するセッション トラフィックと流出するセッション トラフィックは、異なるクラスタ メンバー上にある可能性があります。
- バックアップ セッションを別のシャーシのセキュリティ モジュールに割り当てるように要求することができます。これにより、シャーシの障害を防止します。または、クラスタ内の任意のノードにバックアップセッションを割り当てることもできます。これはノードの障害のみを防止します。クラスタにシャーシが 2 つある場合は、リモートシャーシバックアップを強く推奨します。
- 分散型 S2S VPN モードでは IKEv2 IPsec S2S VPN のみがサポートされ、IKEv1 はサポートされていません。IKEv1 S2S は、集中型 VPN モードでサポートされています。
- 各セキュリティ モジュールは、6 つのメンバーにわたる最大約 36,000 のセッションに対し、最大 6,000 の VPN セッションをサポートします。クラスタ メンバーでサポートされる実際のセッション数は、プラットフォームの容量、割り当てられたライセンス、コンテキストごとのリソース割り当てによって決まります。使用率が制限値に近い場合、各クラスタユニットで最大容量に達していなくても、セッションの作成が失敗することがあります。これは、アクティブ セッションの割り当てが外部スイッチングによって決定され、バックアップ セッションの割り当てが内部クラスタ アルゴリズムによって決定されるためです。顧客は、使用率を適宜調整し、不均一な配布に対するスペースを確保することが推奨されます。

クラスタ イベントの分散型 VPN の処理

表 *23：*

イベント	分散型 VPN
メンバーの障害	この障害が発生したメンバー上のすべてのアクティブセッションに対し、（別のメンバー上の）バックアップセッションがアクティブになり、バックアップセッションはバックアップ戦略に従って別のユニットに再割り当てされます。

イベント	分散型 VPN
シャーシ障害	リモートシャーシバックアップ戦略が使用されている場合、障害が発生したシャーシ上のすべてのアクティブセッションに対し、（他のシャーシのメンバー上の）バックアップセッションがアクティブになります。ユニットが交換されると、これらの現在アクティブなセッションに対するバックアップセッションが、交換されたシャーシのメンバーに再割り当てされます。 フラット バックアップ戦略が使用されている場合、アクティブ セッションとバックアップ セッションの両方が障害の発生したシャーシ上にあると、接続は切断されます。他のシャーシのメンバー上にバックアップセッションがあるアクティブセッションはすべて、これらのセッションにフォールバックします。新しいバックアップセッションは、残存しているシャーシ内の別のメンバーに割り当てられます。
クラスタ メンバーの非アクティブ化	非アクティブになっているクラスタ メンバー上のすべてのアクティブセッションに対し、（別のメンバー上の）バックアップセッションがアクティブになり、バックアップ戦略に従って別のユニットにバックアップ セッションを再割り当てします。
クラスタ メンバーの参加	VPN クラスタモードが分散型に設定されていない場合、制御ユニットはモード変更を要求します。 VPN モードに互換性がある場合、または以前互換性があった場合、クラスタ メンバーには、通常の操作の流れでアクティブセッションとバックアップ セッションが割り当てられます。

サポートされていないインスペクション

次のタイプの検査は、分散型 S2S VPN モードではサポートされていないか、または無効になっています。

- CTIQBE
- DCERPC
- H323、H225、および RAS
- IPSec パススルー
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH

- RTSP
- SCCP（Skinny）
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

IPsec IKEv2 の変更

IKEv2 は、分散型 S2S VPN モードでは次のように変更されます。

- IP/ポート タプルの代わりに ID が使用されます。これにより、パケットの適切な転送の決定、および他のクラスタ メンバー上にある可能性がある以前の接続のクリーンアップが可能になります。
- 単一の IKEv2 セッションを識別する（SPI）識別子は、ローカルで生成されたランダムな 8 バイトの値で、クラスタ全体で一意です。SPI には、タイム スタンプとクラスタ メンバー ID が埋め込まれています。IKE ネゴシエーション パケットの受信時に、タイム スタンプまたはクラスタ メンバー ID のチェックに失敗すると、パケットがドロップされ、理由を示すメッセージが記録されます。
- NAT-T ネゴシエーションがクラスタ メンバー間で分割されることによって失敗しないように IKEv2 処理が変更されました。新しい ASP 分類ドメインである *cluster_isakmp_redirect*、およびルールは、IKEv2 がインターフェイスで有効になっている場合に追加されます。

サポート モデル

分散型 VPN でサポートされる唯一のデバイスは、Firepower 9300 です。分散型 VPN では、最大 2 シャーシで、最大 6 モジュールをサポートしています。各シャーシで異なる数のセキュリティ モジュールを設置することができますが、均等な分配を推奨しています。

サイト間クラスタリングはサポートされていません。

ファイアウォール モード

分散型 S2S VPN は、ルーテッド モードでのみサポートされています。

コンテキスト モード

分散型 S2S VPN は、シングル コンテキスト モードおよびマルチ コンテキスト モードの両方で動作します。ただし、マルチ コンテキスト モードでは、アクティブ セッションの再配布はコンテキスト レベルではなくシステム レベルで行われます。これにより、コンテキストに関連付けられたアクティブセッションが、異なるコンテキストに関連付けられたアクティブセッションを含むクラスタ メンバーに移動し、予期せずに持続不可能な負荷が発生するのを防ぎます。

ハイ アベイラビリティ

次の機能により、セキュリティモジュールまたはシャーシの単一障害に対する復元力が提供されます。

- 任意のシャーシ上のクラスタ内にある別のセキュリティモジュールにバックアップされたVPN セッションは、セキュリティ モジュールの障害に耐性があります。
- 別のシャーシにバックアップされた VPN セッションは、シャーシの障害に耐性があります。
- 制御ユニットは、VPN S2S セッションを失うことなく変更できます。

クラスタが安定する前に追加の障害が発生すると、アクティブセッションとバックアップセッションの両方が障害の発生したユニットにある場合、接続が失われる可能性があります。

VPN クラスタ モードの無効化、クラスタ メンバーのリロード、およびその他の予想されるシャーシの変更など、メンバーが正常な状態でクラスタを離れるときにセッションが失われないように、すべての試行が行われます。これらのタイプの操作では、操作間でセッションのバックアップを再確立する時間がクラスタに与えられている限り、セッションは失われません。最後のクラスタ メンバーで正常な終了がトリガーされた場合、既存のセッションが正常に切断されます。

ダイナミック PAT

分散型 VPN モードでは使用できません。

CMPv2

CMPv2 ID 証明書とキーペアはクラスタ メンバー間で同期されます。ただし、クラスタ内の制御ユニットのみが CMPv2 証明書を自動的に更新してキーの再生成を行います。制御ユニットは更新時に、これらの新しい ID 証明書とキーをすべてのクラスタメンバーに同期させます。このようにして、クラスタ内のすべてのメンバーは CMPv2 証明書を利用して認証を行い、また、すべてのメンバーが制御ユニットを継承することができます。

分散型 S2S VPN の有効化

分散型サイト間VPNを有効にして、VPNセッションのクラスタリングの拡張性を活用します。

（注） VPNモードを集中型と分散型の間で変更すると、既存のすべてのセッションが切断されます。バックアップ モードの変更は動的で、セッションは終了しません。

始める前に

- クラスタのすべてのメンバーにキャリア ライセンスが設定されている必要があります。
- S2S VPN 設定を行う必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] の順に選択します。

ステップ 2 [VPN Cluster Mode] 領域で、クラスタの [VPN Mode] を [Centralized] または [Distributed] から選択します。

ステップ 3 [Backup Distribution Mode] を [Flat] または [Remote-chassis] から選択します。

フラット バックアップ モードでは、他のクラスタ メンバーにスタンバイ セッションが確立されます。これにより、ユーザーはブレード障害から保護されますが、シャーシ障害の保護は保証されません。

リモートシャーシ バックアップ モードでは、クラスタ内の別のシャーシのメンバーにスタンバイ セッションが確立されます。これにより、ユーザーはブレード障害とシャーシ障害の両方から保護されます。

リモートシャーシが単一のシャーシ環境（意図的に構成されたものまたは障害の結果）で構成されている場合、別のシャーシが結合されるまでバックアップは作成されません。

分散型 S2S VPN セッションの再配布

アクティブ セッションの再配布（ASR）では、アクティブな VPN セッションの負荷がクラスタ メンバー全体に再配布されます。セッションの開始と終了の動的な性質のため、ASR は、すべてのクラスタ メンバー間でセッションのバランスを取るためのベスト エフォートです。繰り返される再配布アクションによってバランスが最適化されます。

再配布はいつでも実行でき、クラスタ内のトポロジ変更後に実行する必要があります。また、新しいメンバーがクラスタに参加した後に実行することを推奨します。再配布の目的は、安定した VPN クラスタを作成することです。安定した VPN クラスタには、ノード間でほぼ同数のアクティブ セッションとバックアップ セッションがあります。

セッションを移動するには、バックアップ セッションがアクティブ セッションになり、別のノードが新しいバックアップ セッションをホストするように選択されます。移動セッションは、アクティブ セッションのバックアップの場所と、その特定のバックアップ ノード上にすでに存在するアクティブセッションの数に依存します。何らかの理由でバックアップセッション ノードがアクティブセッションをホストできない場合、元のノードはセッションのオーナーのままです。

マルチコンテキスト モードでは、アクティブ セッションの再配布は、個々のコンテキスト レベルではなくシステム レベルで行われます。コンテキスト レベルで実行されない理由は、あるコンテキスト内のアクティブセッションが別のコンテキスト内のより多くのアクティブセッションを含むメンバーに移動され、そのクラスタ メンバーに多くの負荷がかかるためです。

始める前に

- 再配布アクティビティをモニターする場合は、システム ログを有効にします。

- この手順は、クラスタの制御ユニットで実行する必要があります。

手順

ステップ 1 [Monitoring] > [ASA Cluster] > [ASA Cluster] > [Cluster Summary] > [VPN Cluster Summary] を選択して、アクティブ セッションとバックアップ セッションがクラスタ全体にどのように配布されているかを表示します。

再配布するセッションの数とクラスタの負荷に応じて、これには時間がかかることがあります。再配布アクティビティが発生すると、次のフレーズ（およびここには表示されていない他のシステムの詳細）を含む Syslog が提供されます。

Syslog フレーズ	注
VPN session redistribution started	制御ユニットのみ
Sent request to move *number* sessions from *orig-member-name* to *dest-member-name*	制御ユニットのみ
Failed to send session redistribution message to *member-name*	制御ユニットのみ
Received request to move *number* sessions from *orig-member-name* to *dest-member-name*	データユニットのみ
Moved *number* sessions to *member-name*	名前付きクラスタに移動したアクティブ セッションの数。
Failed to receive session move response from *dest-member-name*	制御ユニットのみ
VPN session completed	制御ユニットのみ
Cluster topology change detected. VPN session redistribution aborted.	

ステップ 2 [Re-Distribute] をクリックします。

ステップ 3 [Monitoring] > [ASA Cluster] > [ASA Cluster] > [ClusterSummary] > [VPN Cluster Summary] を更新して、再配布アクティビティの結果を確認します。

再配布が成功し、実質的なシステムまたはセッションアクティビティがなかった場合、システムのバランスが取られ、このアクションは完了します。

それ以外の場合は、再配布プロセスを繰り返して、バランスの取れた安定したシステムを取得します。

FXOS：クラスタユニットの削除

ここでは、ユニットをクラスタから一時的に、または永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタユニットはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、Firepower Chassis Manager の [Logical Devices] ページで、のクラスタ ステータスを確認します。

- アプリケーションでのクラスタリングの無効化：アプリケーションCLIを使用してクラスタリングを無効にすることができます。**cluster remove unit** *name* コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、制御ユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。制御ユニットを削除するためにデータユニットでこのコマンドを入力した場合は、新しい制御ユニットが選定されます。

  デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。

  クラスタリングを再度有効にするには、ASA で **cluster group** *name* を入力してから **enable** を入力します。

- アプリケーション インスタンスの無効化：Firepower Chassis Manager の [Logical Devices] ページで **有効なスライダ**（  ）をクリックします。**無効なスライダ**（  ）を使用して後で再度有効にすることができます。
- セキュリティ モジュール/エンジン のシャットダウン：Firepower Chassis Manager の [セキュリティモジュール/エンジン（Security Module/Engine）] ページで、**電源オフアイコン**をクリックします。
- シャーシのシャットダウン：Firepower Chassis Manager の [概要（Overview）] ページで、**シャットダウンアイコン**をクリックします。

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

- 論理デバイスの削除：Firepower Chassis Manager の [Logical Devices] ページで、 をクリックします。その後、スタンドアロンの論理デバイスや新しいクラスタを展開したり、同じクラスタに新しい論理デバイスを追加したりすることもできます。
- サービスからのシャーシまたはセキュリティ モジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

ASA：クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのノード上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェック エラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのノードをクラスタから完全に削除します。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタ設定（Cluster Members）]** の順に選択します。

ステップ 2 [Participate in ASA cluster] チェックボックスをオフにします。

（注） [Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソール ポートで CLI にアクセスする必要があります。

ステップ 3 [Apply] をクリックします。

制御ユニットからのデータユニットの非アクティブ化

データノードを非アクティブにするには、次の手順を実行します。

（注） ASA が非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）]** の順に選択します。

ステップ 2 削除するデータノードを選択して [削除（Delete）] をクリックします。

データノードのブートストラップコンフィギュレーションは同じであり、その設定を失うことなく以後データノードを再追加できます。

ステップ 3 [適用（Apply）] をクリックします。

クラスタへの再参加

ノードがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。ただし、ASDM でクラスタリングを手動で無効にした場合、設定を保存してリロードしなかった場合は、ASDM でクラスタリングを再び有効にできます。リロード後、管理インターフェイスは無効になるため、コンソール アクセスがクラスタリングを再び有効にする唯一の方法です。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 ASDM にまだアクセスしている場合は、再イネーブル化するノードに ASDM を接続して、ASDM でクラスタリングを再び有効にすることができます。

新しいメンバーとして追加していない限り、データノードのクラスタリングを制御ノードから再び有効にすることはできません。

a) **[構成（Configuration）] > [デバイス管理（Device Management）] > [高可用性とスケーラビリティ（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）]** の順に選択します。

b) [Participate in ASA cluster] チェックボックスをオンにします。

c) [Apply] をクリックします。

ステップ 2 ASDM を使用できない場合：コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 3 クラスタリングをイネーブルにします。

enable

制御ユニットの変更

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 [Monitoring] > [ASA Cluster] > [Cluster Summary] を選択します。

ステップ 2 ドロップダウンリストから制御ノードにするデータノードを選択し、制御ノードにするボタンをクリックします。

ステップ 3 制御ノードの変更を確認するように求められます。[Yes] をクリックします。

ステップ 4 ASDM を終了し、メイン クラスタ IP アドレスを使用して再接続します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。（または、制御ユニットで show コマンドを入力するとクラスタ全体の統計情報を表示できます。）**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

始める前に

コマンドライン インターフェイス ツールでこの手順を実行します。**[Tools]** > **[Command Line Interface]** を選択します。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit *unit_name*] コマンド

例：

```
cluster exec show xlate
```

メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

例

同じキャプチャファイルをクラスタ内のすべてのユニットから同時に TFTP サーバーにコピーするには、制御ユニットで次のコマンドを入力します。

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバーにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタ ユニット名です。

次の **cluster exec show memory** コマンドの出力例では、クラスタの各メンバーのメモリ情報が表示されています。

```
cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
```

```
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:**********************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:**********************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA：での ASA クラスタのモニターリング Firepower 4100/9300 シャーシ

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニターリング

クラスタの状態のモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [Cluster Summary]**

  このペインには、接続相手のユニットとクラスタのその他のユニットの情報が表示されます。また、このペインでプライマリ装置を変更することができます。

- **[Cluster Dashboard]**

  プライマリ装置のホーム ページの [Cluster Dashboard] と [Cluster Firewall Dashboard] を使用してクラスタをモニターできます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次の画面を参照してください。

[Wizards] > [Packet Capture Wizard]

クラスタ全体のトラブルシューティングをサポートするには、制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

クラスタリソースのモニタリング

クラスタ リソースのモニタリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [System Resources Graphs] > [CPU]**

  このペインでは、クラスタ メンバ全体の CPU 使用率を示すグラフまたはテーブルを作成することができます。

- [Monitoring] > [ASA Cluster] > [System Resources Graphs] > [Memory]。

  このペインでは、クラスタ メンバ全体の [Free Memory] と [Used Memory] を表示するグラフまたはテーブルを作成することができます。

クラスタ トラフィックのモニターリング

クラスタ トラフィックのモニターリングについては、次の画面を参照してください。

- [Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Connections]。

  このペインでは、クラスタ メンバ全体の接続を示すグラフまたはテーブルを作成することができます。

- [Monitoring] > [ASA Cluster] > [Traffic] > [Graphs] > [Throughput]。

  このペインでは、クラスタ メンバ全体のトラフィックのスループットを示すグラフまたはテーブルを作成することができます。

- **[Monitoring] > [ASA Cluster] > [Cluster Load-Monitoring]**

  ここでは、[Load Monitor-Information] ペインと [Load-Monitor Details] ペインについて説明します。**ロードモニター情報**には、最後のインターバルのクラスタメンバのトラフィック負荷、および設定された間隔の合計数の平均（デフォルトでは30）が表示されます。各間隔の各測定値を表示するには、[Load-Monitor Details] ペインを使用します。

クラスタ制御リンクのモニターリング

クラスタの状態のモニターリングについては、次の画面を参照してください。

[Monitoring] > [Properties] > [System Resources Graphs] > [Cluster Control Link]。

このペインでは、クラスタ制御リンクの [Receival] および [Transmittal] 容量使用率を表示するグラフまたはテーブルを作成することができます。

クラスタのルーティングのモニターリング

クラスタのルーティングについては、次の画面を参照してください。

- **[Monitoring] > [Routing] > [LISP-EID Table]**

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

分散型 S2S VPN のモニターリング

VPN クラスタ ステータスのモニターリングについては、次の画面を参照してください。

- **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [Cluster Summary] > [VPN Cluster Summary]**

  クラスタ全体のセッションの分布を表示し、セッションを再配布する機能を提供します。

- **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]**

  クラスタの制御ユニットとデータユニットの両方が表示されます。詳細については、任意のメンバーをクリックしてください。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次の画面を参照してください。

[Configuration] > [Device Management] > [Logging] > [Syslog Setup]

クラスタ内の各ノードは、syslog メッセージを個別に生成します。同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

分散型 S2S VPN のトラブルシューティング

分散型 VPN の通知

分散型 VPN を実行しているクラスタで、次のエラー状況が発生した場合、識別されたフレーズを含むメッセージが通知されます。

状況	通知

クラスタに参加しようとしているときに、既存のまたは参加しているクラスタデータユニットが分散型 VPN モードにない場合は、次のメッセージが通知されます。	`New cluster member (member-name) rejected due to vpn mode mismatch.`
	および
	`Master (control-name) rejects enrollment request from unit (unit-name) for the reason: the vpn mode capabilities are not compatible with the master configuration`

分散型VPNのクラスタ メンバーでライセンスが正しく設定されていない場合は、次のメッセージが通知されます。	`ERROR: Master requested cluster vpn-mode change to distributed. Unable to change mode due to missing Carrier License.`

受信した IKEv2 パケットの SPI でタイム スタンプまたはメンバー ID が無効な場合は、次のメッセージが通知されます。	`Expired SPI received`
	または
	`Corrupted SPI detected`

状況	通知
クラスタがバックアップ セッションを作成できない場合は、次のメッセージが通知されます。	`Failed to create the backup for an IKEv2 session.`
IKEv2 初期接点（IC）処理エラーの場合は、次のメッセージが通知されます。	`IKEv2 Negotiation aborted due to ERROR: Stale backup session found on backup`
再配布の問題の場合は、次のメッセージが通知されます。	`Failed to send session redistribution message to` *`member-name`* `Failed to receive session move response from` *`member-name`* `(master only)`
セッションの再配布中にトポロジが変更された場合は、次のメッセージが通知されます。	`Cluster topology change detected. VPN session redistribution aborted.`

次のいずれかの状況が発生している可能性があります。

- **port-channel load-balance src-dst l4port**コマンドを使用して N7K スイッチにロード バランシング アルゴリズムとして L4port が設定されている場合、L2L VPN セッションはクラスタ内のシャーシの 1 つにのみ配布されます。. クラスタ セッションの割り当ての例を次に示します。

```
SSP-Cluster/slave(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
 5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
 5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
 5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

L2L IKEv2 VPN は送信元ポートと宛先ポートの両方にポート 500 を使用するため、IKE パケットは N7K とシャーシ間に接続されたポート チャネル内のリンクの 1 つにのみ送信されます。

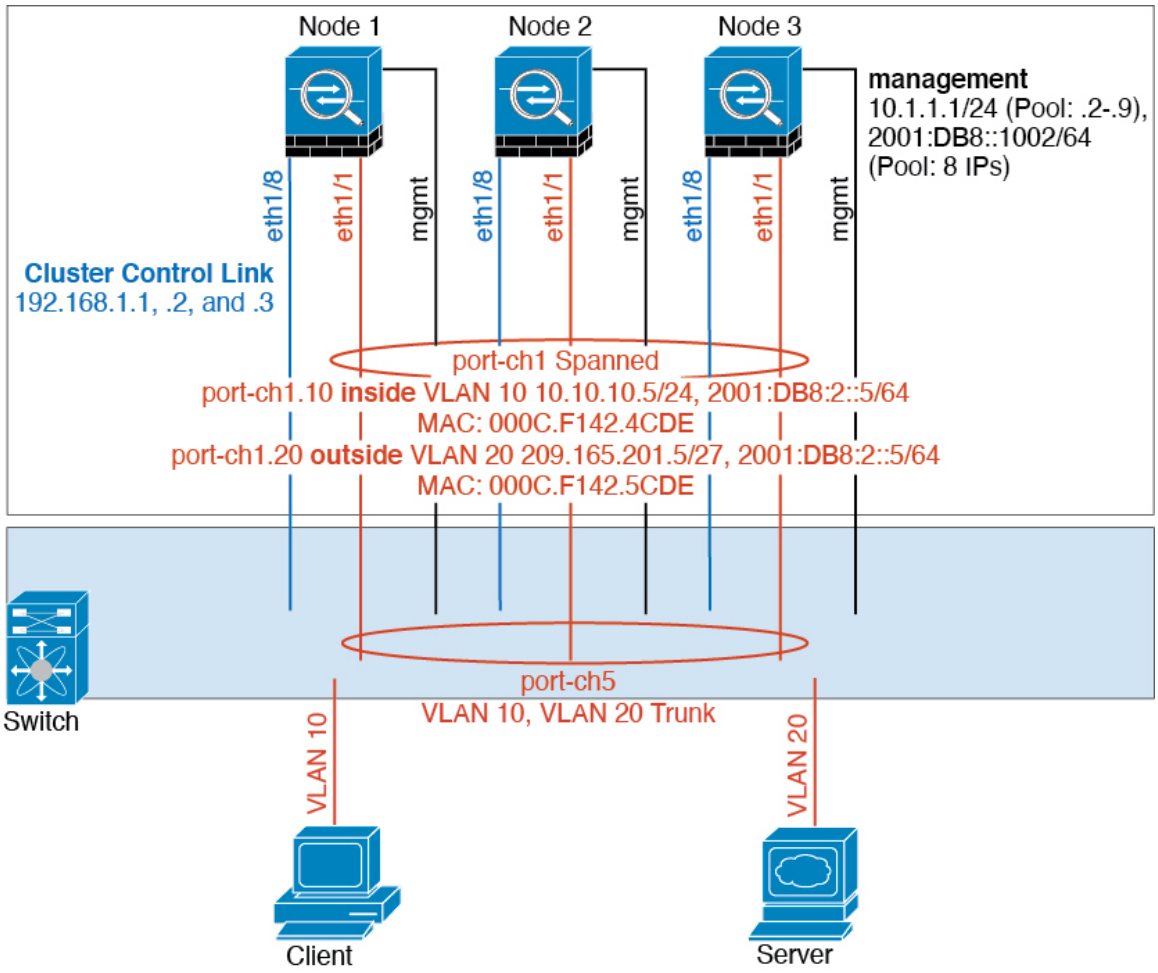
port-channel load-balance src-dst ip-l4port を使用して、N7K ロード バランシング アルゴリズムを IP および L4 ポートに変更します。その後、IKE パケットはすべてのリンクに送信されるので、両方の Firepower9300 シャーシに送信されます。

より即座に調整するには、ASA クラスタの制御ユニットで **cluster redistribute vpn-sessiondb** を実行することで、アクティブな VPN セッションを他のシャーシのクラスタメンバーに再配布できます。

ASA クラスタリングの例

これらの例には、一般的な導入が含まれます。

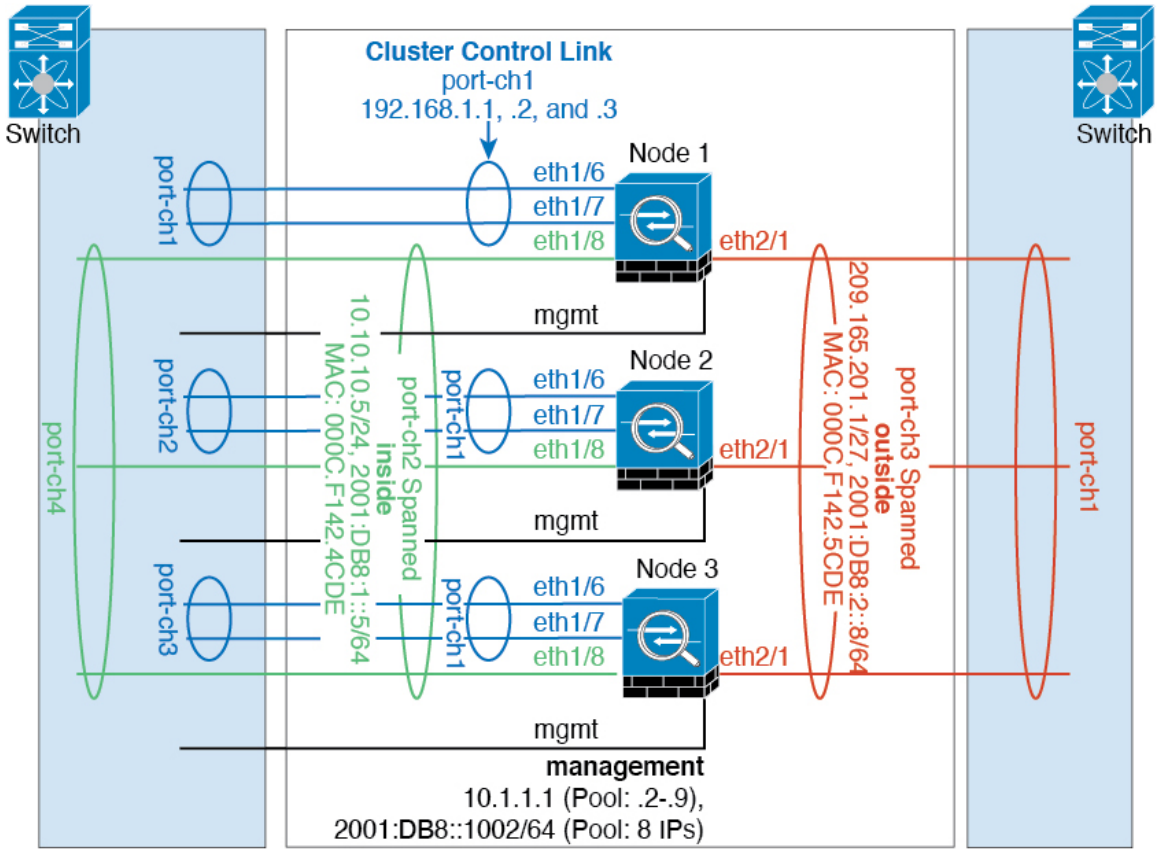
スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。ASA が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

トラフィックの分離



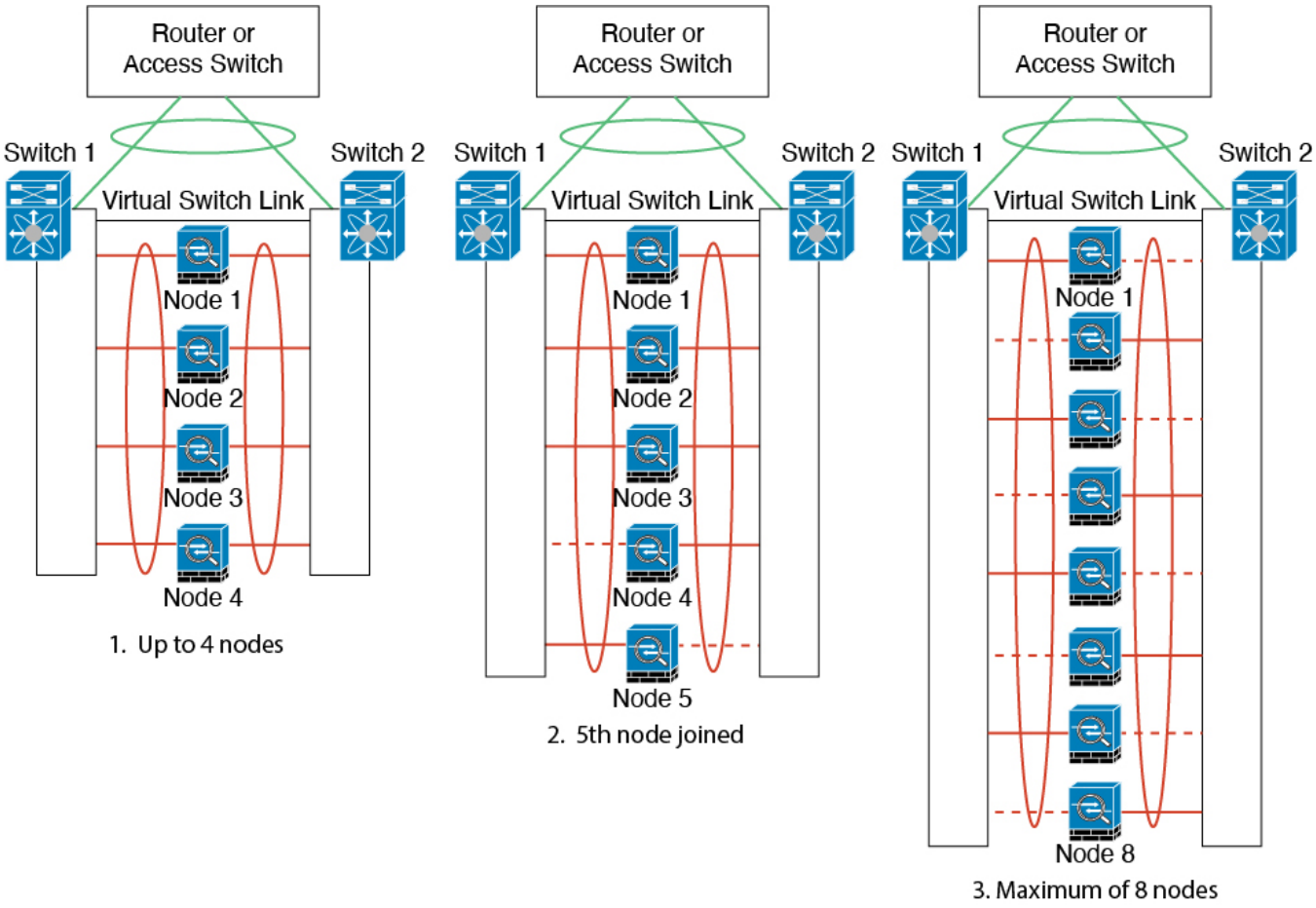
内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

スパンドEtherChannelとバックアップ リンク（従来の8アクティブ/8スタンバイ）

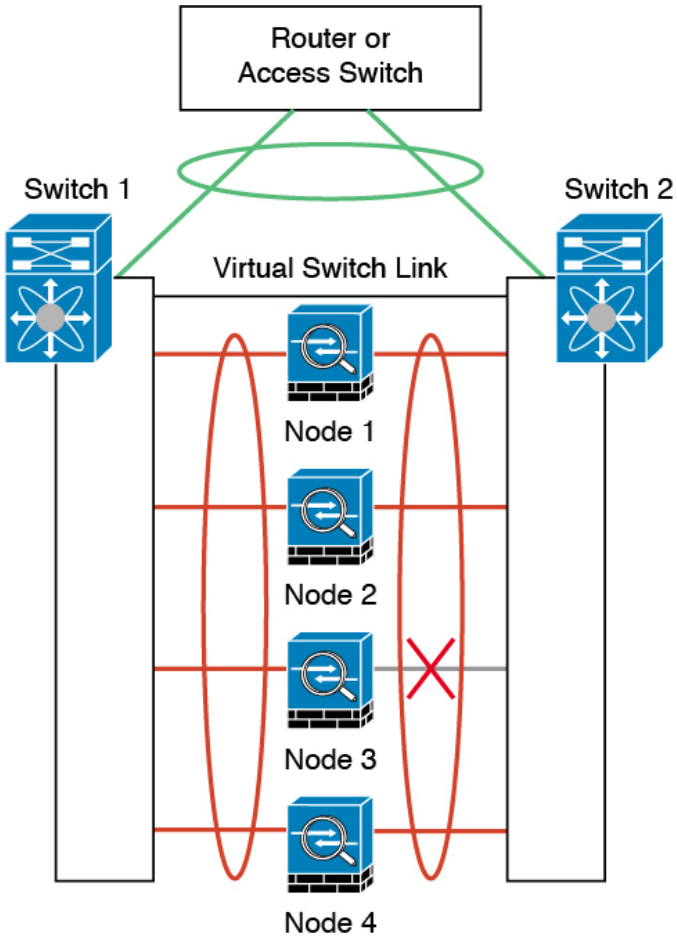
従来のEtherChannelのアクティブ ポートの最大数は、スイッチ側からの8に制限されます。8ユニットから成るクラスタがあり、EtherChannelにユニットあたり2ポートを割り当てた場合は、合計16ポートのうち8ポートをスタンバイ モードにする必要があります。ASAは、どのリンクをアクティブまたはスタンバイにするかを、LACPを使用してネゴシエートします。VSSまたはvPCを使用してマルチスイッチEtherChannelをイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASAでは、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「制御」ポートとなり（たとえばEthernet 1/1）、他方が「データ」ポートとなります（たとえばEthernet 1/2）。ハードウェア接続の対称性を保証する必要があります。つまり、すべての制御リンクは1台のスイッチが終端

となり、すべてのデータリンクは別のスイッチが終端となっている必要があります（VSS/vPC が使用されている場合）。次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。

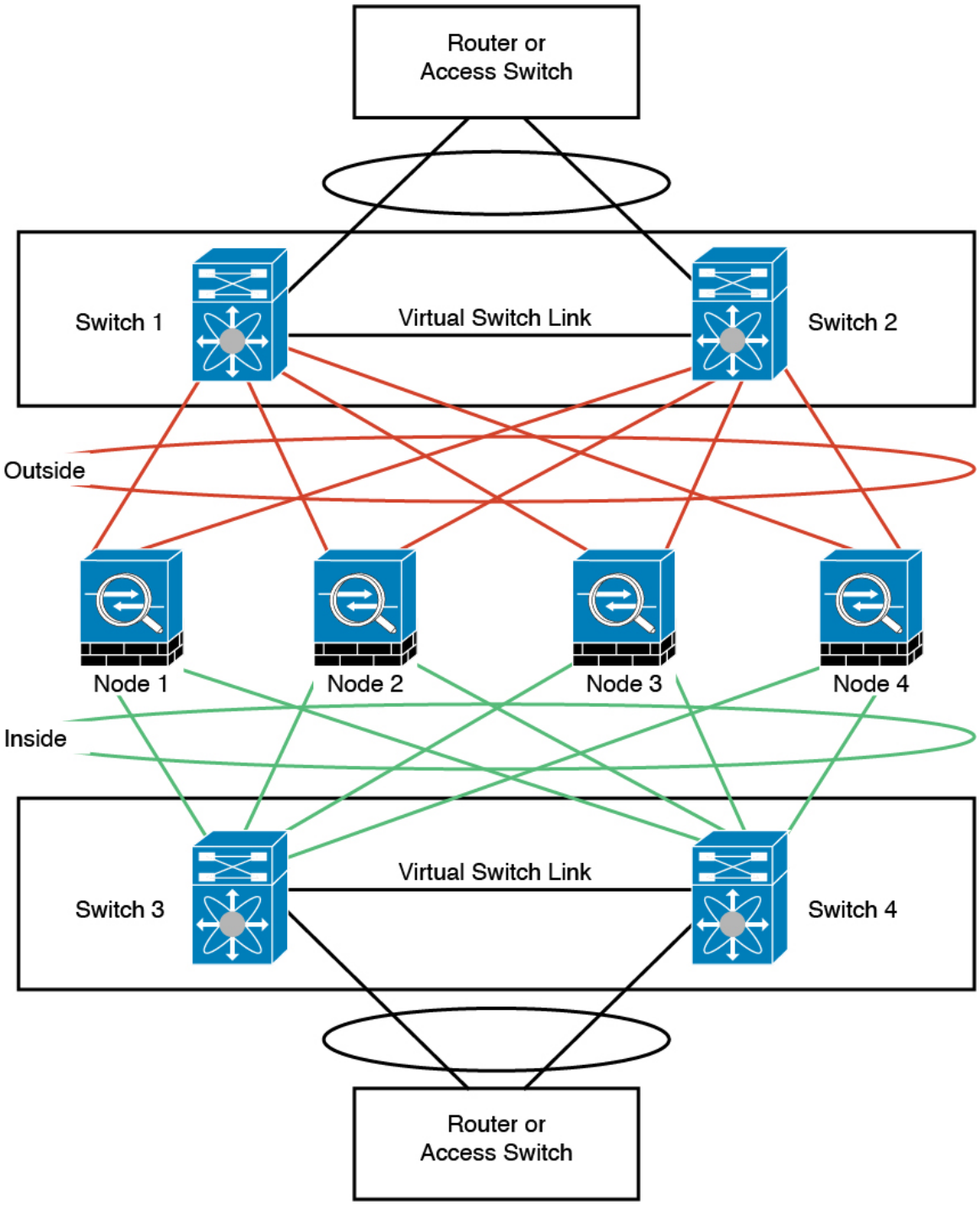


原則として、初めにチャネル内のアクティブポート数を最大化し、そのうえで、アクティブな制御ポートとアクティブなデータポートの数のバランスを保ちます。5 番目のユニットがクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

リンクまたはデバイスの障害が発生したときも、同じ原則で処理されます。その結果、ロードバランシングが理想的な状態にはならないこともあります。次の図は、4 ユニットのクラスタを示しています。このユニットの 1 つで、単一リンク障害が発生しています。



ネットワーク内に複数の EtherChannel を設定することも考えられます。次の図では、EtherChannel が内部に 1 つ、外部に 1 つあります。ASA は、一方の EtherChannel で制御とデータの両方のリンクが障害状態になった場合にクラスタから削除されます。これは、その ASA がすでに内部ネットワークへの接続を失っているにもかかわらず、外部ネットワークからトラフィックを受信するのを防ぐためです。



ルーテッド モード サイト間クラスタリングの OTV 設定

スパンド EtherChannel を使用したルーテッド モードに対するサイト間クラスタリングの成功は、OTV の適切な設定とモニタリングによって異なります。OTV は、DCI 全体にパケットを

転送することで、重要な役割を果たします。OTVは、転送テーブルにMACアドレスを学習するときにのみ、DCI 全体にユニキャスト パケットを転送します。MAC アドレスが OTV 転送テーブルに学習されていない場合、ユニキャスト パケットはドロップされます。

OTV 設定の例

```
//Sample OTV config:
//3151 – Inside VLAN, 3152 – Outside VLAN, 202 – CCL VLAN
//aaaa.1111.1234 – ASA inside interface global vMAC
//0050.56A8.3D22 – Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
```

```
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

サイト障害のために必要な OTV フィルタの変更

サイトがダウンした場合は、グローバル MAC アドレスをそれ以上ブロックしなくて済むように、フィルタを OTV から削除する必要があります。必要ないくつかの追加設定があります。

機能しているサイトで OTV スイッチ上の ASA グローバル MAC アドレスに対するスタティック エントリを追加する必要があります。このエントリによって、反対側の OTV はオーバーレイ インターフェイスにこれらのエントリを追加できます。サーバとクライアントに ASA 用の ARP エントリがすでにある場合（これは既存の接続の場合です）、ARP は再送信されないので、この手順が必要になります。したがって、OTV は転送テーブルに ASA グローバル MAC アドレスを学習する機会はありません。OTV には転送テーブル内にグローバル MAC アドレスがなく、OTV の設計ごとに OTV はオーバーレイ インターフェイスを介してユニキャスト パケットをフラッディングしないので、ユニキャスト パケットはサーバからのグローバル MAC アドレスにドロップされ、既存の接続は切断されます。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

他のサイトが復元した場合は、フィルタを再度追加して、OTV でこのスタティック エントリを削除する必要があります。グローバル MAC アドレスのオーバーレイ エントリをクリアするには、両方の OTV でダイナミック MAC アドレス テーブルをクリアすることが非常に重要です。

MAC アドレス テーブルのクリア

サイトがダウンし、グローバル MAC アドレスへのスタティック エントリが OTV に追加される場合は、他の OTV がオーバーレイ インターフェイスのグローバル MAC アドレスを学習できるようにする必要があります。他のサイトが起動したら、これらのエントリをクリアする必要があります。OTV の転送テーブルにこれらのエントリがないことを確認するために、MAC アドレス テーブルを必ず消去してください。

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP キャッシュのモニタリング

OTV は、OTV インターフェイス全体で学習した IP アドレスに対するプロキシ ARP への ARP キャッシュを維持します。

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド EtherChannel ルーテッド モードの例

次の例では、各サイトのゲートウェイ ルータと内部ネットワーク間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部両方のネットワークに対しスパンド EtherChannel

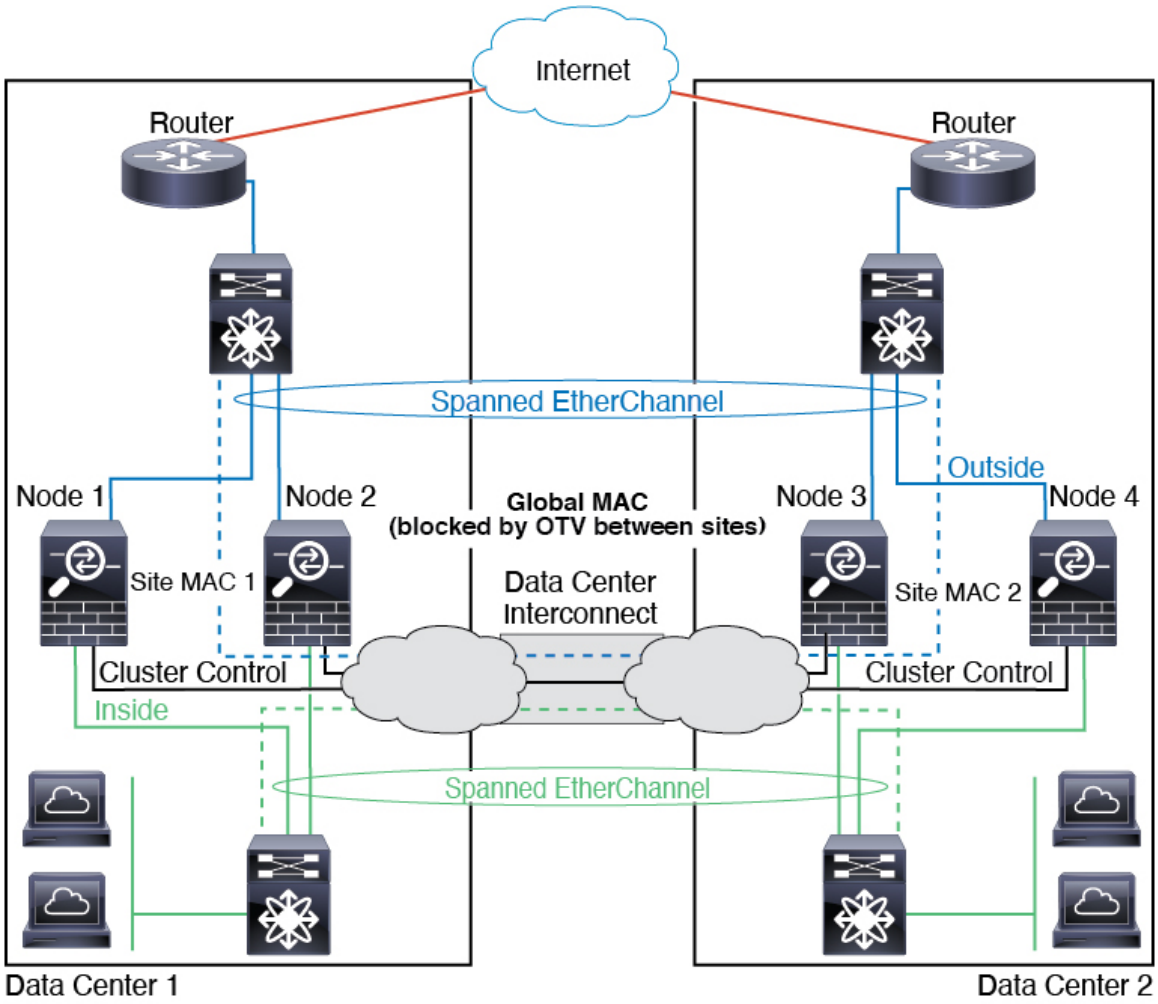
を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロックするフィルタを追加する必要があります。1 つのサイトのクラスタノードが到達不能になった場合、トラフィックが他のサイトのクラスタノードに送信されるようにフィルタを削除する必要があります。Vacl を使用して、グローバルの MAC アドレスのフィルタ リングする必要があります。F3 シリーズラインカードが搭載された Nexus などの一部のスイッチでは、グローバル MAC アドレスからの ARP パケットをブロックするために ARP インスペクションも使用する必要があります。ARP インスペクションでは、ASA でサイトの MAC アドレスとサイトの IP アドレスの両方を設定する必要があります。サイトの MAC アドレスのみを設定する場合は必ず ARP インスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタノード間で共有されるグローバルな仮想 MAC は、パケットを受信するためだけに使用されます。発信パケットは、各 DC クラスタからのサイト固有の MAC アドレスを使用します。この機能により、スイッチが 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。

この場合のシナリオは次のとおりです。

- クラスタから送信されるすべての出力パケットは、サイトの MAC アドレスを使用し、データセンターでローカライズされます。
- クラスタへのすべての入力パケットは、グローバル MAC アドレスを使用して送信されるため、両方のサイトにある任意のノードで受信できます。OTV のフィルタによって、データセンター内のトラフィックがローカライズされます。



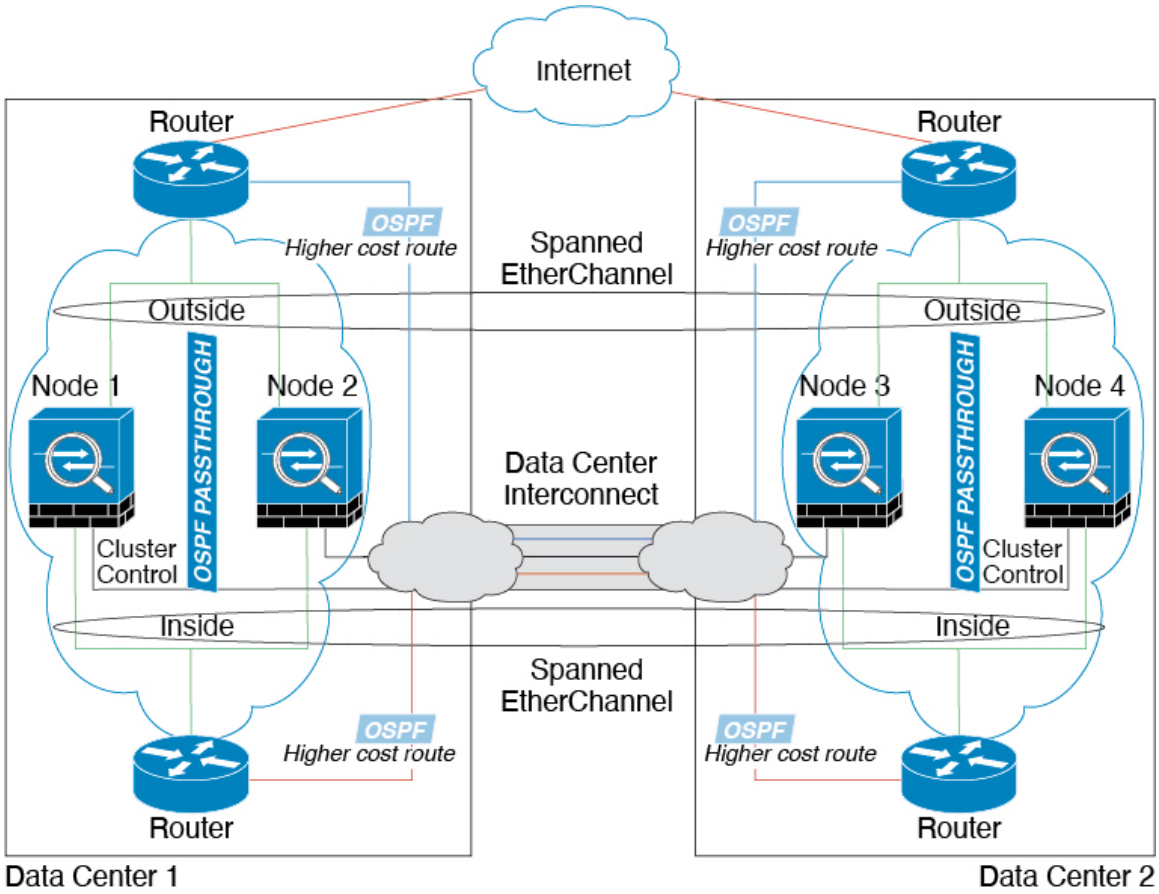
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コストルートを割り当てることにより、特定のサイトですべてのクラスタ メンバーがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1 つのサイトのすべてのクラスタ メンバーに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタ メンバーに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS/vPC：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタ ノードはローカルスイッチだけに接続し、VSS/vPC トラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCI が余分なトラフィックを処理できる場合、必要に応じて、各ノードを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS/vPC：スイッチの冗長性を高めるには、各サイトに 2 つの異なる VSS/vPC ペアをインストールできます。この場合、クラスタ ノードは、両方のローカルスイッチだけに接続されたデータセンター 1 のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター 2 のシャーシではスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。

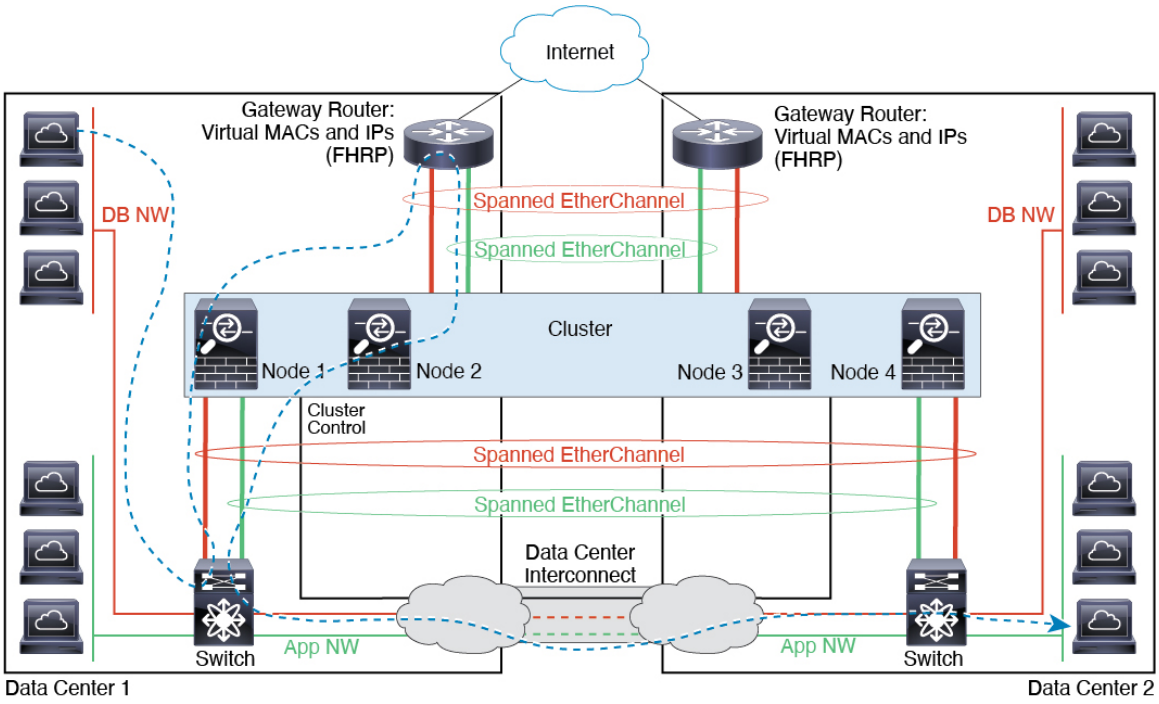


スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバーがある場合を示します。クラスタ メンバーは、

DCI経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバーは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイ ルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレス と IP アドレスを提供します。MAC アドレスの予期せぬフラッピングを避けるため、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト1のゲートウェイがサイト2のゲートウェイと通信する場合に、そのトラフィックがASAを通過して、内部インターフェイスからサイト2に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイ ルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1 つのサイトのゲートウェイ ルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- IS-IS ルーティング
- 次のアプリケーション インスペクション：
  - CTIQBE
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- VPN ロード バランシング
- フェールオーバー
- 統合ルーティングおよびブリッジング
- デッド接続検出（DCD）
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ユニット上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーユニットから制御ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ユニット以外のユニットに転送されることがあります。この場合は、トラフィックが制御ユニットに送り返されます。

中央集中型機能については、制御ユニットで障害が発生するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング
- スタティック ルート トラッキング
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス
- サイト間 IKEv1/IKEv2 VPN

  集中モードでは、VPN 接続はクラスタの制御ユニットとのみ確立されます。これは VPN クラスタリングのデフォルト モードです。サイト間 VPN は、分散 VPN モードでも展開できます。この場合、S2S IKEv2 VPN 接続がメンバー間で分散されます。

個々のユニットに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。
- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証と許可は、クラスタリング制御ノード上で中央集中型機能として実装されており、データ構造がクラスタデータノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザーおよびユーザーに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザー認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるため、フローに対するアカウンティングが設定されている場合、そのフローを所有するクラスタノードがアカウンティング開始と停止のメッセージを AAA サーバーに送信します。

接続設定

接続制限は、クラスタ全体に適用されます（**[構成（Configuration）] > [ファイアウォール（Firewall）] > [サービスポリシー（Service Policy）]** ページを参照）。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

FTP とクラスタリング

- FTP Dチャネルとコントロールチャネルのフローがそれぞれ別のクラスタ メンバーによって所有されている場合は、D チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロールフローのオーナーがリロードされて、コントロールフローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用する場合、制御チャネルのフローは制御ノードに集中されます。

ICMP インスペクション

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインスペクションが有効かどうかによって異なります。ICMPインスペクションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インスペクションを使用する場合、ICMP フローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットのディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

マルチキャスト ルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャストルーティング パケットとデータパケットを処理します。接続が確立された後は、各データユニットがマルチキャスト データ パケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラ

スタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。

- バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
- PAT IP アドレスのオーナーがダウンすると、バックアップノードは PAT の IP アドレス、対応するポートブロック、および xlate を所有します。通常の PAT アドレスでポートが不足している場合、新しい要求を処理するために引き継いだアドレスを使用できます。接続が最終的にタイムアウトすると、ブロックは解放されます。
- PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。

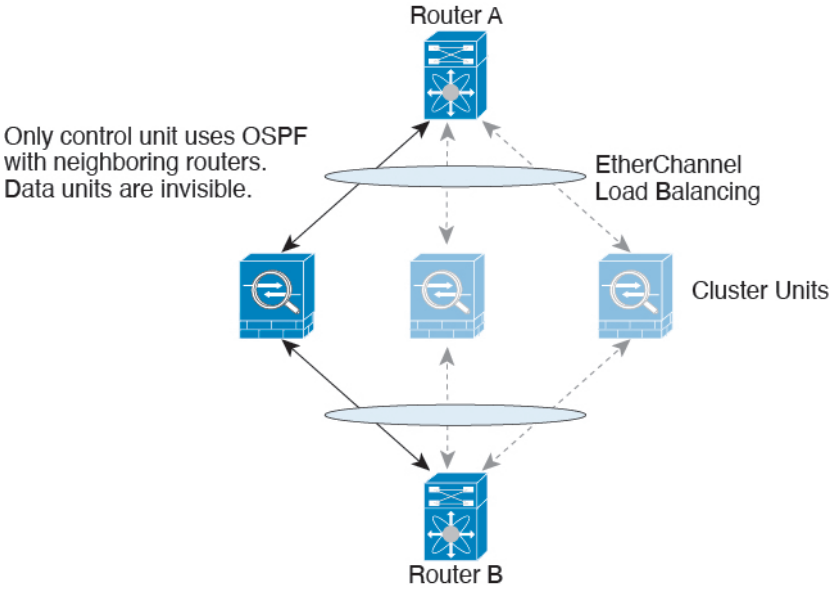
- ダイナミック PAT 用 NAT プールアドレス分散：制御ノードは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信し、アドレスが割り当てられていない場合、その接続は PAT の制御ノードに転送されます。クラスタメンバが（障害により）クラスタから離脱した場合、バックアップメンバは PAT IP アドレスを取得し、バックアップで通常の PAT IP アドレスが使い果たされると、新しいアドレスを使用できるようになります。各ノードがアドレスを受信し、アドレスを引き継いだメンバーが古いアドレスを使用している場合に障害が発生したノードが新しいアドレスを取得できるようにするには、少なくともクラスタ内のノードと同じ数の NAT アドレスに加えて、少なくとも 1 つの追加アドレスが含まれていることを確認してください。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。

- 旧式の xlates：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、ファイアウォールの設定ガイドを参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

ダイナミック ルーティングおよびクラスタリング

ルーティングプロセスは制御ユニット上だけで実行されます。ルートは制御ユニットを介して学習され、セカンダリに複製されます。ルーティングパケットがデータユニットに到着した場合は、制御ユニットにリダイレクトされます。

図 *58 :* ダイナミック ルーティング



データユニットが制御ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、制御ユニットからデータユニットに同期されません。制御ユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、その 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザーは新しいノードに複製されません。SNMPv3ユーザーは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、STUNインスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN要求の受信後にノードに障害が発生し、別のノードがSTUN応答を受信した場合、STUN応答はドロップされます。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。
- NetFlow：クラスタの各ノードは自身のNetFlowストリームを生成します。NetFlowコレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

FXOS シャーシ上の VPN とクラスタリング

ASA FXOS クラスタは、S2S VPN に対する相互排他的な 2 つのモード（集中型または分散型）のいずれかをサポートしています。

- 集中型 VPN モード。デフォルト モードです。集中モードでは、VPN 接続はクラスタの制御ユニットとのみ確立されます。

  VPN機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御ユニットで障害が発生した場合は、すべての既存のVPN接続が失われ、VPN接続されたユーザーにとってはサービスの中断となります。新しい制御ユニットが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散され、拡張性が提供されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

（注） 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。

分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。

分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。

リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタ パフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- 合計 UDP スループットの 90 %
- トラフィックの組み合わせに応じて、イーサネット MIX（EMIX）の合計スループットの 60 %

たとえば、TCP スループットについては、3 つの SM-44 モジュールを備えた Firepower 9300 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 135 Gbps となります。2 シャーシの場合、最大スループットの合計は 270 Gbps（2 シャーシ X 135 Gbps）の約 80 %、つまり 216 Gbps です。

制御ユニットの選定

クラスタのメンバーは、クラスタ制御リンクを介して通信して制御ユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットが制御ユニットになります。

(注) 最高のプライオリティを持つユニットが複数ある場合は、クラスタユニット名、次にシリアル番号を使用して制御ユニットが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的に制御ユニットになることはありません。既存の制御ユニットは常に制御ユニットのままです。ただし、制御ユニットが応答を停止すると、その時点で新しい制御ユニットが選定されます。

5. 「スプリットブレイン」シナリオで一時的に複数の制御ユニットが存在する場合、優先順位が最も高いユニットが制御ユニットの役割を保持し、他のユニットはデータユニットの役割に戻ります。

（注） 特定のユニットを手動で強制的に制御ユニットにすることができます。中央集中型機能については、制御ユニット変更を強制するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

シャーシ アプリケーションのモニターリング

シャーシ アプリケーションのヘルス モニターリングは常に有効になっています。Firepower 4100/9300 シャーシ スーパバイザは、ASA アプリケーションを定期的に確認します（毎秒）。Secure Firewall ASA が作動中で、Firepower 4100/9300 シャーシ スーパバイザと 3 秒間通信できなければ、Secure Firewall ASA は syslog メッセージを生成して、クラスタを離れます。

Firepower 4100/9300 シャーシ スーパバイザが 45 秒後にアプリケーションと通信できなければ、Secure Firewall ASA をリロードします。Secure Firewall ASA がスーパバイザと通信できなければ、自身をクラスタから削除します。

装置のヘルス モニターリング

各ユニットは、クラスタ制御リンクを介してブロードキャストキープアライブハートビートパケットを定期的に送信します。設定可能なタイムアウト期間内にデータユニットからキープアライブハートビートパケットまたはその他のパケットを受信しない場合、制御ユニットはクラスタからデータユニットを削除します。データユニットが制御ユニットからパケットを受信しない場合、新しい制御ユニットが残りのメンバーから選択されます。

ユニットで実際に障害が発生したためではなく、ネットワークの障害が原因で、ユニットがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータユニットが独自の制

御ユニットを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元のコントロールユニットは、ロケーション 2 のデータユニットをクラスタから削除します。一方、ロケーション 2 のユニットは、独自の制御ユニットを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ユニットが制御ユニットの役割を保持します。詳細については、制御ユニットの選定 （588 ページ）を参照してください。

インターフェイス モニターリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンクステータスをモニターし、ステータス変更を制御ユニットに報告します。シャーシ間クラスタリングでは、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニターして EtherChannel でポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には ASA アプリケーションに通知します。ヘルスモニターリングを有効にすると、デフォルトではすべての物理インターフェイスがモニターされます（EtherChannel インターフェイスのメイン EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニターできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません（最小ポート バンドル設定により異なる）。ヘルスチェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

あるモニター対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。Secure Firewall ASA がメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。Secure Firewall ASA は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、Secure Firewall ASA はクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます。

シャーシ間クラスタリングでは、クラスタから EtherChannel を追加または削除した場合、各シャーシに変更を加えられるように、インターフェイス ヘルス モニタリングは 95 秒間中断されます。

デコレータ アプリケーションのモニタリング

インターフェイスに Radware DefensePro アプリケーションなどのデコレータ アプリケーションをインストールした場合、ユニットがクラスタ内にとどまるには Secure Firewall ASA、デコレータ アプリケーションの両方が動作している必要があります。両方のアプリケーションが動作状態になるまで、ユニットはクラスタに参加しません。いったんクラスタに参加すると、ユニットはデコレータ アプリケーションが正しく動作しているか 3 秒ごとにモニターします。デコレータ アプリケーションがダウンすると、ユニットはクラスタから削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASAが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでノードがまだ非アクティブになっていると、管理インターフェイスは無効になります。さらに設定を行う場合は、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害（最初の参加時）：クラスタ制御リンクの問題を解決した後、と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASAは、無限に5分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、 と入力して、クラスタリングを手動でイネーブルにする必要があります。この動作は設定可能です。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。ユニットは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシ アプリケーション通信の障害：ASA がシャーシ アプリケーションの状態が回復したことを検出すると、ASA は自動的にクラスタの再参加を試みます。
- デコレータ アプリケーションの障害：ASA はデコレータ アプリケーションが復帰したことを確認すると、クラスタへ再参加します。

- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 ユニットは5分、10分、および20分の間隔でクラスタに自動的に再参加を試行します。この動作は設定可能です。

データ パス接続状態の複製

どの接続にも、1つのオーナーおよび少なくとも1つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *24*：クラスタ全体で複製される機能

トラフィック	状態のサポート	注記（**Notes**）
アップ タイム	○	システム アップ タイムをトラッキングします。
ARP テーブル	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	○	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	対応	—
ダイナミック ルーティング	対応	—
SNMP エンジン ID	なし	—
Firepower 4100/9300 用の分散型 VPN（サイト間）	Yes	バックアップ セッションがアクティブ セッションになると、新しいバックアップ セッションが作成されます。

クラスタが接続を管理する方法

接続をクラスタの複数のメンバーにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。

- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーが自分をディレクタとして選択した場合は、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

  サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルバックアップとグローバルバックアップの2つのバックアップ オーナー権限があります。オーナーは、常に同じサイトのローカルバックアップをオーナー自身として選択します（サイト ID に基づいて）。グローバルバックアップはどのサイトにも配置でき、ローカルバックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

  サイトの冗長性が有効になっており、バックアップ オーナーがオーナーと同じサイトに配置されている場合は、サイトの障害からフローを保護するために、別のサイトから追加のバックアップ オーナーが選択されます。シャーシ バックアップとサイト バックアップは独立しているため、フローにはシャーシ バックアップとサイト バックアップの両方が含まれている場合があります。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

サイト間クラスタリングのディレクタローカリゼーションを有効にすると、ローカルディレクタとグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（Site Id に基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにも配置でき、ローカルディレクタと同一ノードとすることもできます。最初のオーナーに障害が発生すると、ローカルディレクタは、同じサイトの新しい接続オーナーを選択します。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子で、宛先ポートは 0 です。
- 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
- 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタローカリゼーションを有効にすると、フォワーダは常にローカル ディレクタに問い合わせを行います。フォワーダがグローバル ディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタメンバーが受信する場合などです。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください。（TCP シーケンスのランダム化をディセーブルにした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

  注 クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロード

バランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを決定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。これが既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続の所有者はすべてのフラグメントを再構築します。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

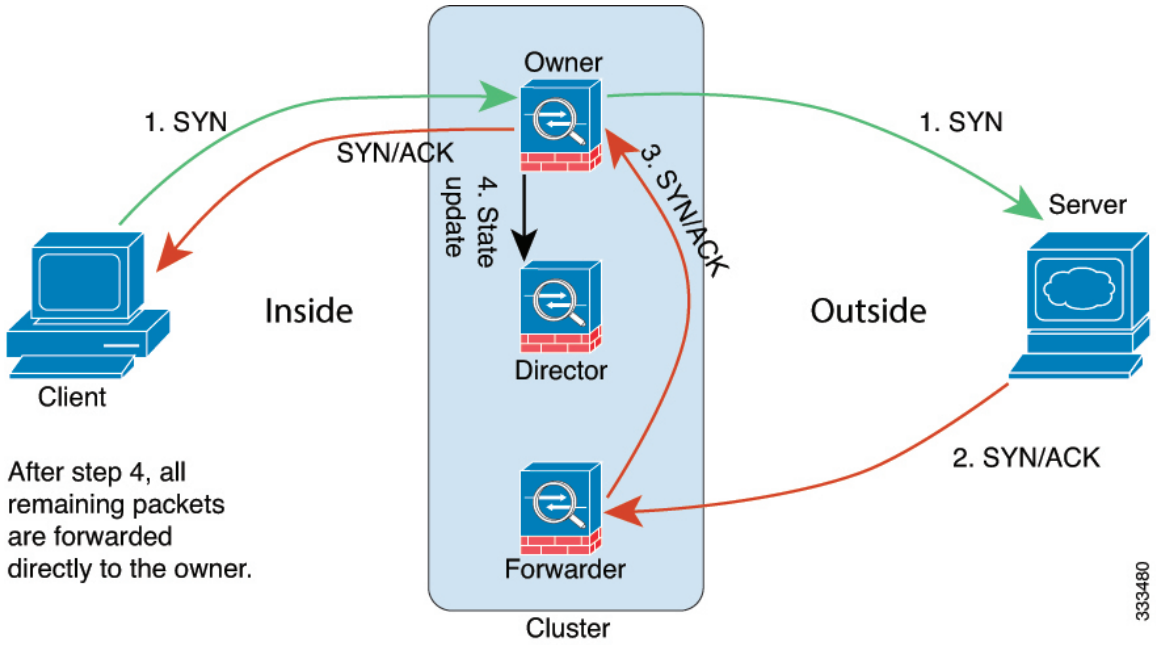
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

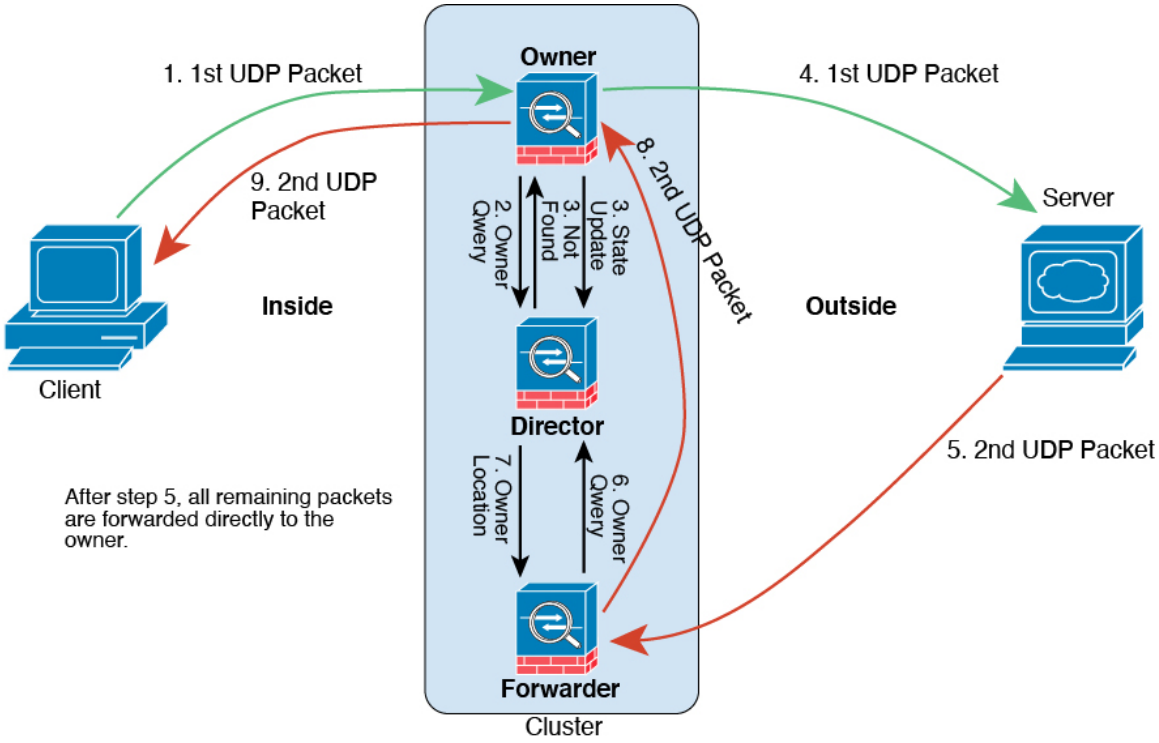


1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP 状態情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

1. 図 *59 : ICMP* および *UDP* データフロー



UDP パケットがクライアントから発信され、1 つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバーにパケットを転送します。
5. 2 番目の UDP パケットはサーバーから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

Firepower 4100/9300 での ASA クラスタリング履歴

機能名	バージョン	機能情報
データユニットとの設定の並列同期	9.14(1)	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable parallel configuration replicate]** チェックボックス
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 **show cluster history**	9.14(1)	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history** 新規/変更された画面：なし。
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 変更された画面はありません。
クラスタのトラフィック負荷のモニター	9.13(1)	クラスタ メンバのトラフィック負荷をモニターできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable Cluster Load Monitor]** チェックボックス • **[Monitoring]** > **[ASA Cluster]** > **[Cluster Load-Monitoring]**

機能名	バージョン	機能情報
クラスタ結合の高速化	9.13(1)	データユニットが制御ユニットと同じ設定の場合、設定の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。 （注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Enable config sync acceleration]** チェックボックス
サイトごとのクラスタリング用 Gratuitous ARP	9.12(1)	ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチング インフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]** > **[Site Periodic GARP]**フィールド
Firepower 9300 シャーシごとのユニットのパラレル クラスタ参加	9.10(1)	Firepower 9300 の場合、この機能により、シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されるようになります。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 新規/変更されたオプション：[Parallel Join of Units Per Chassis] エリア

機能名	バージョン	機能情報
Firepower 4100/9300 の Cluster Control Link のカスタマイズ可能な IP アドレス	9.10(1)	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された [Firepower Chassis Manager] 画面： **[Logical Devices]** > **[Add Device]** > **[Cluster Information]** 新規/変更されたオプション：[CCL Subnet IP] フィールド
クラスタインターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。	9.10(1)	インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで **health-check monitor-interface debounce-time** コマンドまたは ASDM **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタユニットの方がポートのバンドルが速いという理由だけで、クラスタユニット上でインターフェイスがエラー表示されるのを防ぐことができます。 変更された画面はありません。
内部障害発生後に自動的にクラスタに再参加する	9.9(2)	以前は、多くのエラー状態によりクラスタユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Auto Rejoin]**
クラスタの信頼性の高いトランスポートプロトコルメッセージのトランスポートに関連する統計情報の表示	9.9(2)	ユニットごとのクラスタの信頼性の高いトランスポート バッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**

機能名	バージョン	機能情報
動作と一致する**cluster remove unit**コマンドの動作**no enable**	9.9(1)	**cluster remove unit** コマンドは、**no enable** コマンドと同様に、クラスタリングまたはリロードを手動で再度有効にするまで、クラスタからユニットを削除するようになりました。以前は、FXOS からブートストラップ設定を再展開すると、クラスタリングが再度有効になりました。無効化されたステータスは、ブートストラップ設定の再展開の場合でも維持されるようになりました。ただし、ASA をリロードすると、クラスタリングが再度有効になります。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**
Firepower シャーシのシャーシ ヘルス チェックの障害検出の向上	9.9(1)	シャーシ ヘルス チェックの保留時間をより低い値（100 ms）に設定できるようになりました。以前の最小値は 300 ms でした。最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできないことに注意してください。 新規または変更されたコマンド：**app-agent heartbeat interval** ASDM サポートはありません。
クラスタリングのサイト間冗長性	9.9(1)	サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

機能名	バージョン	機能情報
Firepower 9300 上のクラスタリングによる分散型サイト間 VPN	9.9(1)	Firepower 9300 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ユニットだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスタ（合計 6 つのクラスタ メンバー）上で動作し、各モジュールは最大約 36,000 のアクティブ セッション（合計 72,000)に対し、最大 6,000 のアクティブ セッション（合計 12,000）をサポートします。 新規または変更された画面： **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Configuration] > [Device Management] > [High Availablility and Scalability] > [ASA Cluster]** **[Wizards] > [Site-to-Site]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [System Resource Graphs] > [CPU/Memory]** **[Monitoring] > [Logging] > [Real-Time Log Viewer]**
クラスタ ユニット ヘルスチェック障害検出の改善	9.8(1)	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージング アクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビート メッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

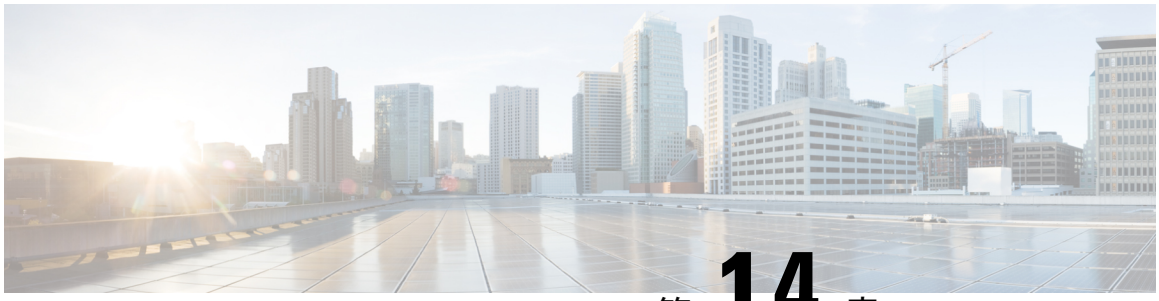
機能名	バージョン	機能情報
に対してインターフェイスを障害としてマークするために設定可能なデバウンス時間 Firepower 4100/9300 シャーシ	9.8(1)	ASA がインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。 新規または変更された画面：**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]**
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次の画面が変更されました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]**
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	9.7(1)	データセンターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次の画面を変更しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [Cluster Configuration]**
の 16 個のシャーシのサポート Firepower 4100 シリーズ	9.6(2)	Firepower 4100 シリーズ では最大 16 個のシャーシをクラスタに追加できるようになりました。 変更された画面はありません。
Firepower 4100 シリーズ のサポート	9.6(1)	FXOS 1.1.4 では、ASA は最大 6 個のシャーシの Firepower 4100 シリーズ でサイト間クラスタリングをサポートします。 変更された画面はありません。

機能名	バージョン	機能情報
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	9.6(1)	スパンド EtherChannel のルーテッドモードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイ トランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次の画面を変更しました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add/Edit EtherChannel Interface]** > **[Advanced]**
16 のモジュールのシャーシ間クラスタリング、および Firepower 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 16 のモジュールを搭載することができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。 変更された画面はありません。
ルーテッド ファイアウォールモードのスパンド EtherChannel のサイト間クラスタリング サポートのサイト別 MAC アドレス	9.5(2)	ルーテッドモードでは、スパンド EtherChannel サイト間クラスタリングを使用することができます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Cluster Configuration]**
インターフェイスまたはクラスタ制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスタのカスタマイズ	9.5(2)	インターフェイスまたはクラスタ制御リンクが失敗した場合、auto-rejoin 動作をカスタマイズできます。 次の画面を導入しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Auto Rejoin]**
ASA クラスタは、GTPv1 と GTPv2 をサポートします	9.5(2)	ASA クラスタは、GTPv1 および GTPv2 インスペクションをサポートします。 変更された画面はありません。
TCP 接続のクラスタ複製遅延	9.5(2)	この機能で、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。 次の画面を導入しました。**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster Replication]**

機能名	バージョン	機能情報
サイト間フローモビリティの LISP インスペクション	9.5(2)	Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID をその場所から 2 つの異なるナンバリング スペースに分離し、サーバーの移行をクライアントに対して透過的にします。ASA は、場所変更の LISP トラフィックを検査し、その情報をシームレスなクラスタリング運用に活用できます。ASA クラスタ メンバーは、最初のホップ ルータと出力トンネル ルータまたは入力トンネル ルータの間の LISP トラフィックを検査し、フロー オーナーの所在場所を新規サイトに変更します。 次の画面が導入または変更されました。 **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]** **[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [LISP]** **[Configuration] > [Firewall] > [Service Policy Rules] > [Protocol Inspection]** **[Configuration] > [Firewall] > [Service Policy Rules] > [Cluster]** **[Monitoring] > [Routing] > [LISP-EID Table]**
キャリア グレード NAT の強化がフェールオーバーおよび ASA クラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 変更された画面はありません。
クラスタリング トレース エントリの設定可能なレベル	9.5(2)	デフォルトで、すべてのレベル クラスタリング イベントは、多くの下位レベルのイベント以外に、トレース バッファに含まれます。より上位レベルのイベントへのトレースを制限するために、クラスタの最小トレース レベルを設定できます。 変更された画面はありません。
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4 (1.150)	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次の画面を導入しました。**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster Replication]**

第 III 部

インターフェイス



第 14 章

基本的なインターフェイス設定

この章では、イーサネット設定、ジャンボ フレーム設定などの基本的なインターフェイス設定について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。まだシステム実行スペースに入っていない場合は、[Configuration] > [Device List] ペイン内で、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

（注） プラットフォーム モードの Firepower 2100 および Firepower 4100/9300 シャーシ では、FXOS オペレーティング システムで基本的なインターフェイス設定を行います。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

基本的なインターフェイス設定について

この項では、インターフェイスの機能と特殊なインターフェイスについて説明します。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

管理インターフェイス

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用の管理スロット/ポート インターフェイス（使用しているモデルで使用できる場合）

管理アクセス（1139ページ）の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理スロット/ポート インターフェイス

次の表に、モデルごとの管理インターフェイスを示します。

表 *25*：モデルごとの管理インターフェイス

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 1000	—	—	—	対応	対応	対応

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 2100	—	—	—	対応	— （注） 技術的には、通過トラフィックを有効にすることはできますが、このインターフェイスのループバックはデータ操作には適していません。	○

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 4100/9300	該当なし インターフェイス ID は ASA 論理デバイスに割り当てた物理 mgmt タイプ インターフェイスに基づいています。	—	—	—	—	対応
ASA 5506-X	—	—	—	対応	—	—
ASA 5508-X	—	—	—	対応	—	—
ASA 5516-X	—	—	—	対応	—	—
ASA 5525-X	対応	—	—	—	—	—
ASA 5545-X	対応	—	—	—	—	—
ASA 5555-X	対応	—	—	—	—	—
ISA 3000	—	—	—	対応	—	—
ASAv	対応	—	—	—	対応	—

（注） モジュールをインストールした場合は、モジュール管理インターフェイスでは、モジュールの管理アクセスのみが提供されます。ソフトウェア モジュールを搭載したモデルでは、ソフトウェア モジュールによって ASA と同じ物理管理インターフェイスが使用されます。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます。

トランスペアレント モードの管理インターフェイス

トランスペアレント ファイアウォール モードでは、許可される最大通過トラフィック インターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）のいずれか）を個別の管理専用インターフェイスとして使用できます。他のインターフェイスタイプは管理インターフェイスとして使

用できません。Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。Firepower モデルでコンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ただし、ASA モデルでは、管理インターフェイスのサブインターフェイスが許可されないため、それらのモデルでコンテキスト単位の管理を行うには、データインターフェイスに接続する必要があります。Firepower 4100/9300 シャーシでは、管理インターフェイスとそのサブインターフェイスは、コンテキスト内で特別に許可された管理インターフェイスとして認識されません。この場合、管理サブインターフェイスをデータインターフェイスとして扱い、BVI に追加する必要があります。

管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

（注） トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータインターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、管理インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

冗長管理インターフェイスの非サポート

冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

ASA モデルの管理インターフェイスの特性

Asaasa 5500-X モデルの管理インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません
- マルチキャスト MAC はサポートされません

- ソフトウェア モジュールは、管理インターフェイスを共有します。ASA とモジュールに対して、別の MAC アドレスと IP アドレスがサポートされます。モジュールのオペレーティング システムでモジュールの IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスの有効化など）は、ASA 上で設定されます。

基本インターフェイスの設定のガイドライン

トランスペアレント ファイアウォール モード

マルチ コンテキストのトランスペアレント モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバー

データ インターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

その他のガイドライン

一部の管理関連のサービスは、管理対象外のインターフェイスが有効になり、ASA が「システム レディ」状態になるまで使用できません。ASA が「System Ready」状態になると、次の syslog メッセージを生成します。

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

基本インターフェイスのデフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- VXLAN VNI インターフェイス：イネーブル。
- EtherChannel ポートチャネル インターフェイス（ASA モデル、ISA 3000）：有効。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（その他のモデル）：無効。

（注） Firepower 4100/9300 の場合、管理上、シャーシおよび ASA の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと ASA の間の不一致が生じることがあります。

デフォルトの速度および二重通信

- デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。

デフォルトのコネクタ タイプ

2 つのコネクタ タイプ（copper RJ-45 と fiber SFP）を持つモデルもあります。RJ-45 がデフォルトです。ASA にファイバ SFP コネクタを使用するように設定できます。

デフォルトの MAC アドレス

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

物理インターフェイスのイネーブル化およびイーサネット パラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- フロー制御のポーズ フレームをイネーブルにする。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2 設定する物理インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

（注） シングル モードでは、この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチ コンテキスト モードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

ステップ 3 インターフェイスをイネーブルにするには、[Enable Interface] チェックボックスをオンにします。

ステップ 4 説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。こ

のインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 5 （任意）メディア タイプ、二重通信、速度を設定し、フロー制御のポーズ フレームをイネーブルにするには、[Configure Hardware Properties] をクリックします。

a) RJ-45 インターフェイスにデュプレックスを設定するには、[Duplex] ドロップダウンリストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

（注） EtherChannel インターフェイスのデュプレックスの設定は [Full] または [Auto] である必要があります。

b) 速度を設定するには、[Speed] ドロップダウンリストから値を選択します。

使用できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate]（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンク パラメータのネゴシエーションを行いません。RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。

c) 1 ギガビット イーサネット インターフェイスおよび 10 ギガビット イーサネット インターフェイスでフロー制御のポーズ（XOFF）フレームをイネーブルにするには、[Enable Pause Frame] チェック ボックスをオンにします。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。ポーズ（XOFF）および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーターマークを超えると、ポーズ フレームが送信されます。デフォルトの *high_water* 値は 128 KB（10 ギガビット イーサネット）および 24 KB（1 ギガビット イーサネット）です。0 ～ 511（10 ギガビット イーサネット）または 0 ～ 47 KB（1 ギガビット イーサネット）に設定できます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます。デフォルトでは、*low_water* 値は 64 KB（10 ギガビット イーサネット）および 16 KB（1 ギガビット イーサネット）です。0 ～ 511（10 ギガビット イーサネット）または 0 ～ 47 KB（1 ギガビット イーサネット）に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。デフォルトの *pause_time* 値は 26624 です。この値は 0 ～ 65535 に設定できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

[Low Watermark]、[High Watermark]、[Pause Time] のデフォルト値を変更するには、[Use Default Values] チェックボックスをオフにします。

（注） 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティ ベースのフロー制御はサポートされていません。

d) [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 6 [OK] をクリックして [Interface] の変更を受け入れます。

ジャンボフレームサポートの有効化（ASA モデル）

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネットフレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。ASA MTU はレイヤ 2（14 バイト）および VLAN ヘッダー（4 バイト）を含まずにペイロードサイズを設定するので、モデルによっては MTU 最大値が 9198 になることに注意してください。

（注） この手順は、ASA ハードウェアモデルと ASAv にのみ適用できます。Firepower モデルは、デフォルトでジャンボフレームをサポートしています。

始める前に

- マルチ コンテキスト モードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボフレームを送信する必要のある各インターフェイスの MTU を、デフォルト値の 1500 より大きい値に設定してください。たとえば、。マルチ コンテキスト モードでは、各コンテキスト内で MTU を設定します。
- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic, or to increase it in accord with the MTU.

手順

コンテキスト モードによって次のように異なります。

- マルチ モード：ジャンボ フレーム サポートをイネーブルにするには、[Configuration] > [Context Management] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。
- シングル モード：1500 バイトを超える MTU を設定すると、ジャンボ フレームが自動的にイネーブルになります。この設定を手動でイネーブルまたはディセーブルにするには、

[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] を選択し、[Enable jumbo frame support] チェック ボックスをオンにします。

基本インターフェイスの例

次の設定例を参照してください。

物理インターフェイス パラメータの例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

マルチ コンテキスト モードの例

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

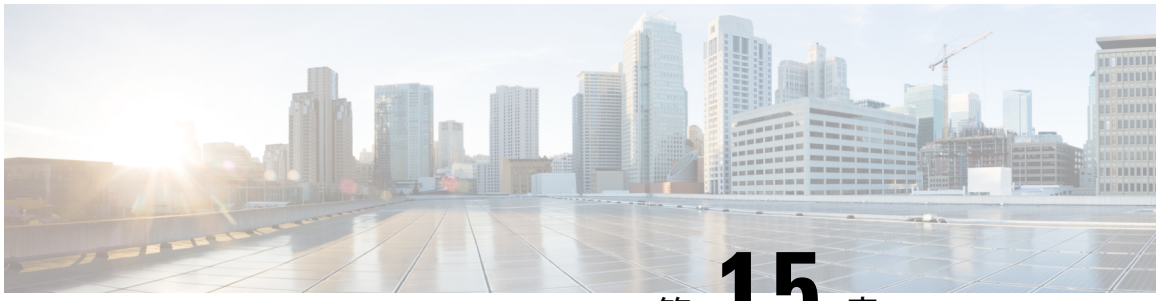
基本インターフェイスの設定の履歴

表 *26 :* インターフェイスの履歴

機能名	リリース	機能情報
Firepower 1000 および 2100 の SFP インターフェイスでの速度の自動ネゴシエーションの無効化	9.14(1)	自動ネゴシエーションを無効にするように Firepower 1100 または 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10 GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更された画面：**[構成（Configuration）] > [デバイスの設定（Device Settings）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）] > [ハードウェアプロパティの構成（Configure Hardware Properties）] > [速度（Speed）]**
ASAv の管理 0/0 インターフェイスでの通過トラフィック サポート	9.6(2)	ASAv の管理 0/0 インターフェイスでトラフィックを通過させることができるようになりました。以前は、Microsoft Azure 上の ASAv のみで通過トラフィックをサポートしていました。今後は、すべての ASAv で通過トラフィックがサポートされます。任意で、このインターフェイスを管理専用に設定できますが、デフォルトでは管理専用に設定されていません。

機能名	リリース	機能情報
ギガビットイーサネットインターフェイスでのフロー制御のポーズフレームのサポート	8.2(5)/8.4(2)	すべてのモデルでギガビットインターフェイスのフロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 次の画面が変更されました。[(Single Mode) Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General (Multiple Mode, System)] [Configuration] > [Interfaces] > [Add/Edit Interface]
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 この機能は、ASA 5585-X でもサポートされます。 次の画面が変更されました。[(Single Mode) Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General (Multiple Mode, System)] [Configuration] > [Interfaces] > [Add/Edit Interface]

機能名	リリース	機能情報
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。 この機能は、ASA 5585-X でもサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。



第 15 章

Firepower 1010 スイッチポートの基本インターフェイス設定

各 Firepower 1010 インターフェイスは、通常のファイアウォール インターフェイスとしてまたはレイヤ 2 ハードウェア スイッチ ポートとして実行するように設定できます。この章では、スイッチモードの有効化と無効化、VLANインターフェイスの作成、そのインターフェイスのスイッチポートへの割り当てなど、スイッチポート設定を開始するためのタスクについて説明します。また、サポート対象のインターフェイスで Power on Ethernet（PoE）をカスタマイズする方法についても説明します。

Firepower 1010 スイッチ ポートについて

この項では、Firepower 1010 のスイッチ ポートについて説明します。

Firepower 1010 ポートおよびインターフェイスについて

ポートとインターフェイス

Firepower 1010 物理インターフェイスごとに、ファイアウォール インターフェイスまたはスイッチポートとしてその動作を設定できます。物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理 VLAN インターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。 トランスペアレントモードでは、これらのインターフェイスは、設定済みのセキュリティポリ

シーを使用してファイアウォールサービスを適用することによって、レイヤ2の同じネットワーク上のインターフェイス間でトラフィックを転送するブリッジグループメンバーです。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット 1/1 インターフェイスはファイアウォール インターフェイスとして設定されます。

- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、ASA セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数の VLAN に属することができます。デフォルトでは、イーサネット 1/2 ～ 1/8 は VLAN 1 のアクセススイッチポートとして設定されています。Management インターフェイスをスイッチポートとして設定することはできません。
- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、冗長インターフェイス、またはEtherChannelインターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、ASA は VLAN インターフェイスにセキュリティポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループメンバーとしてVLANインターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックに ASA セキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、特定のセグメント間のレイヤブリッジグループとスイッチポートを選択することができます。

Power Over Ethernet

イーサネット 1/7 およびイーサネット 1/8 は Power on Ethernet+（PoE+）をサポートしています。

Auto-MDI/MDIX 機能

すべての Firepower 1010 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

Firepower 1010 スイッチ ポートの注意事項と制約事項

コンテキスト モード

Firepower 1010 はマルチ コンテキスト モードをサポートしません。

フェールオーバー とクラスタリング

- クラスタのサポートなし。
- アクティブ/スタンバイのフェールオーバーのサポートのみ。
- フェールオーバー を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェールオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、フェールオーバー を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
- ファイアウォールインターフェイスはフェールオーバー リンクとしてのみ使用できます。

論理 VLAN インターフェイス

- 最大 60 の VLAN インターフェイスを作成できます。
- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID は使用できません。
- MAC アドレス：
  - ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。手動 MAC アドレス、MTU、および TCP MSS の設定 （724 ページ） を参照してください。
  - トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。手動 MAC アドレス、MTU、および TCP MSS の設定 （724 ページ）を参照してください。

ブリッジ グループ

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- ポリシーベース ルーティング
- 等コストマルチパス（ECMP）ルーティング
- VXLAN
- EtherChannel
- 冗長インターフェイス。Firepower 1010 は、どのインターフェイス タイプに対しても冗長インターフェイスをサポートしていません。
- フェールオーバーおよびステートリンク
- トラフィック ゾーン
- セキュリティグループタグ（SGT）

その他のガイドラインと制約事項

- Firepower 1010 には、最大 60 の名前付きインターフェイスを設定できます。
- Management インターフェイスをスイッチポートとして設定することはできません。

デフォルト設定

- イーサネット 1/1 はファイアウォール インターフェイスです。
- イーサネット 1/2 ～ 1/8 は、VLAN 1 に割り当てられたスイッチ ポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

スイッチ ポートと Power Over Ethernet の設定

スイッチ ポートおよび PoE を設定するには、次のタスクを実行します。

VLAN インターフェイスの設定

ここでは、関連付けられたスイッチ ポートで使用するための VLAN インターフェイスの設定方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、**[Add]** > **[VLAN Interface]** を選択します。

ステップ 2 [VLAN ID] フィールドに、このインターフェイスの VLAN ID を 1 ー 4070 の範囲で入力します。ただし、内部使用のために予約されている 3968 ー 4047 の範囲の ID は除きます。

ステップ 3 （任意） [Block Traffic From this Interface to] ドロップダウンリストで、この VLAN インターフェイスがトラフィックを開始できない VLAN を選択します。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホームネットワークはビジネスネットワークにアクセスする必要がないので、ホーム VLAN で [Block Traffic From this Interface to] オプションを使用できます。ビジネスネットワークはホームネットワークにアクセスできますが、その反対はできません。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックします。

スイッチ ポートのアクセス ポートとしての設定

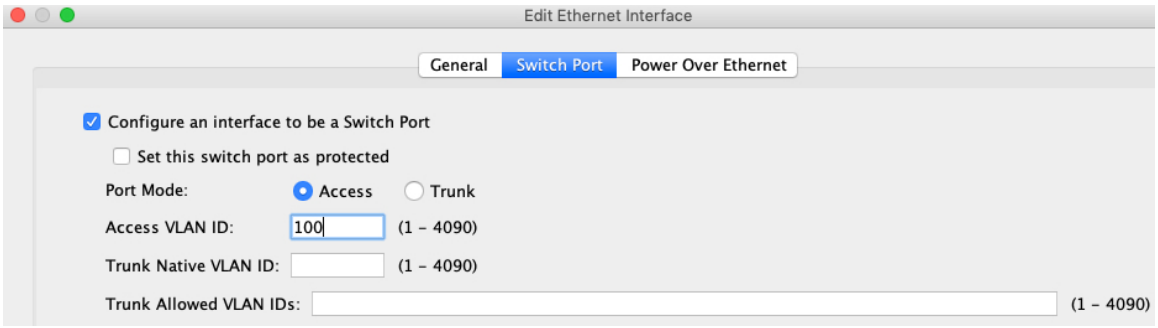
1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。アクセス ポートは、タグなしのトラフィックのみを受け入れます。デフォルトでは、Ethernet1/2 ～ 1/8 のスイッチ ポートが有効になっていて、VLAN 1 に割り当てられています。

（注） Firepower 1010 では、ネットワーク内のループ検出のためのスパニングツリー プロトコルはサポートされません。したがって、ASA との接続はいずれもネットワークループ内で終わらないようにする必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、編集するインターフェイスを選択して [Edit] をクリックします。

ステップ 2 [Switch Port] をクリックします。



ステップ 3 [Configure an interface to be a Switch Port] チェックボックスをオンにします。

ステップ 4 （任意） [Set this switch port as protected] チェックボックスをオンにして、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぎます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに [Set this switch port as protected] オプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 5 [Port Mode] の場合は、[Access] オプションボタンをクリックします。

ステップ 6 このスイッチポートに関連付けられている [Access VLAN ID] を 1 ～ 4070 の範囲で入力します。

デフォルトは VLAN 1 です。

ステップ 7 [General] をクリックします。

ステップ 8 [Enable Interface] をオンにします。

（注） [General] ページのその他のフィールド（[Interface Name] など）は、スイッチポートには適用されません。

ステップ 9 （任意） ハードウェアのプロパティを設定します。

a) [Configure Hardware Properties] をクリックします。

b) [Duplex] を選択します。

デフォルトは [自動（Auto）] です。

c) [Speed] を選択します。

デフォルトは [自動（Auto）] です。

d) [OK] をクリックします。

ステップ 10 [OK] をクリックします。

ステップ 11 [Apply] をクリックします。

スイッチ ポートのトランク ポートとしての設定

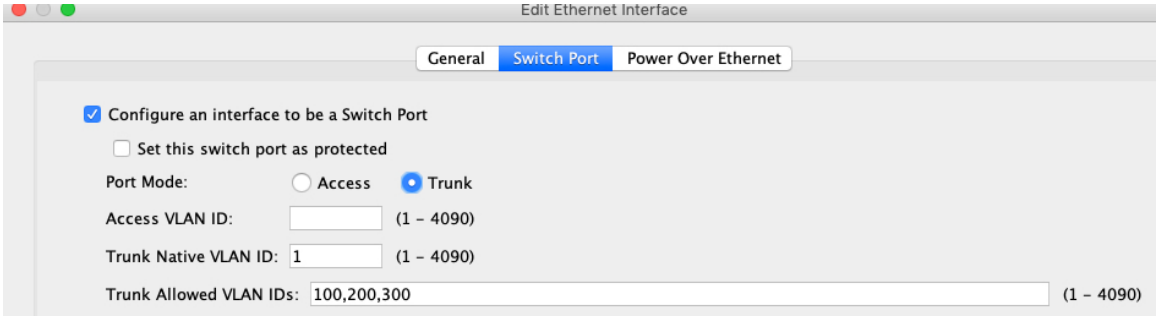
この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしおよびタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、編集するインターフェイスを選択して [Edit] をクリックします。

ステップ 2 [Switch Port] をクリックします。



ステップ 3 [Configure an interface to be a Switch Port] チェックボックスをオンにします。

ステップ 4 （任意） [Set this switch port as protected] チェックボックスをオンにして、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぎます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに [Set this switch port as protected] オプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 5 [Port Mode] の場合は、[Trunk] オプションボタンをクリックします。

ステップ 6 [Trunk Native VLAN ID] を 1 ～ 4070 の範囲で入力します。デフォルトは VLAN 1 です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

ステップ 7 このスイッチポートに関連付けられている [Trunk Allowed VLAN IDs] を 1 ～ 4070 の範囲で入力します。

このフィールドにネイティブ VLAN を含めても無視されます。トランク ポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。

ステップ 8 [General] をクリックします。

ステップ 9 [Enable Interface] をオンにします。

（注） [General] ページのその他のフィールド（[Interface Name] など）は、スイッチポートには適用されません。

ステップ 10 （任意） ハードウェアのプロパティを設定します。

a) [Configure Hardware Properties] をクリックします。

b) [Duplex] を選択します。

デフォルトは [自動（Auto）] です。

c) [Speed] を選択します。

デフォルトは [自動（Auto）] です。

d) [OK] をクリックします。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックします。

Power over Ethernet の設定

Ethernet 1/7 および Ethernet 1/8 は、IP 電話や無線アクセスポイントなどのデバイス用に Power over Ethernet（PoE）をサポートしています。Firepower 1010 は、IEEE 802.3af（PoE）と 802.3at（PoE+）の両方をサポートしています。PoE+ は、Link Layer Discovery Protocol（LLDP）を使用して電力レベルをネゴシエートします。PoE+ は、受電デバイスに最大 30 ワットの電力を提供できます。電力は必要なときのみ供給されます。

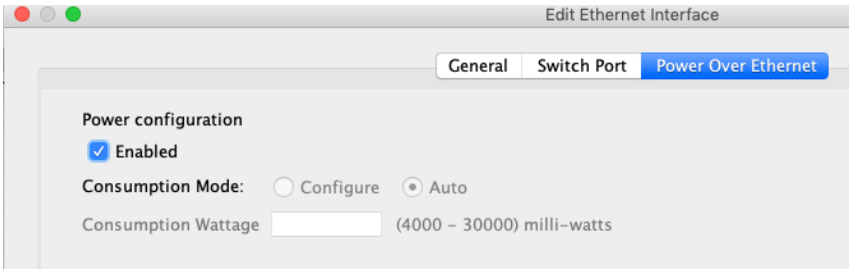
インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。

PoE は、デフォルトで Ethernet 1/7 および Ethernet 1/8 で有効になっています。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、編集するインターフェイス（イーサネット 1/7 または 1/8）を選択して [Edit] をクリックします。

ステップ 2 [Power Over Ethernet] をクリックします。



ステップ 3 [Enabled] をオンにします。

ステップ 4 [Consumption Mode] で、[Configure] または [Auto] オプションボタンをクリックします。

- [Auto]：給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。Firepower 1010 は LLDP を使用して、適切なワット数をさらにネゴシエートします。
- [Configure]：[Consumption Wattage] フィールドにワット数を手動で指定します（4000 ～ 30000）。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックします。

ステップ 7 現在の PoE+ ステータスを表示するには、**[Monitor]** > **[Interfaces]** > **[Power on Ethernet]** を選択して、現在の PoE+ ステータスを表示します。

スイッチポートのモニターリング

- **[Monitoring]** > **[Interfaces]** > **[ARP Table]**

  スタティック エントリやダイナミック エントリを含む ARP テーブルを表示します。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

- **[Monitoring]** > **[Interfaces]** > **[MAC Address Table]**

  スタティックおよびダイナミック MAC アドレス エントリを表示します。

- **[Monitoring]** > **[Interfaces]** > **[Interface Graphs]**

  インターフェイスの統計情報をグラフ形式またはテーブル形式で表示できます。

- **[Monitoring]** > **[Interfaces]** > **[L2 Switching]**

  VLAN とスイッチポートの関連付けおよびスタティックおよびダイナミック MAC アドレスエントリを表示します。

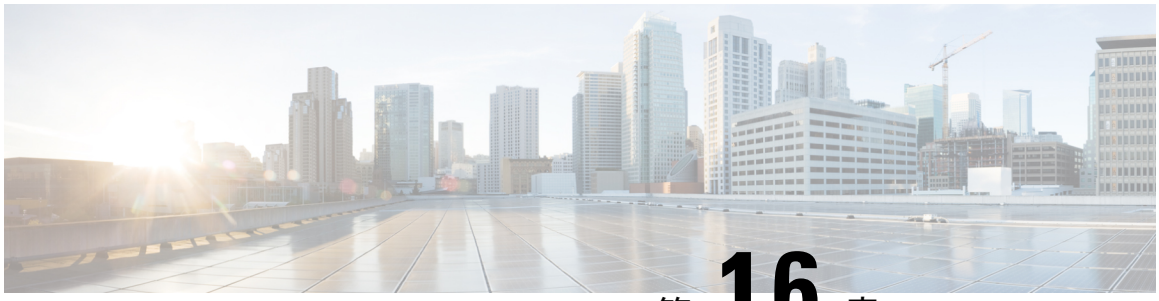
- **[Monitoring]** > **[Interfaces]** > **[Power Over Ethernet]**

  PoE+ ステータスを表示します。

スイッチポートの履歴

表 *27:* スイッチポートの履歴

機能名	バージョン	機能情報
Firepower 1010 ハードウェア スイッチのサポート	9.13(1)	Firepower 1010 では、各イーサネット インターフェイスをスイッチ ポートまたはファイアウォール インターフェイスとして設定できます。 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit]** > **[Switch Port]** • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add VLAN Interface]** • **[Monitoring]** > **[Interfaces]** > **[L2 Switching]**
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	9.13(1)	Firepower 1010 は、イーサネット 1/7 およびイーサネット 1/8 での Power over Ethernet+（PoE+） をサポートしています。 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit]** > **[Power Over Ethernet]** • **[Monitoring]** > **[Interfaces]** > **[Power Over Ethernet]**



第 16 章

EtherChannelインターフェイスと冗長インターフェイス

この章では、EtherChannel インターフェイスと冗長インターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。まだシステム実行スペースに入っていない場合は、[Configuration] > [Device List] ペイン内で、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

特殊な必須要件を保有する ASA クラスタ インターフェイスについては、ASA クラスタ （399 ページ） を参照してください。

（注） プラットフォームモードの Firepower 2100 および Firepower 4100/9300 シャーシ、EtherChannel インターフェイスはFXOSオペレーティングシステムで設定されます。冗長インターフェイスはサポートされません。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

EtherChannel インターフェイスと冗長インターフェイスについて

ここでは、EtherChannel インターフェイスと冗長インターフェイスについて説明します。

冗長インターフェイスについて（ASA プラットフォームのみ）

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してSecure Firewall ASAの信頼性を高めることができます。この機能は、デバイス レベルのフェールオーバーとは別個のものですが、必要な場合はデバイス レベルのフェールオーバーとともに冗長インターフェイスも設定できます。

最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに手動で MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

関連トピック

手動 MAC アドレス、MTU、および TCP MSS の設定 （724 ページ）
マルチ コンテキストの設定 （301 ページ）

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャネル グループ インターフェイス

各チャネルグループには、最大 16 個のアクティブインターフェイスを持たせることができます。ただし、Firepower 1000、2100 モデルは、8 個のアクティブインターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大16個のインターフェイスを割り当てることができます。インターフェイスは8個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブインターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

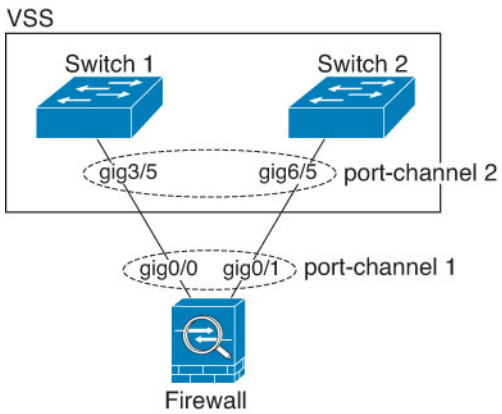
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

ASA EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

スイッチが仮想スイッチング システム（VSS）または 仮想ポート チャネル（vPC）の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

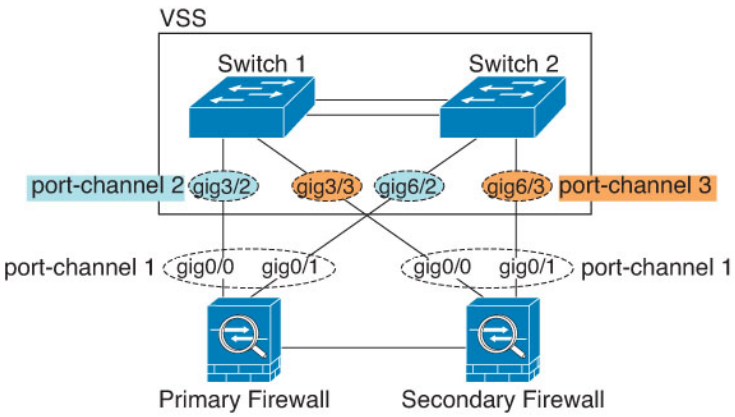
図 *60 : VSS/vPC* への接続



（注） ASA がトランスペアレント ファイアウォール モードで、2 組の VSS/vPC スイッチの間に ASA を配置する場合は、EtherChannel で ASA に接続されたすべてのスイッチポートで単方向リンク検出（UDLD）を無効にしてください。スイッチポートで UDLD を有効にすると、他の VSS/vPC ペアの両方のスイッチから送信された UDLD パケットを受信する場合があります。受信側スイッチの受信インターフェイスは「UDLD Neighbor mismatch」という理由でダウン状態になります。

ASA をアクティブ/スタンバイ フェールオーバー配置で使用する場合、ASA ごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 ASA で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチインターフェイスを両方の ASA に接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の ASA システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ ASA に送信しないようにするためです。

図 *61 : アクティブ/スタンバイ フェールオーバーと VSS/vPC*



リンク集約制御プロトコル

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。Firepower ハードウェアモデルではサポートされていません。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

ASA は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です）。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスに送信され、以降は結果が 1 となるものは 2 番目のインターフェイスに、結果が 2 となるものは 3 番目のインターフェイスに、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

クラスタリングのスパンド EtherChannel では、ロードバランシングは ASA ごとに行われます。たとえば、8 台の ASA にわたるスパンド EtherChannel 内に 32 個のアクティブインターフェイスがあり、EtherChannel 内の 1 台の ASA あたり 4 個のインターフェイスがある場合、ロードバランシングは 1 台の ASA の 4 個のインターフェイス間でのみ行われます。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

関連トピック

EtherChannel のカスタマイズ （646 ページ）

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチコンテキストモードでは、EtherChannel ポートインターフェイスを含め、一意の MAC アドレスを共有インターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを,手動で設定するか、または共有インターフェイスのマルチ コンテキスト モードでは自動的に設定することを推奨します。ポート チャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポート チャネル MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

EtherChannel インターフェイスと冗長インターフェイスのガイドライン

ブリッジ グループ

ルーテッドモードでは、ASA 定義の EtherChannel はブリッジグループメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。

フェールオーバー

- EtherChannel インターフェイスまたは冗長インターフェイスをフェールオーバー リンクとして使用する場合、フェールオーバーペアの両方のユニットでその事前設定を行う必要があります。プライマリユニットで設定し、セカンダリユニットに複製されることは想定できません。これは、複製には フェールオーバー リンク自体が必要であるためです。
- EtherChannel インターフェイスまたは冗長インターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリユニットから複製されます。Firepower 4100/9300 シャーシでは、EtherChannel を含むすべてのインターフェイスを、両方のユニットで事前に設定する必要があります。
- **monitor-interface** コマンドを使用して、フェールオーバー の EtherChannel インターフェイスまたは冗長インターフェイスをモニタできます。。アクティブなメンバーインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、EtherChannel インターフェイスまたは冗長インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、EtherChannel インターフェイスまたは冗長インターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバインターフェイスの数を設定できます）。
- EtherChannel インターフェイスをフェールオーバーまたはステートリンクに対して使用する場合、パケットが順不同にならないように、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、フェールオーバーを一時的に無効にする必要があります。これにより、その期間中は フェールオーバー が発生することはありません。

モデルのサポート

- プラットフォームモードの Firepower 2100、Firepower 4100/9300、または ASAv の場合、ASA に EtherChannel を追加することはできません。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。

- 冗長インターフェイスは、ASA 5500-X プラットフォームでのみサポートされます。
- EtherChannel で Firepower 1010 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

クラスタリング

- スパンドEtherChannelまたは個別クラスタインターフェイスを設定するには、クラスタリングの章を参照してください。

EtherChannel の一般的なガイドライン

- モデルで利用可能なインターフェイスの数に応じて、最大48個のEtherchannelを設定できます。
- 各チャネルグループには、最大 16 個のアクティブインターフェイスを持たせることができます。ただし、Firepower 1000、2100 モデルは、8 個のアクティブインターフェイスをサポートしています。8個のアクティブインターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブインターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。
- チャネルグループ内のすべてのインターフェイスは、同じメディアタイプと容量である必要があり、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。
- ASA の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- ASA は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにするとASAはタグ付きのLACPDUをドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。マルチ コンテキスト モードでは、これらのメッセージはパケット キャプチャに含まれていないため、問題を効率的に診断できません。
- ASA 5500-X モデル、Firepower 1000、および Firepower 2100（アプライアンスモードとプラットフォームモードの両方）は、LACP レート高速機能をサポートしていません。LACP では常に通常のレートが使用されます。この値は設定不可能です。FXOS で EtherChannel を設定する Firepower 4100/9300 では、LACP レートがデフォルトで高速に設定されていることに注意してください。これらのプラットフォームでは、レートを設定できます。

- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する ASA では、スイッチ スタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、ASA EtherChannel がクロススタックに接続されている場合、プライマリスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。

EtherChannel インターフェイスと冗長インターフェイのデフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。

- EtherChannel ポートチャネル インターフェイス：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。

冗長インターフェイスの設定

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。

この項では、冗長インターフェイスを設定する方法について説明します。

冗長インターフェイスの設定

この項では、冗長インターフェイスを作成する方法について説明します。デフォルトでは、冗長インターフェイスはイネーブルになっています。

始める前に

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 冗長インターフェイス遅延値は設定可能ですが、デフォルトでは、ASA はそのメンバーインターフェイスの物理タイプに基づくデフォルトの遅延値を継承します。
- 両方のメンバーインターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビット イーサネットにする必要があります。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインで、名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードを開始していない場合は、[Configuration] > [Device List] ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

⚠

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** ペインを選択します。
- マルチ モードの場合、システム実行スペースで、**[Configuration]** > **[Context Management]** > **[Interfaces]** ペインを選択します。

ステップ 2 **[Add]** > **[Redundant Interface]** の順に選択します。

[Add Redundant Interface] ダイアログボックスが表示されます。

（注） シングル モードでは、この手順では [Edit Redundant Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチ コンテキスト モードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。マルチ コンテキストの設定（301 ページ）を参照してください。

ステップ 3 [Redundant ID] フィールドで、1 ～ 8 の整数を入力します。

ステップ 4 [Primary Interface] ドロップダウンリストから、プライマリにする物理インターフェイスを選択します。

サブインターフェイスを持たず、まだコンテキストに割り当てられていないインターフェイスを必ず選択してください。冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。

ステップ 5 [Secondary Interface] ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。

ステップ 7 説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 8 [OK] をクリックします。

[Interfaces] ペインに戻ります。メンバー インターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。冗長インターフェイスがテーブルに追加されます。

GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

アクティブ インターフェイスの変更

デフォルトでは、コンフィギュレーションで最初にリストされているインターフェイスが（使用可能であれば）、アクティブ インターフェイスになります。

手順

ステップ 1 どのインターフェイスがアクティブかを表示するには、**[Tools]** > **[Command Line Interface]** ツールで次のコマンドを入力します。

show interface redundant *number* **detail** | **grep Member**

例：

```
show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

ステップ 2 アクティブ インターフェイスを変更します。

redundant-interface redundant *number* **active-member** *physical_interface*

redundant*number* 引数には、冗長インターフェイス ID（**redundant1** など）を指定します。

physical_interface には、アクティブにするメンバ インターフェイスの ID を指定します。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

EtherChannel へのインターフェイスの追加

ここでは、EtherChannel ポートチャネル インターフェイスを作成し、インターフェイスを EtherChannel に割り当てる方法について説明します。デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。

始める前に

- 使用しているモデルに設定されているインターフェイスの数に応じて、最大 48 個の EtherChannel を設定できます。
- 次のメンバー制限を参照してください。
  - ASA ハードウェア、ISA 3000：各チャネルグループは、最大 16 個のアクティブインターフェイスを設定できます。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
  - Firepower 1000、2100：各チャネルグループに最大 8 つのアクティブインターフェイスを設定できます。
- クラスタリング用にスパンド EtherChannel を設定するには、この手順の代わりにクラスタリングの章を参照してください。
- チャネルグループ内のすべてのインターフェイスは、同じメディアタイプと容量である必要があり、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。
- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインで、名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードを開始していない場合は、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイス IP アドレスの下にある [System] をダブルクリックします。

⚠

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** ペインを選択します。

- マルチ モードの場合、システム実行スペースで、**[Configuration]** > **[Context Management]** > **[Interfaces]** ペインを選択します。

ステップ 2 **[Add]** > **[EtherChannel Interface]** の順に選択します。

[Add EtherChannel Interface] ダイアログボックスが表示されます。

（注） シングル モードでは、この手順では [Edit EtherChannel Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチ コンテキスト モードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。マルチ コンテキストの設定（301 ページ）を参照してください。

ステップ 3 In the **Port Channel ID** field, enter a number between 1 and 48（1 and 8 for the Firepower 1010).

ステップ 4 [Available Physical Interface] 領域で、インターフェイスをクリックし、[Add] をクリックしてそれを [Members in Group] 領域に移動します。

トランスペアレント モードで、複数の管理インターフェイスがあるチャネル グループを作成する場合は、この EtherChannel を管理専用インターフェイスとして使用できます。

（注） EtherChannel モードをオンに設定する場合、最初はインターフェイスを 1 個のみ含める必要があります。この手順を完了後、メンバー インターフェイスを編集し、このモードを**オン**に設定します。変更を適用し、EtherChannel を編集してメンバー インターフェイスをさらに追加します。

ステップ 5 チャネル グループに追加するインターフェイスごとに繰り返します。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。ASDM では、一致しないインターフェイスの追加は防止されません。

ステップ 6 [OK] をクリックします。

[Interfaces] ペインに戻ります。メンバー インターフェイスで、基本パラメータのみが設定できることを示すロックが、インターフェイス ID の左側に表示されます。EtherChannel インターフェイスがテーブルに追加されます。

ステップ 7 [Apply] をクリックします。すべてのメンバー インターフェイスは自動的にイネーブルになります。

関連トピック

リンク集約制御プロトコル （636 ページ）
EtherChannel のカスタマイズ （646 ページ）

EtherChannel のカスタマイズ

この項では、EtherChannel のインターフェイスの最大数、EtherChannel をアクティブにするための動作インターフェイスの最小数、ロード バランシング アルゴリズム、およびその他のオプション パラメータを設定する方法について説明します。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** ペインを選択します。
- マルチ モードの場合、システム実行スペースで、**[Configuration]** > **[Context Management]** > **[Interfaces]** ペインを選択します。

ステップ 2 カスタマイズするポートチャネル インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

ステップ 3 すべてのメンバインターフェイスについて、メディア タイプ、二重通信、速度、およびフロー制御のポーズ フレームを上書きするには、[Configure Hardware Properties] をクリックします。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 4 （オプション。ASA 5500-X および ISA 3000 のみ）EtherChannel をカスタマイズするには、[詳細設定（Advanced）] タブをクリックします。

a) [EtherChannel] 領域で、[Minimum] ドロップダウンリストから、EtherChannel をアクティブにするために必要なアクティブ インターフェイスの最小数を 1 ～ 16 の範囲で選択します。デフォルトは 1 です。

b) [Maximum] ドロップダウンリストから、EtherChannel で許可されるアクティブ インターフェイスの最大数を 1 ～ 16 の範囲で選択します。デフォルトは 16 です。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。

c) [Load Balance] ドロップダウンリストから、パケットをグループ チャネル インターフェイス間でロード バランスするために使用する基準を選択します。デフォルトでは、ASA はパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロード バランシングの詳細については、ロード バランシング （637 ページ）を参照してください。

d) [Secure Group Tagging] 設定については、ファイアウォール コンフィギュレーション ガイドを参照してください。

e) [ASA Cluster] 設定については、（推奨、マルチコンテキストモードでは必須）制御ユニットでのインターフェイスの設定 （427 ページ）を参照してください。

ステップ 5 [OK] をクリックします。

[Interfaces] ペインに戻ります。

ステップ 6 チャネル グループ内の物理インターフェイスのモードおよびプライオリティを設定するには、次の手順を実行します。

a) [Interfaces] テーブルで物理インターフェイスを選択し、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

b) [Advanced] タブをクリックします。

c) [EtherChannel] 領域で、[Mode] ドロップダウンリストから、[Active]、[Passive]、または [On] を選択します。[Active] モード（デフォルト）を使用することを推奨します。

d) （オプション。ASA 5500-X および ISA 3000 のみ）[LACPポートの優先順位（LACP Port Priority）] フィールドで、ポートの優先順位を 1 ～ 65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポート プライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、0/7 インターフェイスでのデフォルトの 32768 に対し、1/3 インターフェイスでプライオリティ値を 12345 にします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。システム プライオリティを設定するには、ステップ 9 を参照してください。

ステップ 7 [OK] をクリックします。

[Interfaces] ペインに戻ります。

ステップ 8 [Apply] をクリックします。

ステップ 9 （オプション。ASA 5500-X および ISA 3000 のみ）LACP システムプライオリティを設定するには、次の手順を実行します。EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システムプライオリティを使用して使用するポートプライオリティが決定されます。詳細については、ステップ 6d を参照してください。

a) コンテキスト モードによって次のように異なります。

- シングルモードの場合、**[構成（Configuration）] > [デバイス設定（Device Setup）] > [EtherChannel]**ペインを選択します。
- マルチモードの場合、システム実行スペースで、**[構成（Configuration）] > [コンテキスト管理（Context Management）] > [EtherChannel]**ペインを選択します。

b) [LACP System Priority] フィールドに、プライオリティを 1 ～ 65535 の範囲で入力します。デフォルトは 32768 です。

関連トピック

ロード バランシング （637 ページ）
EtherChannel へのインターフェイスの追加 （643 ページ）

EtherChannel の例

次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

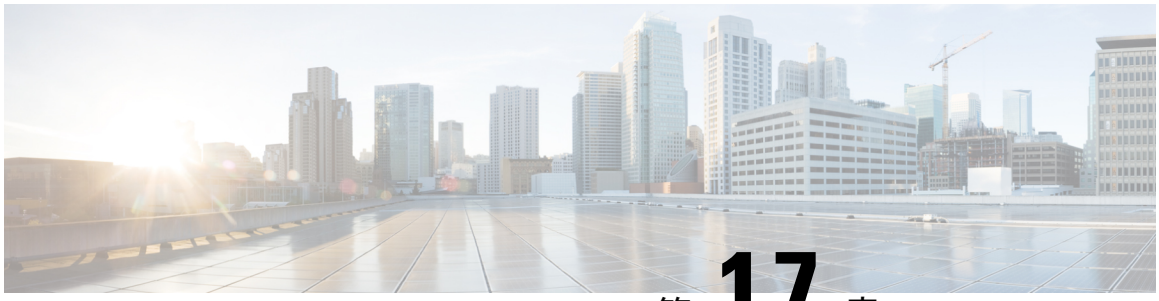
```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

EtherChannel インターフェイスと冗長インターフェイスの履歴

表 *28 : EtherChannel* インターフェイスと冗長インターフェイスの履歴

機能名	リリース	機能情報
冗長インターフェイス	8.0(2)	論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブインターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイスペアを設定できます。
EtherChannel サポート	8.4(1)	最大 48 個の 802.3ad EtherChannel（1 つあたりのアクティブインターフェイス 8 個）を設定できます。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] [Configuration] > [Device Setup] > [EtherChannel] （注） EtherChannel は ASA 5505 ではサポートされません。

機能名	リリース	機能情報
EtherChannel あたり 16 個のアクティブ リンクのサポート	9.2(1)	EtherChannel あたり最大で 16 個のアクティブ リンクを設定できるようになりました。これまでは、8 個のアクティブ リンクと 8 個のスタンバイ リンクが設定できました。スイッチは、16 個のアクティブ リンクをサポート可能である必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 （注） 旧バージョンの ASA からアップグレードする場合、互換性を得るために、アクティブなインターフェイスの最大数を 8 に設定します。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit EtherChannel Interface] > [Advanced]。



第 17 章

VLAN サブインターフェイス

この章では、VLAN サブインターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。システム実行スペースに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイス IPアドレスの下にある **[System]** をダブルクリックします。

VLAN サブインターフェイスについて

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチ コンテキスト モードで特に便利です。

1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN を設定できます。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。

VLAN サブインターフェイスのライセンス

モデル	ライセンス要件
Firepower 1010	標準ライセンス：60
Firepower 1120	標準ライセンス：512
Firepower 1140、1150	標準ライセンス：1024
Firepower 2100	標準ライセンス：1024
Firepower 4100	標準ライセンス：1024
Firepower 9300	標準ライセンス：1024
ASAv	スループット機能： 100 Mbps：25 1 Gbps：50 2 Gbps：200 10 Gbps：1024
ASA 5506-X ASA 5506W-X ASA 5506H-X	基本ライセンス：5 Security Plus ライセンス：30
ASA 5508-X	基本ライセンス：50
ASA 5516-X	基本ライセンス：50
ASA 5525-X	基本ライセンス：200
ASA 5545-X	基本ライセンス：300
ASA 5555-X	基本ライセンス：500
ISA 3000	基本ライセンス：5 Security Plus ライセンス：100

（注） VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- Firepower 1010：VLAN サブインターフェイスは、スイッチ ポートまたは VLAN インターフェイスではサポートされていません。
- ASA モデルでは、管理インターフェイスのサブインターフェイスを設定できません。サブインターフェイスのサポートについては、管理スロット/ポート インターフェイス （610 ページ）を参照してください。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。トラフィックがサブインターフェイスを通過するには、物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスがイネーブルになっている必要があるため、トラフィックが物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを通過しないように、インターフェイスには名前を設定しないでください。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常どおり nameを設定できます。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- ASA は Dynamic Trunking Protocol（DTP）をサポートしていないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。一意の MAC アドレスを自動的に生成できます。マルチコンテキストモードでの MAC アドレスの自動割り当て （723 ページ）を参照してください。

VLAN サブインターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスに追加します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインを選択します。

- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

ステップ 2 **[Add]** > **[Interface]** の順に選択します。

[Add Interface] ダイアログボックスが表示されます。

（注） シングル モードの場合、この手順で対象としているのは [Edit Interface] ダイアログボックスのパラメータのサブセットのみであるため、他のパラメータを設定する場合は、ルーテッド モードおよびトランスペアレント モードのインターフェイス （675 ページ）を参照してください。マルチ コンテキスト モードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。マルチ コンテキストの設定 （301 ページ）を参照してください。

ステップ 3 [ハードウェアポート（Hardware Port）] ドロップダウンリストから、サブインターフェイスを追加する物理インターフェイス、冗長インターフェイス、またはポートチャネルインターフェイスを選択します。

ステップ 4 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。

ステップ 5 [VLAN ID] フィールドに、1 ～ 4094 の VLAN ID を入力します。

VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。マルチ コンテキスト モードの場合、VLAN はシステム設定でしか設定できません。

ステップ 6 [Secondary VLAN ID] フィールドに、1 つ以上の VLAN ID をスペースまたはカンマで区切って入力します。連続する範囲の場合はダッシュを使用します。

ASA はセカンダリ VLAN でトラフィックを受信すると、そのトラフィックをプライマリ VLAN にマップします。

ステップ 7 [Subinterface ID] フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

ステップ 8 （オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9 [OK] をクリックします。

[Interfaces] ペインに戻ります。

関連トピック

VLAN サブインターフェイスのライセンス （652 ページ）

VLAN のサブインターフェイスの例

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

次に、Catalyst 6500 でどのように VLAN マッピングが機能するのかを示します。ノードを PVLANS に接続する方法については、Catalyst 6500 の設定ガイドを参照してください。

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

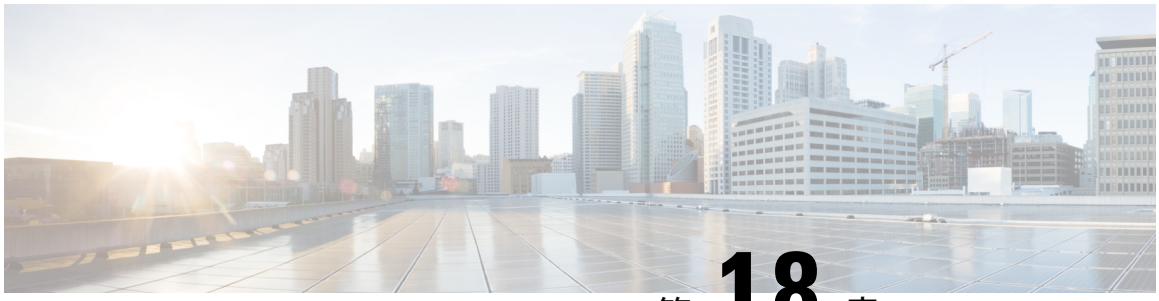
```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
```

```
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

VLAN サブインターフェイスの履歴

表 *29 : VLAN* サブインターフェイスの履歴

機能名	バージョン	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
セカンダリ VLAN のプライマリ VLAN へのマッピングのサポート	9.5(2)	サブ インターフェイスで、1 つ以上のセカンダリ VLAN を設定できるようになりました。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。 次の画面が変更されました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add Interface]** > **[General]**
ISA 3000 の VLAN 数の増加	9.13(1)	Security Plus ライセンスが有効な ISA 3000 について、最大 VLAN 数が 25 から 100 に増えました。



第 18 章

VXLAN インターフェイス

この章では、仮想拡張 LAN（VXLAN）インターフェイスを設定する方法について説明します。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

VXLAN インターフェイスの概要

VXLAN は、VLAN の場合と同じイーサネットレイヤ 2 ネットワークサービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。VXLAN の詳細については、RFC 7348 を参照してください。

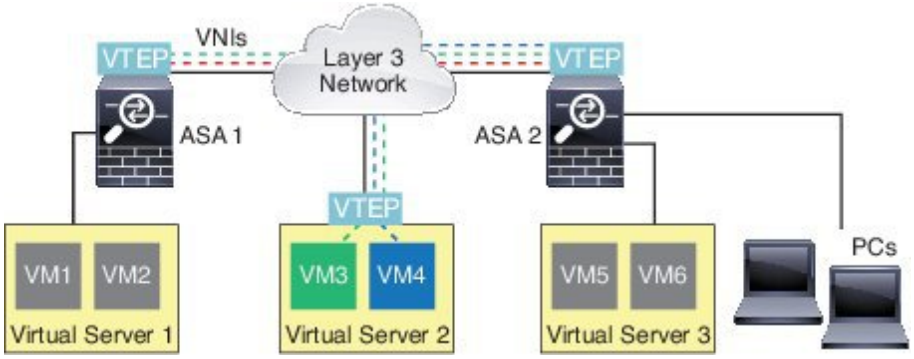
VXLAN カプセル化

VXLAN は、レイヤ 3 ネットワーク上のレイヤ 2 オーバーレイ方式です。VXLAN は、MAC Address-in-User Datagram Protocol（MAC-in-UDP）のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。

VXLAN トンネル エンドポイント

VXLAN トンネルエンドポイント（VTEP）デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ（セキュリティ ポリシーを適用する VXLAN Network Identifier（VNI）インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、 VTEP 間に VNI をトンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス）があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図に、レイヤ 3 ネットワークで VTEP として機能し、サイト間の VNI 1、2、3 を拡張する 2 つの ASA と仮想サーバ 2 を示します。ASA は、VXLAN と VXLAN 以外のネットワークの間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャストグループにすることができます。デフォルトでは、 宛先ポートは UDP ポート 4789 です（ユーザ設定可能）。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる予定の標準の ASA インターフェイス（物理、冗長、EtherChannel、または VLAN）です。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティ ポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレント ファイアウォール モードでは、VTEP 送信元インターフェイスは、BVI の一部ではないため、その IP アドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。

追加できる VTEP インターフェイスは 1 つだけで、すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。

VXLAN パケット処理

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP送信元インターフェイスにより、VXLANヘッダーが含まれている内部MACフレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に ASA によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- VXLAN パケット形式が標準に準拠します。

ピア VTEP

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

  手動で複数のピアを定義することはできません。

  ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

  ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

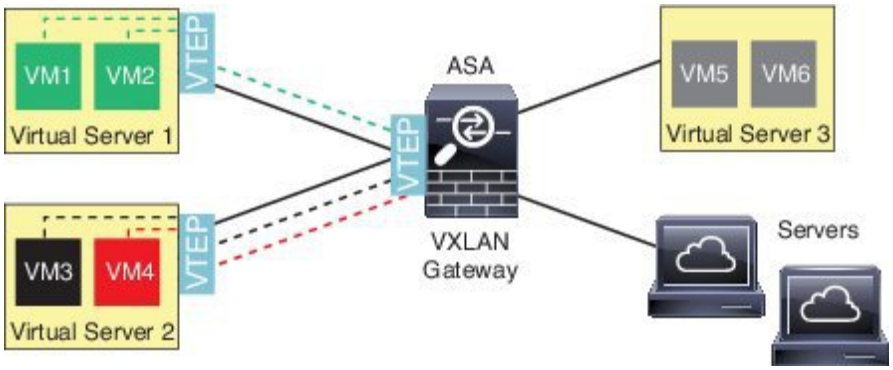
VXLAN 使用例

ここでは、ASA 上への VXLAN の実装事例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

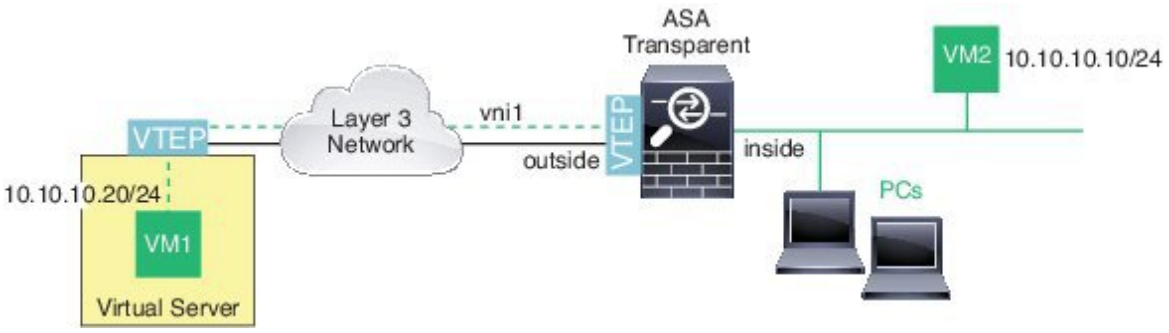
各 ASA の VTEP は、VM、サーバ、PC、VXLAN のオーバーレイ ネットワークなどのエンド ノードの間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイス経由の VXLAN カプセル化を使用して受信された着信フレームの場合は、ASA が VXLAN ヘッダーを抽出して、内部イーサネット フレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続された物理インターフェイスにその着信フレームを転送します。

ASA は、常に VXLAN パケットを処理します。未処理の VXLAN パケットを他の 2 つの VTEP 間でそのまま転送しません。



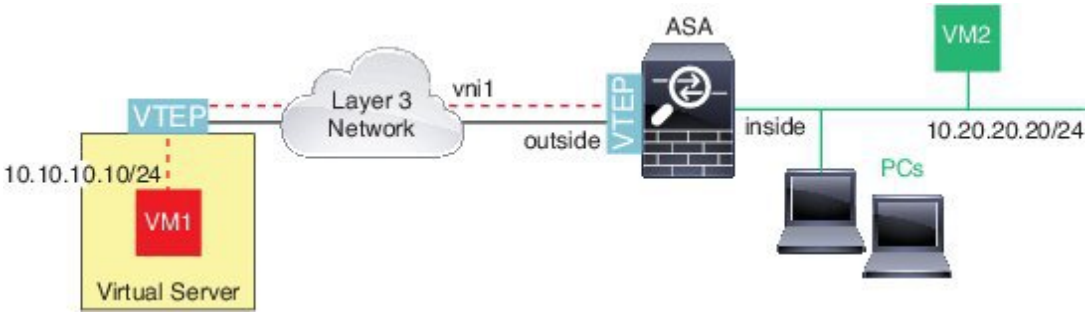
VXLAN ブリッジ

ブリッジグループを使用する場合（トランスペアレント ファイアウォール モードまたは任意ルーテッドモード）、ASAは、同じネットワークに存在するVXLANセグメント（リモート）とローカルセグメント間のVXLANブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス1つのメンバーが通常のインターフェイスで、もう1つのメンバーがVNIインターフェイスです。



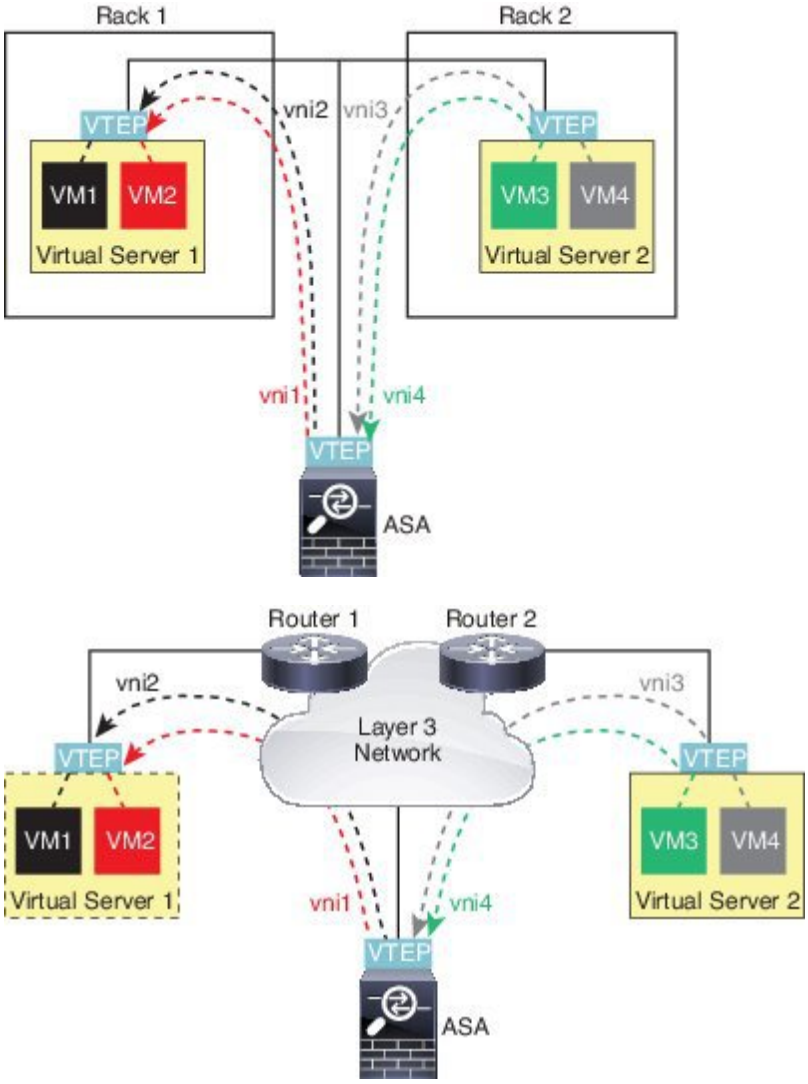
VXLAN ゲートウェイ（ルーテッド モード）

ASAは、VXLANドメインとVXLAN以外のドメインの間のルータとして機能し、異なるネットワーク上のデバイスを接続できます。



VXLAN ドメイン間のルータ

VXLAN拡張レイヤ2ドメインを使用すると、VMは、ASAが同じラックにないとき、あるいはASAがレイヤ3ネットワーク上の離れた場所にあるときに、ゲートウェイとしてASAを指し示すことができます。



このシナリオに関する次の注意事項を参照してください。

1. VM3 から VM1 へのパケットでは、ASA がデフォルト ゲートウェイであるため、宛先 MAC アドレスは ASA の MAC アドレスです。
2. 仮想サーバー 2 の VTEP 送信元インターフェイスは、VM3 からパケットを受信してから、VNI 3 の VXLAN タグでパケットをカプセル化して ASA に送信します。
3. ASA は、パケットを受信すると、パケットをカプセル化解除して内部フレームを取得します。
4. ASA は、ルート ルックアップに内部フレームを使用して、宛先が VNI 2 上であることを認識します。VM1 のマッピングがまだない場合、ASA は VNI 2 カプセル化された ARP ブロードキャストを VNI 2 のマルチキャスト グループ IP で送信します。

(注) このシナリオでは複数の VTEP ピアがあるため、ASA は複数のダイナミック VTEP ピア ディスカバリを使用する必要があります。

5. ASA は VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバー 1 に送信します。カプセル化の前に、ASA は内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします（ASA で VM1 の MAC アドレスを取得するためにマルチキャスト カプセル化 ARP が必要な場合があります）。
6. 仮想サーバー 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

VXLAN インターフェイスのガイドライン

IPv6

- VNI インターフェイスでは、IPv6 トラフィックをサポートしますが、VTEP 送信元インターフェイス IP アドレスでは、IPv4 のみをサポートします。
- IPv6 OSPF インターフェイス設定はサポートされていません。

クラスタリング

- ASA クラスタリングでは、個別インターフェイス モードの VXLAN をサポートしません。Spanned EtherChannel モードでのみ VXLAN をサポートします。

Routing

- VNI インターフェイスでは、スタティック ルーティングまたはポリシー ベース ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。

MTU

- 送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU + 54 バイトに設定する必要があります。この MTU は、ジャンボ フレーム予約を有効にする必要があります。ジャンボフレームサポートの有効化（ASA モデル）（618 ページ） を参照してください。

モデルのガイドライン

- Firepower 1010 スイッチポートおよび VLAN インターフェイスは、VTEP インターフェイスとしてサポートされていません。

VXLAN インターフェイスのデフォルト設定

デフォルトでは、VNI インターフェイスはイネーブルになっています。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

手順

ステップ 1 VTEP 送信元インターフェイスの設定 （666 ページ）。

ステップ 2 VNI インターフェイスの設定 （667 ページ）

VTEP 送信元インターフェイスの設定

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。VXLAN VTEP が現時点でサポートされている NVE です。

始める前に

マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）]** の順に選択し、VTEP 送信元インターフェイスに使用するインターフェイスを編集します。

ステップ 2 （トランスペアレント モード）[VTEP Source Interface] チェック ボックスをオンにします。

この設定により、インターフェイスの IP アドレスを設定することができます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN のみに制限されるルーテッド モードではオプションです。

ステップ 3 送信元インターフェイス名と IPv4 アドレスを設定し、[OK] をクリックします。

ステップ 4 **[構成（Configuration）]>[デバイスの設定（Device Setup）]>[インターフェイス設定（Interface Settings）]>[VXLAN]** の順に選択します。

ステップ 5 （オプション）デフォルト 4789 から変更する場合は、[VXLAN Destination Port] の値を入力します。

マルチ コンテキスト モードでは、システム実行スペースでこの設定を行います。

ステップ 6 [VXLANを使用してネットワーク仮想化エンドポイントのカプセル化を有効にする（Enable Network Virtualization Endpoint encapsulation using VXLAN）] チェックボックスをオンにします。

ステップ 7 ドロップダウン リストから [VTEP Tunnel Interface] を選択します。

（注） VTEP インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。

ステップ 8 （オプション）[Configure Packet Recipient] チェック ボックスをオンにします。

- （マルチ コンテキスト モード（シングル モードではオプション）[Specify Peer VTEP IP Address] を入力して、手動でピア VTEP の IP アドレスを指定します。

  ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

- （シングル モードのみ）[Multicast traffic to default multicast address] を入力して、関連付けられたすべての VNI インターフェイスにデフォルトのマルチキャスト グループを指定します。

  VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

ステップ 9 [Apply] をクリックします。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

手順

ステップ 1 **[構成（Configuration）]>[デバイス設定（Device Setup）]>[インターフェイス設定（Interface Settings）]>[インターフェイス（Interfaces）]**の順に選択し、**[追加（Add）]>[VNIインターフェイス（VNI Interface）]**をクリックします。

ステップ 2 [VNI ID] は 1 ～ 10000 の間で入力します。

この ID は内部インターフェイス識別子です。

ステップ 3 [VNI Segment ID] は 1 ～ 16777215 の間で入力します。

セグメント ID は VXLAN タギングに使用されます。

ステップ 4 （トランスペアレント モード）このインターフェイスを割り当てる [Bridge Group] を指定します。

BVI インターフェイスを設定して通常のインターフェイスをこのブリッジ グループに関連付けるには、のブリッジグループ インターフェイスの設定 （685 ページ）を参照してください。

ステップ 5 [Interface Name] を入力します。

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 6 [Security Level] に 0（最低）～100（最高）を入力します。セキュリティ レベル （676 ページ）を参照してください。

ステップ 7 （シングル モード）[Multicast Group IP Address] を入力します。

VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

ステップ 8 [VTEP トンネルインターフェイスへマッピング（Map to VTEP Tunnel Interface）] チェックボックスをオンにします。

この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 9 [Enable Interface] チェック ボックスをオンにします。この設定はデフォルトでイネーブルになっています。

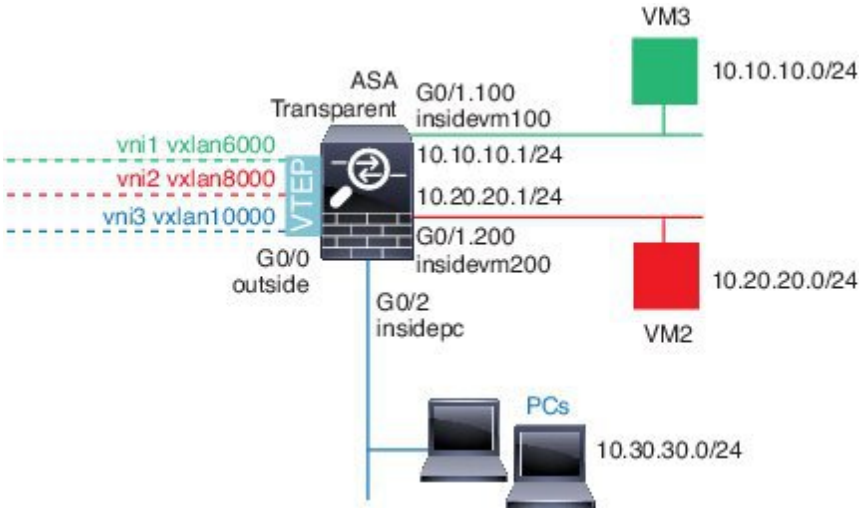
ステップ 10 （ルーテッド モード）[IP Address] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。

ステップ 11 [OK]、続いて [Apply] をクリックします。

VXLAN インターフェイスの例

次の VXLAN の設定例を参照してください。

トランスペアレント VXLAN ゲートウェイの例



この例の次の説明を参照してください。

- GigabitEthernet 0/0 の外部インターフェイスは、VTEP 送信元インターフェイスとして使用され、レイヤ 3 ネットワークに接続されます。
- GigabitEthernet 0/1.100 の insidevm100 VLAN サブインターフェイスは、VM3 が存在する 10.10.10.0/24 ネットワークに接続されます。VM3 が VM1 と通信する場合（表示されません。両方とも、10.10.10.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 6000 を使用します。
- GigabitEthernet 0/1.200 の insidevm200 VLAN サブインターフェイスは、VM2 が存在する 10.20.20.0/24 ネットワークに接続されます。VM2 が VM4 と通信する場合（表示されません。両方とも、10.20.20.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 8000 を使用します。
- GigabitEthernet 0/2 の insidepc インターフェイスは、数台の PC が存在する 10.30.30.0/24 ネットワークに接続されます。それらの PC が、同じネットワーク（すべて 10.30.30.0/24 の IP アドレスを持つ）に属するリモート VTEP の裏の VMs/PCs（表示されません）と通信する場合、ASA は VXLAN タグ 10000 を使用します。

ASA の設定

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
```

```
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

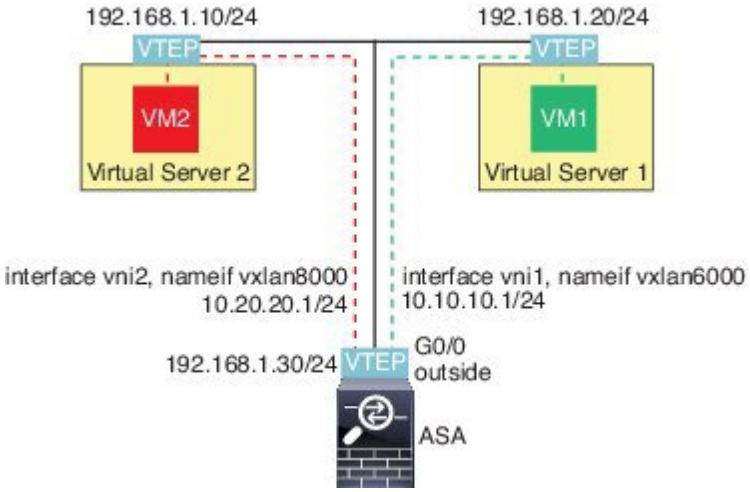
注意

- VNI インタフェース vni1 と vni2 の場合、カプセル化時に内部 VLAN タグが削除されます。
- VNI インターフェイス vni2 と vni3 は、マルチキャストでカプセル化された ARP に対して同じマルチキャスト IP アドレスを共有します。この共有は許可されます。
- ASA は、上記の BVI とブリッジグループ設定に基づいて VXLAN トラフィックを非 VXLAN でサポートされているインターフェイスにブリッジします。拡張されたレイヤ 2 ネット

ワークの各セグメント（10.10.10.0/24、10.20.20.0/24、10.30.30.0/24）の場合、ASA はブリッジとして機能します。

- 複数の VNI または複数の通常のインターフェイス（VLAN または単に物理インターフェイス）をブリッジ グループに設定できます。VXLAN セグメント ID から VLAN ID（物理インターフェイス）の転送または関連付けは、宛先 MAC アドレスによって決定され、どちらかのインターフェイスが宛先に接続されます。
- VTEP 送信元インターフェイスは、インターフェイス設定で **nve-only** によって示されるトランスペアレント ファイアウォール モードのレイヤ 3 インターフェイスです。VTEP 送信元インターフェイスは、BVI インターフェイスまたは管理インターフェイスではありませんが、IP アドレスがあり、ルーティング テーブルを使用します。

VXLAN ルーティングの例



この例の次の説明を参照してください。

- VM1（10.10.10.10）は仮想サーバー 1 にホストされ、VM2（10.20.20.20）は仮想サーバー 2 にホストされます。
- VM1 のデフォルト ゲートウェイは ASA であり、仮想サーバー 1 と同じのポッドにありませんが、VM1 はそれを認識しません。VM1 は、そのデフォルト ゲートウェイの IP アドレスが 10.10.10.1 であることだけを認識します。同様に、VM2 はデフォルト ゲートウェイの IP アドレスが10.20.20.1 であることだけを認識します。
- 仮想サーバー 1 および 2 の VTEP サポート型ハイパーバイザは、同じサブネットまたはレイヤ 3 ネットワーク（表示なし。この場合、ASA と仮想サーバーのアップリンクに異なるネットワーク アドレスがある）経由で ASA と通信できます。
- VM1 のパケットは、そのハイパーバイザの VTEP によってカプセル化され、VXLAN トンネリングを使用してそのデフォルト ゲートウェイに送信されます。

- VM1 がパケットを VM2 に送信すると、パケットはその観点からデフォルト ゲートウェイ 10.10.10.1 を介して送信されます。仮想サーバー 1 は 10.10.10.1 がローカルにないことを認識しているので、VTEP は VXLAN 経由でパケットをカプセル化し、ASA の VTEP に送信します。
- ASA で、パケットはカプセル化解除されます。VXLAN セグメント ID は、カプセル化解除時に取得されます。次に、ASA は、VXLAN セグメント ID に基づいて、VNI インターフェイス（vni1）に対応する内部フレームを再投入します。その後に、ASA はルート ルックアップを実行し、別の VNI インターフェイス（vni2）経由で内部パケットを送信します。vni2 を経由するすべての出力パケットは、VXLAN セグメント 8000 でカプセル化され、VTEP 経由で外部に送信されます。
- 最後に、カプセル化されたパケットが仮想サーバー 2 の VTEP によって受信され、カプセル化解除され、VM2 に転送されます。

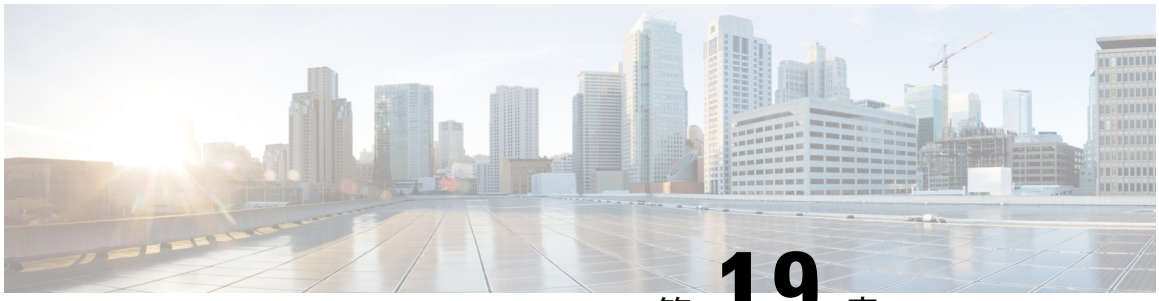
ASA の設定

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN インターフェイスの履歴

表 *30 : VXLAN* インターフェイスの履歴

機能名	リリース	機能情報
VXLAN のサポート	9.4(1)	VXLAN のサポートが追加されました（VXLAN トンネル エンドポイント（VTEP）のサポートを含む）。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface]** **[Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]**



第 19 章

ルーテッド モードおよびトランスペアレント モードのインターフェイス

この章では、ルーテッドまたはトランスペアレント ファイアウォール モードですべてのモデルのインターフェイス設定を完了するためのタスクについて説明します。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

ルーテッドモードインターフェイスとトランスペアレント モード インターフェイスについて

Secure Firewall ASA は、ルーテッドおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ 3 ルーテッド インターフェイスに、固有のサブネット上の IP アドレスが必要です。

ブリッジされたインターフェイスはブリッジグループに属し、すべてのインターフェイスが同じネットワーク上にあります。ブリッジグループはブリッジ ネットワークに IP アドレスを持つブリッジ仮想インターフェイス（BVI）によって表されます。ルーテッド モードは、ルーテッド インターフェイスとブリッジ インターフェイスの両方をサポートし、ルーテッド インターフェイスと BVI との間のルーティングが可能です。トランスペアレント ファイアウォール モードでは、ブリッジ グループと BVI インターフェイスのみがサポートされます。

セキュリティ レベル

ブリッジグループ メンバー インターフェイスを含む各インターフェイスには、0（最下位）～100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。

BVI にセキュリティ レベルを割り当てるかどうかは、ファイアウォール モードに応じて異なります。トランスペアレント モードでは、BVI インターフェイスはインターフェイス間のルーティングに参加しないため、BVI インターフェイスにはセキュリティ レベルが割り当てられていません。ルーテッド モードでは、BVI 間や他のインターフェイスとの間のルーティングを選択した場合、BVI インターフェイスはセキュリティ レベルを所有します。ルーテッド モードでは、ブリッジ グループ メンバー インターフェイスのセキュリティ レベルは、ブリッジ グループ内の通信にのみ適用されます。同様に、BVI のセキュリティ レベルは、BVI/レイヤ 3 インターフェイス通信にのみ適用されます。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。ACL をインターフェイスに適用して、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。

  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

デュアル IP スタック（IPv4 および IPv6）

Secure Firewall ASA は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

31 ビット サブネット マスク

ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバーリンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP または Syslog を実行する管理ステーションを直接接続することもできます。

31 ビットのサブネットとクラスタリング

管理インターフェイスとクラスタ制御リンクを除き、スパンドクラスタリング モードで31 ビットのサブネットマスクを使用できます。

インターフェイス上では、クラスタリングモードで 31 ビットのサブネット マスクを使用できません。

31 ビットのサブネットとフェールオーバー

フェールオーバーに関しては、ASA インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバーインターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、ASA はネットワークのテストを実行できず、リンクステートのみしか追跡できません。

ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。

31 ビットのサブネットと管理

直接接続される管理ステーションがあれば、ASA 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。

31 ビットのサブネットをサポートしていない機能

次の機能は、31 ビットのサブネットをサポートしていません。

- ブリッジ グループ用 BVI インターフェイス - ブリッジ グループには BVI、2 つのブリッジ グループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/ 29 サブネット以下を使用する必要があります。
- マルチキャスト ルーティング

ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項

コンテキスト モード

- マルチ コンテキスト モードで設定できるのは、マルチ コンテキストの設定 （301 ページ）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- トランスペアレント モードのマルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- トランスペアレント モードのマルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。
- DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。
- ルーテッド ファイアウォール モードでは、ブリッジ グループ インターフェイスはマルチ コンテキスト モードでサポートされません。

フェールオーバー

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、「フェールオーバー」の章を参照してください。
- フェールオーバー を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- Secure Firewall ASAは、IPv6 エニーキャスト アドレスはサポートしません。

- DHCPv6 とプレフィックス委任オプションは、マルチ コンテキスト モード、トランスペアレント モードおよびクラスタリングではサポートされません。

モデルのガイドライン

- ASAv50 の場合、ブリッジグループは透過的モードまたはルーテッドモードのいずれでもサポートされません。
- FirePOWER 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。

トランスペアレント モードとブリッジ グループのガイドライン

- 64 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Secure Firewall ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および Secure Firewall ASA を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- ASAv50 の場合、ブリッジグループは透過的モードまたはルーテッドモードのいずれでもサポートされません。
- FirePOWER 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower 1010 では、同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Secure Firewall ASA の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1つのブリッジグループネットワークからの管理トラフィックにだけ

適用されます。これは、デフォルト ルートはブリッジグループのインターフェイスとブリッジグループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジグループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は Management インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、ASA 定義の EtherChannel および VNI インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに「inside」という名前を付けて、明示的にセキュリティ レベルを設定しないと、ASA はセキュリティ レベルを 100 に設定します。

（注） インターフェイスのセキュリティレベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear conn** コマンドを使用して接続をクリアできます。

その他のガイドラインと要件

- ASA では、パケットで 802.1Q ヘッダーが 1 つだけサポートされ、複数のヘッダー（Q-in-Q）はサポートされません。

ルーテッド モードのインターフェイスの設定

ルーテッド モードのインターフェイスを設定するには、次の手順を実行します。

ルーテッド モードの一般的なインターフェイス パラメータの設定

この手順では、名前、セキュリティ レベル、IPv4 アドレス、およびその他のオプションを設定する方法について説明します。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

（注） Firepower 1010 の場合、スイッチポートをルーテッドモードインターフェイスとして設定することはできません。

ステップ 3 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

ステップ 5 （任意）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] チェックボックスをオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

（注） [Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7 IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注） フェールオーバーやクラスタリングの場合は、IPアドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。

  フェールオーバーの場合は、[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブでスタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。

ポイントツーポイント接続の場合、31 ビットのサブネットマスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。この場合、スタンバイ IP アドレスを設定できません。

- DHCP サーバーから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。

1. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

   いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。

2. オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。

3. （任意）DHCP サーバーからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

4. （オプション）アドミニストレーティブディスタンスを既知のルートに割り当てるには、[DHCP Learned Route Metric] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブディスタンスは 1 になります。

5. （任意）DHCP の既知のルートのトラッキングをイネーブルにするには、[Enable Tracking for DHCP Learned Routes] をオンにします。次の値を設定します。

   [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

   [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクスト ホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

   （注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

   [SLA ID]：SLA モニターリング プロセスの一意の識別子。有効な値は 1 ～ 2147483647 です。

   [Monitor Options]：このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニターリング プロセスのパラメータを設定できます。

6. （オプション）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

   DHCP サーバーはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

7. （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

- （シングル モードのみ）PPPoE を使用して IP アドレスを取得するには、[Use PPPoE] をオンにします。

  1. [Group Name] フィールドで、グループ名を指定します。
  2. [PPPoE Username] フィールドで、ISP から提供されたユーザー名を指定します。
  3. [PPPoE Password] フィールドで、ISP から提供されたパスワードを指定します。
  4. [Confirm Password] フィールドに、パスワードを再入力します。
  5. PPP 認証の場合、[PAP]、[CHAP]、または [MSCHAP] のいずれかのオプション ボタンをクリックします。

     PAP は認証時にクリアテキストのユーザー名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリアテキストパスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
  6. （オプション）フラッシュ メモリにユーザー名とパスワードを保存するには、[Store Username and Password in Local Flash] チェック ボックスをオンにします。

     ASA は、NVRAM の特定の場所にユーザー名とパスワードを保存します。Auto Update Server が **clear config** コマンドを ASA に送信して、接続が中断されると、ASA は NVRAM からユーザー名とパスワードを読み取り、アクセス コンセントレータに対して再度認証できます。
  7. （オプション）[PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレッシングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。

ステップ 8 （オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9 [OK] をクリックします。

関連トピック

IPv6 アドレスの設定 （690 ページ）
物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 （616 ページ）
PPPoE の設定 （684 ページ）

PPPoE の設定

インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。

手順

ステップ 1 **[Configuration] > [Interfaces] > [Add/Edit Interface] > [General]** の順に選択し、[PPPoE IP Address and Route Settings] をクリックします。

ステップ 2 [IP Address] 領域で、次のいずれかを選択します。

- [Obtain IP Address using PPP]：IP アドレスを動的に設定します。
- [Specify an IP Address]：IP アドレスを手動で設定します。

ステップ 3 [Route Settings Area] で、次の設定を行います。

- [Obtain default route using PPPoE]：PPPoE クライアントがまだ接続を確立していない場合に、デフォルト ルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。
- [PPPoE learned route metric]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。
- [Enable tracking]：PPPoE の既知のルートのルート トラッキングをイネーブルにします。ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。
- [Primary Track]：プライマリ PPPoE ルート トラッキングを設定します。
- [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。
- [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクスト ホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。
- [SLA ID]：SLA モニターリング プロセスの一意の識別子。有効な値は 1 ～ 2147483647 です。
- [Monitor Options]：このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニターリング プロセスのパラメータを設定できます。
- [Secondary Track]：セカンダリ PPPoE ルート トラッキングを設定します。
- [Secondary Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

ステップ 4 [OK] をクリックします。

のブリッジグループ インターフェイスの設定

ブリッジ グループは、Secure Firewall ASA がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、ブリッジグループについて （247 ページ）を参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVIに名前を指定すると、BVIがルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

一部のモデルでは、デフォルト コンフィギュレーションにブリッジ グループと BVI が含まれています。追加のブリッジグループおよびBVIを作成して、グループの間でメンバーインターフェイスを再割り当てすることもできます。

（注） トランスペアレントモードの個別の管理インターフェイスでは（サポートされているモデルの場合）、設定できないブリッジグループ（ID 301）がコンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

手順

ステップ 1 **[Configuration]** > **[Interfaces]** の順に選択し、**[Add]** > **[Bridge Group Interface]** を選択します。

ステップ 2 [Bridge Group ID] フィールドに、1 ～ 250 の間のブリッジ グループ ID を入力します。

このブリッジ グループ メンバーには、後で物理インターフェイスを割り当てます。

ステップ 3 （ルーテッド モード）[Interface Name] フィールドに、名前を 48 文字以内で入力します。

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジ グループのメンバー）にルーティングする必要がある場合は、BVIに名前を付ける必要があります。

ステップ 4 （ルーテッド モード）[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

ステップ 5 （トランスペアレント モード）IP アドレスを設定します。

a) [IP Address] フィールドに、IPv4 アドレスを入力します。

b) [Subnet Mask] フィールド にサブネット マスクを入力するか、またはメニューから選択します。

トランスペアレント ファイアウォールにホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。ASA は、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約アドレスを割り当てた場合、ASA はダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

ステップ 6 （ルーテッドモード）IPアドレスを設定するには、次のいずれかのオプションを使用します。

フェールオーバーやクラスタリングの場合は、IPアドレスを手動で設定する必要があります。DHCP はサポートされません。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバーから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。

  1. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

     いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。

  2. オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。

  3. （任意）DHCP サーバーからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

  4. （オプション）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

     DHCP サーバーはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

5. （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

ステップ 7 （オプション）[Description] フィールドに、このブリッジ グループの説明を入力します。

ステップ 8 [OK] をクリックします。

ブリッジ仮想インターフェイス（BVI）が、物理およびサブインターフェイスとともに、インターフェイス テーブルに追加されます。

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

この手順は、ブリッジ グループ メンバー インターフェイスの名前、セキュリティ レベル、およびブリッジ グループを設定する方法について説明します。

始める前に

- 同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLANサブインターフェイス、VNIインターフェイス、冗長インターフェイス、EtherChannelインターフェイス）を含めることができます。管理インターフェイスはサポートされていません。 ルーテッド モードでは、EtherChannel と VNI はサポートされません。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- トランスペアレント モードの場合、管理インターフェイスにはこの手順を使用しないでください。管理インターフェイスを設定する場合は、トランスペアレント モードの管理インターフェイスの設定 （688 ページ）を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

BVIは、物理インターフェイス、サブインターフェイス、冗長インターフェイス、EtherChannelポートチャネルインターフェイスとともにテーブルに表示されます。マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2 非 BVI インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

（注） Firepower 1010 では、スイッチポートをブリッジグループメンバーとして設定することはできません。

同じブリッジグループ内に論理 VLAN インターフェイスと物理ルータインターフェイスを混在させることはできません。

（注） ルーテッドモードでは、**port-channel** および **vni** インターフェイスはブリッジグループのメンバーとしてサポートされません。

ステップ 3 [Bridge Group] ドロップダウン メニューで、このインターフェイスを割り当てるブリッジ グループを選択します。

ステップ 4 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

（注） [Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 7 （任意） モジュールを取り付けて非実稼働 ASA 上でモジュール機能をデモンストレーションする場合、[Forward traffic to the ASA module for inspection and reporting] チェック ボックスをオンにします。詳細については、のモジュールに関する章またはクイック スタート ガイドを参照してください。

ステップ 8 （任意） [Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9 [OK] をクリックします。

関連トピック

手動 MAC アドレス、MTU、および TCP MSS の設定 （724 ページ）

トランスペアレント モードの管理インターフェイスの設定

トランスペアレント ファイアウォール モードでは、すべてのインターフェイスがブリッジ グループに属している必要があります。唯一の例外は管理インターフェイス（物理インターフェイス、サブインターフェイス（ご使用のモデルでサポートされている場合）、または管理インターフェイスを構成する EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）です。管理インターフェイスは個別の管理インターフェイスとして設定できます。Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイスに基づいています。他のインターフェイス タイプ

は管理インターフェイスとして使用できません。シングル モードまたはコンテキストごとに1つの管理インターフェイスを設定できます。詳細については、トランスペアレントモードの管理インターフェイス （612 ページ）を参照してください。

始める前に

- このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジグループ（ID 301）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。
- Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。
- マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。データ インターフェイスに接続する必要があります。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 管理インターフェイス、サブインターフェイス、または管理インターフェイスからなる EtherChannel ポートチャネル インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイス（個別インターフェイスまたは EtherChannel インターフェイス）に基づいています。

ステップ 3 [Bridge Group] ドロップダウン メニューで、デフォルトの [--None--] のままにします。管理インターフェイスをブリッジ グループに割り当てることはできません。

ステップ 4 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

（注） [Dedicate this interface to management only] チェックボックスは、デフォルトでイネーブルであり、設定することはできません。

ステップ 6 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7 IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注） フェールオーバーとともに使用する場合は、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバーから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。
  - MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

    いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。
  - オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。
  - （任意）DHCP サーバーからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。
  - （オプション）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

    DHCP サーバーはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。
  - （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

ステップ 8 （オプション）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 9 [OK] をクリックします。

IPv6 アドレスの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、Secure Firewall ASA が自動的にメンバー インターフェイスのリンクローカル アドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカルアドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。Secure Firewall ASAでは、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。

IPv6 プレフィックス委任クライアントの設定

ASA は、クライアント インターフェイス（たとえば、ケーブル モデムに接続された外部インターフェイス）が 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASA はそのプレフィックスを内部インターフェイスをサブネット化および指定することができます。

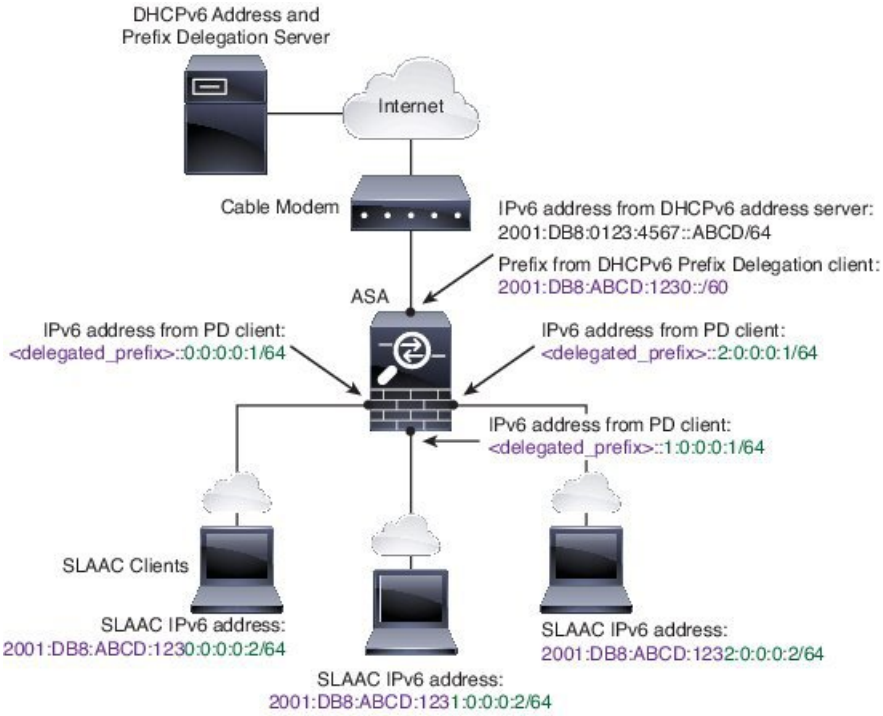
IPv6 プレフィックス委任の概要

ASA は、クライアント インターフェイス（たとえば、ケーブル モデムに接続された外部インターフェイス）が 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASA はそのプレフィックスを内部インターフェイスをサブネット化および指定することができます。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration（SLAAC）を使用してグローバル IPv6 アドレスを取得できます。ただし、内部 ASA インターフェイスはプレフィックス委任サーバーとして機能しませんのでご注意ください。ASA は、SLAAC クライアントにグローバル IP アドレスを提供することしかできません。たとえば、ルータが ASA に接続されている場合、ASA は SLAAC クライアントとして機能し、IP アドレスを取得できます。しかし、ルータの背後のネットワークに代理プレフィックスのサブネットを使用したい場合、ルータの内部インターフェイス上でそれらのアドレスを手動で設定する必要があります。

ASA には光 DHCPv6 サーバーが含まれており、SLAAC クライアントが Information Request（IR）パケットを ASA に送信した場合、ASA は DNS サーバーやドメイン名などの情報を SLAAC クライアントに提供することができます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

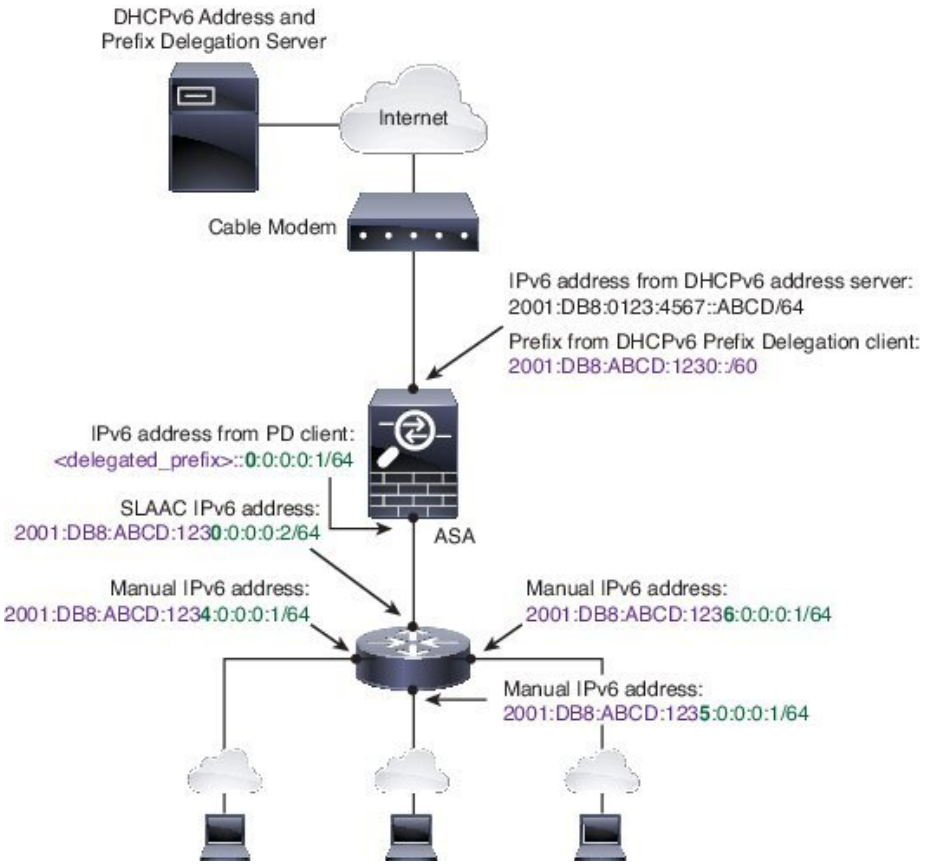
IPv6 プレフィックス委任 /64 サブネットの例

次の例では、ASA が DHCPv6 アドレス クライアントを使用して、外部インターフェイス上で IP アドレスを受け取るところを示しています。また、ASA は DHCPv6 プレフィックス委任クライアントを使用して代理プレフィックスを取得します。ASA は、代理プレフィックスを /64 ネットワークにサブネット化し、代理プレフィックスおよび手動で設定されたサブネット（::0, ::1, or ::2）と各インターフェイスごとの IPv6 アドレス（0:0:0:1）を使用して、動的に内部インターフェイスにグローバル IPv6 アドレスを指定します。これらの内部インターフェイスに接続されている SLAAC クライアントは、各 /64 サブネットの IPv6 アドレスを取得します。



IPv6 プレフィックス委任 /62 サブネットの例

次の例は、ASA が 4/62 サブネットにプレフィックスをサブネット化するところを示しています。2001:DB8:ABCD:123**0**::/62, 2001:DB8:ABCD:123**4**::/62, 2001:DB8:ABCD:123**8**::/62, and 2001:DB8:ABCD:123**C**::/62。ASA は、内部ネットワーク（::0）に 2001:DB8:ABCD:1230::/62 の利用可能な 4 つの 64 サブネットのうちの 1 つを使用します。ダウンストリーム ルータには、手動で追加の /62 サブネットを使用できます。図のルータは、内部インターフェイス（::4, ::5, and ::6）に 2001:DB8:ABCD:1234::/62 の利用可能な 4 つの /64 サブネットのうちの 3 つを使用します。この場合、内部ルータ インターフェイスは動的に代理プレフィックスを取得することはできないため、ASA 上で代理プレフィックスを表示し、ルータ設定にそのプレフィックスを使用する必要があります。通常、リースが期限切れになった場合、ISP は既定のクライアントに同じプレフィックスを委任しますが、ASA が新しいプレフィックスを受け取った場合、新しいプレフィックスを使用するようルータ設定を変更する必要があります。



IPv6 プレフィックス委任クライアントの有効化

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

始める前に

- この機能は、ルーテッド ファイアウォール モードに限りサポートされています。
- この機能はマルチ コンテキスト モードではサポートされません。
- この機能は、クラスタリングではサポートされていません。
- この機能は管理専用インターフェイスでは設定できません。
- プレフィックス委任を使用する場合は、IPv6 トラフィックの中断を防ぐために、ASA IPv6 ネイバー探索のルータ アドバタイズメント間隔を DHCPv6 サーバーによって割り当てられるプレフィックスの推奨有効期間よりもはるかに小さい値に設定する必要があります。たとえば、DHCPv6 サーバーがプレフィックス委任の推奨有効期間を 300 秒に設定してい

る場合は、ASA RA の間隔を 150 秒に設定する必要があります。推奨有効期間を設定するには、**show ipv6 general-prefix** コマンドを使用します。ASA RA の間隔を設定するには、IPv6 ネイバー探索の設定 （700 ページ）を参照してください。デフォルトは 200 秒です。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 [Interface IPv6 DHCP] エリアで、[Client Prefix Delegation Name] ラジオボタンをクリックして、プレフィックス名を入力します。

ステップ 5 （任意） [Prefix Hint] フィールドで、受信する委任されたプレフィックスに関する 1 つ以上のヒントを提供します。

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合には、そのプレフィックスの全体をヒントとして入力できます（2001:DB8:ABCD:1230::/60）。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバーによって決定されます。

ステップ 6 [OK] をクリックします。

[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインに戻ります。

ステップ 7 [Apply] をクリックします。

ステップ 8 ASA インターフェイスのグローバル IP アドレスとしてプレフィックスのサブネットを割り当てるには、グローバル IPv6 アドレスの設定 （695 ページ） を参照してください。

ステップ 9 （任意） SLAAC クライアントにドメイン名とサーバー パラメータを提供するには、DHCPv6 ステートレス サーバーの設定 （779 ページ） を参照してください。

ステップ 10 （任意） BGP でプレフィックスをアドバタイズするには、IPv6 ネットワークの設定 （919 ページ） を参照してください。

グローバル IPv6 アドレスの設定

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

サブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。手動 MAC アドレス、MTU、および TCP MSS の設定 （724 ページ）を参照してください。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

トランスペアレント モード、またはルーテッド モードのブリッジ グループの場合、BVI を選択します。トランスペアレントモードの場合は、管理専用インターフェイスも選択できます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 [Enable IPv6] チェックボックスをオンにします。

ステップ 5 （任意）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

ステップ 6 （ルーテッド インターフェイス）グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- ステートレス自動設定：[Interface IPv6 Addresses] 領域で、[Enable address autoconfiguration] チェックボックスをオンにします。

  インターフェイス上でステートレス自動設定を有効にすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定が有効になっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

（注） RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定していますが、ASA はこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、[Suppress RA] チェックボックスをオンにします。

デフォルト ルートをインストールする場合は、ドロップダウン メニューから [DHCP] または [Ignore] を選択します。[DHCP] を指定すると、ASA は信頼できる送信元から（言い換えると、IPv6 アドレスを提供した同じサーバーから）取得されたルータ アドバタイズメントからのデフォルト ルートのみを使用します。[Ignore] を指定すると、別のネットワークからルータ アドバタイズメントを取得できるようになります（この方法では、リスクが高くなる可能性があります）。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

1. [Interface IPv6 Addresses] 領域で、[Add] をクリックします。

   [Add IPv6 Address for Interface] ダイアログボックスが表示されます。

2. [Address/Prefix Length] フィールドに入力する値は、使用する方法によって異なります。

   - 完全なグローバルアドレス：手動でアドレス全体を入力する場合は、完全なアドレスに加え、プレフィックス長を入力します。
   - Modified EUI 64 形式：IPv6 プレフィックスとプレフィックス長を入力した後、[EUI 64] チェックボックスをオンにします。これにより、Modified EUI 64 形式を使用してインターフェイス ID が生成されるようになります。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。
   - 委任されたプレフィックス：委任されたプレフィックスから IPv6 プレフィックスを生成するには、IPv6 アドレスとプレフィックス長を入力します。次に、DHCPv6 プレフィクス委任クライアントに設定したプレフィックス名（IPv6 プレフィックス委任クライアントの有効化 （694 ページ）を参照）を [Prefix Name] フィールドに入力してから、[Add] をクリックします。

     通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

3. [OK] をクリックします。

- DHCPv6 を使用してアドレスを取得します。
  1. [Interface IPv6 DHCP] 領域で、[Enable DHCP] チェックボックスをオンにします。
  2. （オプション）ルータ アドバタイズメントからデフォルト ルータを取得する場合は、[Enable Default] チェックボックスをオンにします。

ステップ 7 （BVIインターフェイス）BVIに手動でグローバルアドレスを割り当てます。トランスペアレント モードの管理インターフェイスでも、この方法を使用します。

a) [Interface IPv6 Addresses] 領域で、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

b) [Address/Prefix Length] フィールドに、完全なグローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。

c) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインに戻ります。

（オプション）リンクローカル アドレスの自動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカルアドレスをインターフェイスのMACアドレスに基づいて作成することもできます（Modified EUI-64 形式。MACアドレスで使用するビット数は48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります）。

リンクローカル アドレスをインターフェイスに自動的に設定するには、次の手順を実行します。

始める前に

ルーテッド モードのみでサポートされます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ルーテッド モードのブリッジグループの場合は、BVI を選択します。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 [IPv6 configuration] 領域で、[Enable IPv6] チェック ボックスをオンにします。

このオプションでは、IPv6 をイネーブルにし、インターフェイスの MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカル アドレスを自動的に生成します。

ルーテッド モードのブリッジグループでは、BVI に対して IPv6 を有効にすると、すべてのメンバー インターフェイスのリンクローカル アドレスが生成されます。

ステップ 5 [OK] をクリックします。

（オプション）リンクローカル アドレスの手動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカル アドレスによりパケットがドロップされることがあります。

インターフェイスにリンクローカル アドレスを割り当てるには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ブリッジグループの場合は、ブリッジグループ メンバー インターフェイスを選択します。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 （任意）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

ステップ 5 リンクローカル アドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。たとえば fe80::20d:88ff:feee:6a82 のようになります。IPv6 アドレッシングの詳細については、IPv6 アドレス （1367 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

-

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 IPv6 ネイバーの設定を行う IPv6 インターフェイスを選択し、[Edit] をクリックします。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 許可される [DAD Attempts] の回数を入力します。

値の範囲は 0 ～ 600 です。この値が 0 の場合、指定されたインターフェイスでの DAD 処理が無効化されます。デフォルト値は 1 件です。

DAD は、割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンク ベースで確認します。Secure Firewall ASA は、ネイバー送信要求メッセージを使用して、DAD を実行します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

ステップ 5 [NS Interval]（ミリ秒単位）に入力して、IPv6 ネイバー要請メッセージの再送信間隔を設定します。

value 引数の有効な値は、1000 ～ 3600000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャスト アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

ステップ 6 [Reachable Time]（秒単位）に入力して、リモート IPv6 ノードに到達可能な時間を設定します。

到達可能時間を 0 ～ 3600000 ミリ秒で設定します。時間を 0 に設定すると、到達可能時間は「不明」として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 7 [RA Lifetime]（秒単位）に入力して、ローカル リンク上のノードが、ASA をリンク上のデフォルト ルータと見なす時間の長さを設定します。

値の範囲は 0 ～ 9000 秒です。0 を入力すると、ASA は選択したインターフェイスのデフォルト ルータと見なされません。

ステップ 8 ルータ アドバタイズメントを抑制するには、[Suppress RA] チェックボックスをオンにします。

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

Secure Firewall ASA で IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージをディセーブルにできます。

このオプションを有効にすると、ASA がリンク上では IPv6 ルータではなく、通常の IPv6 ネイバーのように見えるようになります。

ステップ 9 [RA Interval] に入力して、IPv6 ルータ アドバタイズメントの送信間隔を設定します。

有効値の範囲は 3 ～ 1800 秒です。デフォルトは 200 秒です。

ルータ アドバタイズメント送信間隔の値をミリ秒単位で追加するには、[RA Interval in Milliseconds] チェックボックスをオンにして、500 ～ 1800000 の範囲で値を入力します。

ステップ 10 [Hosts should use DHCP for address config] チェックボックスをオンにして、取得されるステートレス自動設定のアドレス以外のアドレスの取得には DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

このオプションは、IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定します。

ステップ 11 [Hosts should use DHCP for non-address config] チェックボックスをンにして、DNS サーバー アドレスなどの追加情報を DHCPv6 から取得するには DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

このオプションは、IPv6 ルータ アドバタイズメント パケットのその他のアドレス設定フラグを設定します。

ステップ 12 IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。

a) [Interface IPv6 Prefixes] 領域で、[Add] をクリックします。

b) デフォルトのプレフィックスを使用するには、[Address/Prefix Length] に入力するか、[Default] チェック ボックスをオンにします。

c) IPv6 アドレスを手動で設定するようにホストに強制するには、[No Auto-Configuration] チェックボックスをオンにします。指定したプレフィックスのローカル リンク上のホストでは、IPv6 自動設定を使用できません。

d) プレフィックス アドバタイズメントを無効にするには、[No Advertisements] チェックボックスをオンにします。

e) 指定したプレフィックスをオフリンクとして設定するには、[Off Link] チェック ボックスをオンにします。プレフィクスはLビットクリアでアドバタイズされます。プレフィックスは、接続されたプレフィックスとしてルーティング テーブルに挿入されません。

f) [Prefix Lifetime] 領域で、[Lifetime Duration] または [Lifetime Expiration Date] を指定します。

優先有効期間を過ぎると、アドレスは廃止状態になります。廃止状態のアドレスの使用は推奨さませんが、固く禁じられているわけではありません。有効期間の期限が切れた後に、アドレスは無効になり、使用できません。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。

- [Lifetime Duration]：値の範囲は 0 ～ 4294967295 です。デフォルトの有効期間は 2592000（30 日間）です。デフォルトの優先有効期間は 604800（7 日間）です。最大値は無限大です。
- [Lifetime Expiration Date]：有効かつ優先する月と日をドロップダウンリストから選択し、時間を hh:mm 形式で入力します。

g) [OK] をクリックして設定内容を保存します。

ステップ 13 [OK] をクリックします。

ステップ 14 スタティック IPv6 ネイバーを設定します。

次のガイドラインと制限事項は、スタティック IPv6 ネイバーの設定に適用されます。

- この機能は、スタティック ARP エントリの追加に似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。これらのエントリは、copy コマンドを使用して設定を保存するときに設定に保存されます。
- IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

- 生成された ICMP syslog は、IPv6 ネイバー エントリの定期的な更新に起因します。IPv6 ネイバー エントリの ASA デフォルト タイマーは 30 秒であるため、ASA は 30 秒おきに ICMPv6 ネイバー探索および応答パケットを生成します。ASA にフェールオーバー LAN および IPv6 アドレスで設定された状態インターフェイスの両方がある場合は、30 秒ごとに、ICMPv6 ネイバー探索および応答パケットが、設定済みのリンクローカル IPv6 アドレスの 両方の ASA で生成されます。また、各パケットは複数の syslog（ICMP 接続およびローカル ホストの作成またはティアダウン）を生成するため、連続 ICMP syslog が生成されているように見えることがあります。IPV6 ネイバー エントリのリフレッシュ時間は、通常のデータ インターフェイスに設定可能ですが、フェールオーバー インターフェイスでは設定可能ではありません。ただし、この ICMP ネイバー探索トラフィックの CPU の影響はわずかです。

ダイナミックに検出されたネイバーの表示とクリア （703 ページ）も参照してください。

a) [Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache] を選択します。
b) [Add] をクリックします。

   [Add IPv6 Static Neighbor] ダイアログボックスが表示されます。

c) [Interface Name] ドロップダウン リストから、ネイバーを追加するインターフェイスを選択します。
d) [IP Address] フィールドにローカル データリンク アドレスに対応する IPv6 アドレスを入力するか、省略符号（[...]）をクリックしてアドレスを参照します。
e) [MAC address] フィールドに、ローカルのデータ回線（ハードウェア）MAC アドレスを入力します。
f) [OK] をクリックします。

ステップ 15 [Apply] をクリックして、実行コンフィギュレーションを保存します。

ダイナミックに検出されたネイバーの表示とクリア

ホストまたはノードがネイバーと通信する場合、ネイバーはネイバー探索キャッシュに追加されます。ネイバーがキャッシュから削除されるのは、そのネイバーとの通信が行われなくなったときです。

ダイナミックに検出されたネイバーを表示し、そのネイバーを IPv6 ネイバー探索キャッシュから削除するには、次の手順を実行します。

手順

ステップ 1 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache] を選択します。

[IPv6 Neighbor Discovery Cache] ペインでは、スタティックおよびダイナミックに検出されたネイバーをすべて表示できます。

ステップ 2 ダイナミックに検出されたネイバーをすべてキャッシュから削除するには、[Clear Dynamic Neighbor Entries] をクリックします。

ダイナミックに検出されたネイバーがキャッシュから削除されます。

（注） この手順では、ダイナミックに検出されたネイバーだけがキャッシュから削除され、スタティックなネイバーは削除されません。

ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニターリング

インターフェイスの統計情報、ステータス、PPPoE などをモニターできます。

（注） プラットフォームモードの Firepower 2100 および Firepower 4100/9300 の場合、一部の統計情報は ASA コマンドを使用して表示されません。FXOS コマンドを使用して、より詳細なインターフェイス統計情報を表示する必要があります。 これらのコマンドは、アプライアンスモードの Firepower 1000 および 2100 にも役立ちます。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

プラットフォームモードの Firepower 2100 の場合は、次の FXOS connect local-mgmt コマンドも参照してください。

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

詳細については、『FXOS troubleshooting guide』を参照してください。

インターフェイス統計情報

- **[Monitoring] > [Interfaces] > [Interface Graphs]**

  インターフェイスの統計情報をグラフ形式またはテーブル形式で表示できます。インターフェイスをコンテキスト間で共有している場合、ASA には現在のコンテキストの統計情報だけが表示されます。サブインターフェイスに表示される統計情報の数は、物理インターフェイスに表示される統計情報の数のサブセットです。

- **[Monitoring] > [Interfaces] > [Interface Graphs] > [Graph/Table]**

選択した統計情報のグラフを表示します。[Graph] ウィンドウには、最大 4 つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。履歴メトリックをイネーブルにすると、過去の期間の統計情報を表示できます。

DHCP Information

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Client Lease Information]**

  この画面には、設定されている DHCP クライアントの IP アドレスが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Client PD Statistics]**

  この画面は DHCPv6 プレフィックス委任クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Client Statistics]**

  この画面は DHCPv6 クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Interface Statistics]**

  この画面は、すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバー構成用に設定されている場合（DHCPv6 ステートレス サーバーの設定 （779 ページ） を参照）、この画面はサーバーによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、この画面は各クライアントの状態とサーバーから受信した値を表示します。この画面は、DHCP サーバーまたはクライアントのメッセージの統計情報も表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP HA Statistics]**

  この画面は、DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバー ユニット間のトランザクションの統計情報を表示します。

スタティック ルート トラッキング

- **[Monitoring] > [Interfaces] > [interface connection] > [Track Status]**

  追跡対象オブジェクトに関する情報を表示します。

- **[Monitoring] > [Interfaces] > [interface connection] > [Monitoring Statistics]**

  SLA モニターリング プロセスの統計情報を表示します。

PPPoE

- [Monitoring] > [Interfaces] > [PPPoE Client] > [PPPoE Client Lease Information]

  現在の PPPoE 接続に関する情報を表示します。

ダイナミック ACL

[Monitoring] > [Interfaces] > [Dynamic ACLs]

ダイナミック ACL のテーブルを表示します。ダイナミック ACL は、ASA によって自動的に作成、アクティブ化、および削除される点を除いて、ユーザー設定の ACL と機能上同じです。これらの ACL はコンフィギュレーションには表示されず、このテーブルだけに表示されます。ダイナミック ACL は、ACL ヘッダーの “(dynamic)” キーワードで区別されます。

ルーテッドモードおよびトランスペアレントモードのインターフェイスの例

2 つのブリッジグループを含むトランスペアレント モードの例

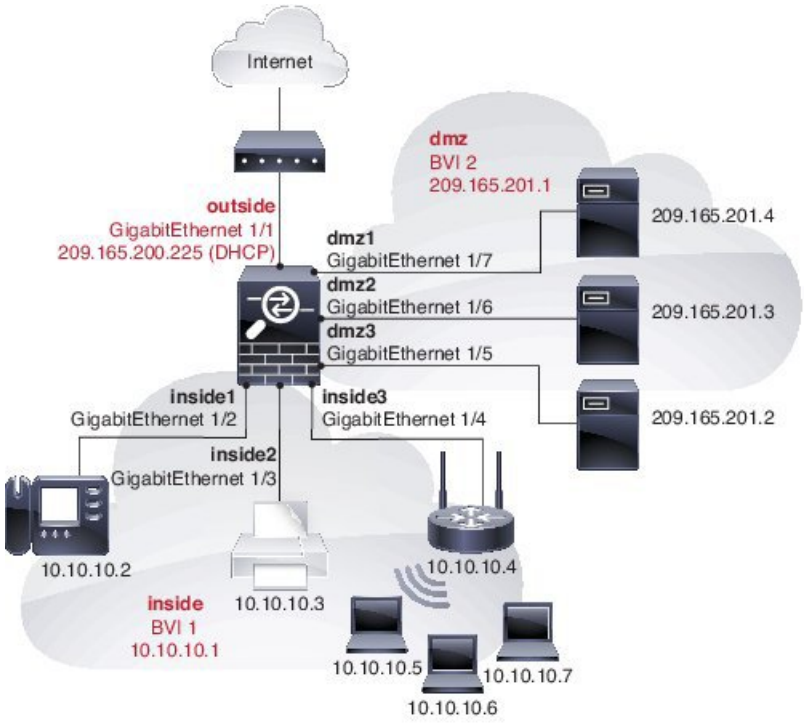
トランスペアレント モードの次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジグループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
```

```
interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

2 つのブリッジグループを含むスイッチド LAN セグメントの例

次の例では、3 つのインターフェイスのそれぞれと 1 つの通常の外部用ルーテッド インターフェイスに 2 つのブリッジグループを設定します。ブリッジグループ 1 は内部であり、ブリッジグループ 2 はパブリック Web サーバーが設定された dmz です。ブリッジグループのメンバー インターフェイスは、各メンバーのセキュリティ レベルが等しく、同一のセキュリティ通信が可能になっているため、ブリッジグループ内で自由に通信できます。内部メンバーのセキュリティ レベルが 100 で、dmz メンバーのセキュリティ レベルも 100 ですが、これらのセキュリティ レベルは BVI 間通信には適用されません。BVI のセキュリティ レベルのみ、BVI 間のトラフィックに影響します。BVI と外部のセキュリティ レベル（100、50、および 0）は、内部から dmz と内部から外部、および dmz から外部へのトラフィックを暗黙的に許可します。dmz 上のサーバーに対するトラフィックを許可するために、アクセス ルールが外部に適用されます。




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
```

```
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
```

```
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴

機能名	プラットフォームリリース	機能情報
IPv6 ネイバー探索	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache.Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache.Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [IPv6]。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。

機能名	プラットフォームリリース	機能情報
トランスペアレントモードのブリッジグループ	8.4(1)	セキュリティコンテキストのオーバーヘッドを避けたい場合、またはセキュリティコンテキストを最大限に使用したい場合、インターフェイスをブリッジグループにグループ化し、各ネットワークに1つずつ複数のブリッジグループを設定できます。ブリッジグループのトラフィックは他のブリッジグループから隔離されます。シングルモードまたはコンテキストごとに、それぞれ4つのインターフェイスからなる最大8個のブリッジグループを設定できます。 次の画面が変更または導入されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	次の画面が変更されました。 [Configuration] > [Device Setup] > [Interfaces] > [IPv6]。

機能名	プラットフォームリリース	機能情報
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	ブリッジグループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジグループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]**
トランスペアレントモードで、ブリッジグループごとのインターフェイス数が最大で 64 に増加	9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更された画面はありません。

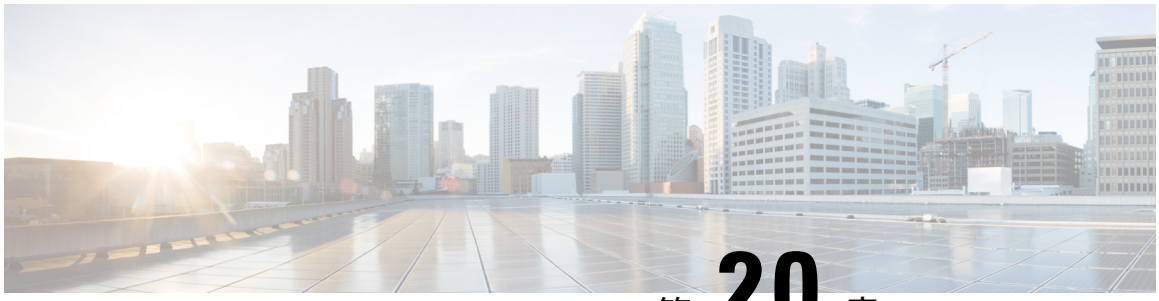
機能名	プラットフォームリリース	機能情報
IPv6 DHCP	9.6(2)	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバーから IPv6 グローバルアドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバー：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次の画面が追加または変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [IPv6]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Pool]** **[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] > [Networks]** **[Monitoring] > [interfaces] > [DHCP]**

機能名	プラットフォームリリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	

機能名	プラットフォームリリース	機能情報
		Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジグループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定するASA上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVIは名前付きインターフェイスとなり、アクセスルールやDHCPサーバーなどの一部の機能に、メンバーインターフェイスとは個別に参加できます。 トランスペアレントモードでサポートされるマルチ コンテキスト モードやASAクラスタリングの各機能は、ルーテッド モードではサポートされません。マルチキャストルーティングとダイナミック ルーティングの機能も、

機能名	プラットフォームリリース	機能情報
		BVI ではサポートされません。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Server]** **[Configuration]** > **[Firewall]** > **[Access Rules]** **[Configuration]** > **[Firewall]** > **[EtherType Rules]**

機能名	プラットフォームリリース	機能情報
31 ビット サブネット マスク	9.7(1)	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの31 ビットのサブネット に IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバー リンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループ用の BVI、またはマルチキャストルーティングではサポートされていません。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add Interface]** > **[General]**



第 20 章

高度なインターフェイス設定

この章では、インターフェイスのMACアドレスを設定する方法、最大伝送ユニット（MTU）を設定する方法、TCP最大セグメントサイズ（TCP MSS）を設定する方法、および同じセキュリティ レベルの通信を許可する方法について説明します。最高のネットワーク パフォーマンスを実現するには、正しい MTU と最大 TCP セグメント サイズの設定が不可欠です。

インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。。

（注） 親インターフェイスと同じ組み込みのMACアドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスはMACアドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010）：ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。手動 MAC アドレス、MTU、および TCP MSS の設定 （724 ページ）を参照してください。

  トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。手動 MAC アドレス、MTU、および TCP MSS の設定（724 ページ）を参照してください。
- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバー インターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。
- EtherChannel（Firepower Models）：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel（ASA モデル）：ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイス メンバーシップが変更された場合に備えて、一意の MAC アドレスを構成することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成が有効になっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効な場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

MTU について

MTU は、Secure Firewall ASA が特定のイーサネット インターフェイスで送信可能な最大フレームペイロードサイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば MTU を 1500 に設定した場合、想定されるフレーム サイズはヘッダーを含めて 1518 バイト、VLAN を使用する場合は 1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

VXLAN については、イーサネット データグラム全体がカプセル化されるため、新しい IP パケットは大きくなり、より大きな MTU が必要となります。そのため、ASA VTEP 送信元インターフェイスをネットワーク MTU + 54 バイトに設定する必要があります。

パス MTU ディスカバリ

Secure Firewall ASA は、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

Secure Firewall ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッド分の 18～22 バイトは含まれません。

VTEP 送信元インターフェイスの VXLAN を有効にし、MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。一般的には、ASA 送信元インターフェイス MTU をネットワーク MTU + 54 バイトに設定する必要があります。

MTU およびフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

TCP パケットでは、通常、エンドポイントは MTU を使用して TCP の最大セグメント サイズを決定します（MTU - 40 など）。途中で追加の TCP ヘッダーが追加された場合（たとえば、サイト間 VPN トンネル）、TCP MSS はトンネリング エンティティで下方調整しないといけない場合があります。 TCP MSS について （721 ページ）を参照してください。

UDP または ICMP の場合、アプリケーションではフラグメント化を避けるために MTU を考慮する必要があります。

（注） Secure Firewall ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信できます。

MTU とジャンボ フレーム

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。

- ジャンボ フレームへの対応：ジャンボ フレームが有効な場合、MTU を最大 9198 バイトに設定できます。最大値は、Firepower 4100/9300 シャーシ の ASAv で 9000、ASA で 9184 です。

TCP MSS について

最大セグメント サイズ（TCP MSS）とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバーは TCP MSS 値を交換します。

デフォルトで、最大 TCP MSS は 1380 バイトに設定されます。この設定は、Secure Firewall ASA が IPsec VPN カプセル化のパケットサイズを大きくする必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、Secure Firewall ASA の最大 TCP MSS を無効化する必要があります。

最大 TCP MSS を設定すると、接続のいずれかのエンドポイントが Secure Firewall ASA で設定した値よりも大きな TCP MSS を要求した場合に、Secure Firewall ASA は要求パケットの TCP MSS を Secure Firewall ASA の最大値で上書きします。ホストやサーバが TCP MSS を要求しない場合、Secure Firewall ASA は RFC 793 のデフォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットを変更することはありません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。Secure Firewall ASA の最大 TCP MSS が 1380（デフォルト）の場合は、Secure Firewall ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。Secure Firewall ASA はさらに 120 バイトのヘッダーをパケットに追加しますが、それでも 1500 の MTU サイズに収まります。

TCP の最小 MSS も設定できます。ホストまたはサーバーが非常に小さい TCP MSS を要求した場合、Secure Firewall ASAは値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。Secure Firewall ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40（IPv4）または MTU - 60（IPv6）となります。

デフォルト TCP MSS

デフォルトでは、Secure Firewall ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU のデフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、Secure Firewall ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。Secure Firewall ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして Secure Firewall ASA を使用しない場合は、

次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。一般に接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

インターフェイス間通信

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。

  各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

- ACL がなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

インターフェイス内通信（ルーテッド ファイアウォール モード）

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブアンドスポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

マルチコンテキストモードでのMACアドレスの自動割り当て

この項では、MAC アドレスの自動生成の設定方法について説明します。マルチ コンテキスト モードの場合、この機能によって、コンテキストに割り当てられたすべてのインターフェイス タイプに一意の MAC アドレスが割り当てられます。

始める前に

- インターフェイスの名前を設定すると、ただちに新規 MAC アドレスが生成されます。インターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 システムで次の手順を実行します。

a) **[Configuration]** > **[Context Management]** > **[Security Contexts]** の順に選択します。
b) [Mac-Address auto] をオンにします。
c) （任意） [Prefix] チェックボックスをオンにしてから、フィールドに 0 ～ 65535 の範囲内の 10 進数値を入力します。

このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 2 [Apply] をクリックします。

手動 MAC アドレス、MTU、および TCP MSS の設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 MTU を設定する場合、またはジャンボ フレームのサポートをイネーブルにする場合（サポート対象モデルのみ）、[MTU] フィールドに 300 ～ 9198（ASAv の場合は 9000、Firepower 4100/9300 シャーシ の場合は 9188）バイトの範囲で値を入力します。

デフォルトは 1500 バイトです。

（注） 冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

- ジャンボ フレームをサポートする、シングル モードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボ フレーム サポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボ フレーム サポートがディセーブルになります。
- ジャンボ フレームをサポートするマルチ モードの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合、必ずシステム コンフィギュレーションのジャンボ フレーム サポートをイネーブルにしてください。ジャンボフレームサポートの有効化（ASA モデル） （618 ページ）を参照してください。

（注） ジャンボ フレーム サポートをイネーブルまたはディセーブルにするには、ASA をリロードする必要があります。

ステップ 5 MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6 フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 7 TCP MSS を設定するには、**[設定（Configuration）]** > **[ファイアウォール（Firewall）]** > **[詳細（Advanced）]** > **[TCPオプション（TCP Options）]** の順に選択します。次のオプションを設定できます。

- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。
- [Force Minimum Segment Size for TCP]：48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 8 [Secure Group Tagging] 設定については、ファイアウォール コンフィギュレーション ガイドを参照してください。

ステップ 9 [ASA Cluster] 設定については、（推奨、マルチコンテキストモードでは必須）制御ユニットでのインターフェイスの設定 （427 ページ）を参照してください。

同一のセキュリティ レベル通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

手順

ステップ 1 同じセキュリティ レベルのインターフェイス間の通信を有効にするには、**[Configuration]** > **[Interfaces]** ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。

ステップ 2 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

ARP および MAC アドレス テーブルのモニターリング

- **[Monitoring] > [Interfaces] > [ARP Table]**

スタティック エントリやダイナミック エントリを含む ARP テーブルを表示します。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

- **[Monitoring] > [Interfaces] > [MAC Address Table]**

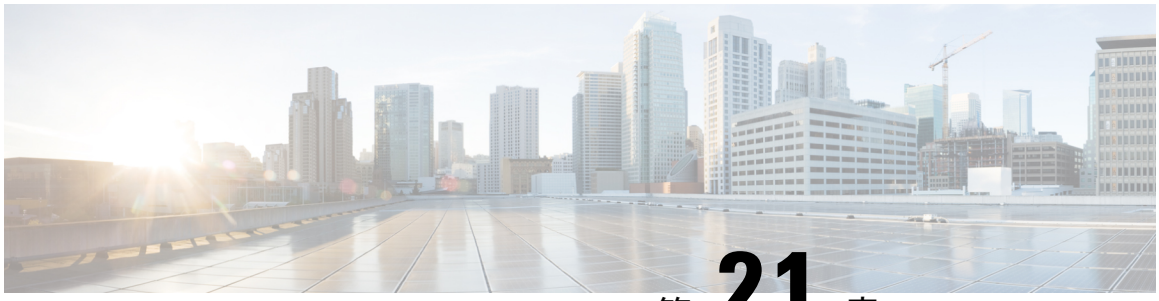
  スタティックおよびダイナミック MAC アドレス エントリを表示します。

インターフェイスの詳細設定の履歴

表 *31* : インターフェイスの詳細設定の履歴

機能名	リリース	機能情報
最大 MTU が 9198 バイトになりました	9.1(6)、9.2(1)	ASA で使用できる最大の MTU は 9198 バイトです（CLI のヘルプでご使用のモデルの正確な最大値を確認してください）。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。 次の画面が変更されました。**[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Edit Interface] > [Advanced]**
Firepower 4100/9300 シャーシ の ASA のMTU サイズ増加	9.6(2)	Firepower 4100 および 9300 で、最大 MTU を 9184 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次の画面が変更されました。**[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Advanced]**

機能名	リリース	機能情報
シングル コンテキスト モード用の一意の MAC アドレス生成	9.8(3), 9.8(4), 9.9(2)	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメイン インターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto** ASDM サポートはありません。



第 21 章

トラフィック ゾーン

トラフィック ゾーンに複数のインターフェイスを割り当てることができます。これにより、既存のフローのトラフィックがゾーン内のインターフェイスで ASA に出入りできるようになります。この機能により、ASA 上での等コスト マルチパス（ECMP）のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。

トラフィック ゾーンの概要

この項では、ネットワークでトラフィック ゾーンを使用する方法について説明します。

ゾーン分割されていない動作

アダプティブセキュリティアルゴリズムは、トラフィックの許可または拒否を決定する際に、パケットの状態を考慮します。フローに適用されたパラメータの1つは、トラフィックが同じインターフェイスに出入りすることです。異なるインターフェイスに入る既存のフローのトラフィックは、ASA によってドロップされます。

トラフィック ゾーンにより、複数のインターフェイスを 1 つにまとめることができるため、ゾーン内の任意のインターフェイスに出入りするトラフィックがアダプティブ セキュリティ アルゴリズムのセキュリティ チェックを満たすことができるようになります。

関連トピック

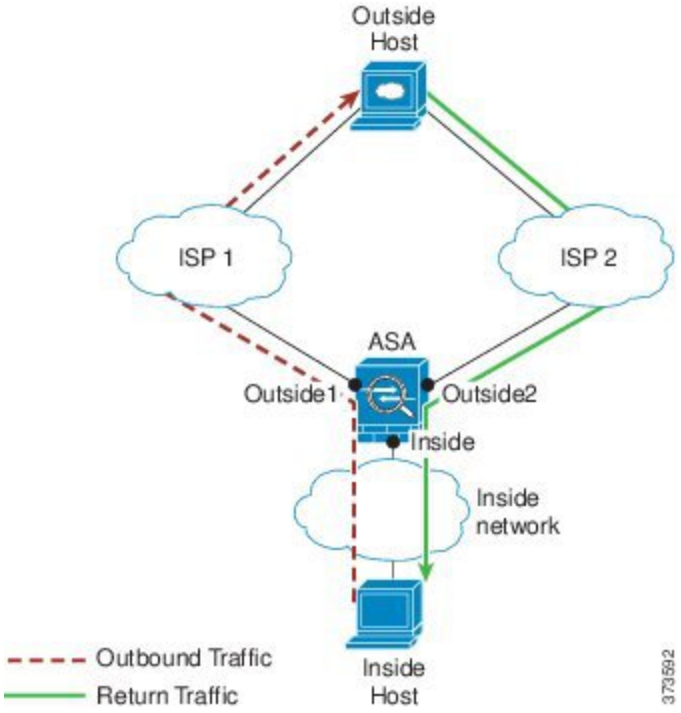
ステートフル インスペクションの概要 （11 ページ）

ゾーンを使用する理由

ゾーンを使用して、複数のルーティングのシナリオに対応することができます。

非対称ルーティング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。宛先ネットワークの非対称ルーティングが原因で、Outside2 インターフェイスの ISP 2 からリターン トラフィックが到達しています。

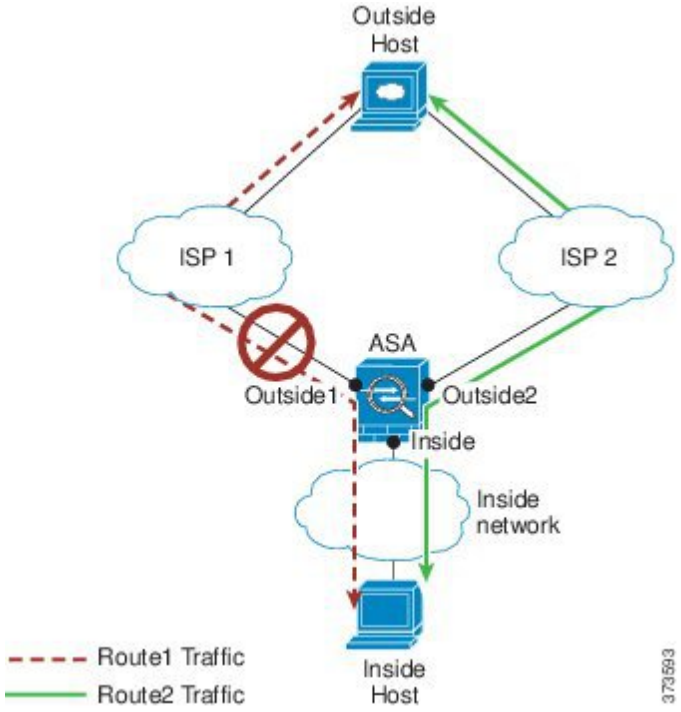


ゾーン分割されていない場合の問題：ASA は、インターフェイスごとに接続テーブルを保持します。リターン トラフィックが Outside2 に到達すると、そのトラフィックは、接続テーブルに一致しないため、ドロップされます。ASA クラスタに関しては、クラスタが同一ルータに対して複数の隣接関係（アジャセンシー）を持つ場合、非対称ルーティングは許容できないトラフィック紛失の原因となることがあります。

ゾーン分割されたソリューション：ASAは、ゾーンごとに接続テーブルを保持します。Outside1 と Outside2 を 1 つのゾーンにグループ化した場合、リターン トラフィックが Outside2 に到達すると、ゾーンごとの接続テーブルに一致するため、接続が許可されます。

紛失したルート

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。Outside1 と ISP 1 間でルートが紛失または移動したため、トラフィックは ISP 2 を経由する別のルートを通る必要があります。

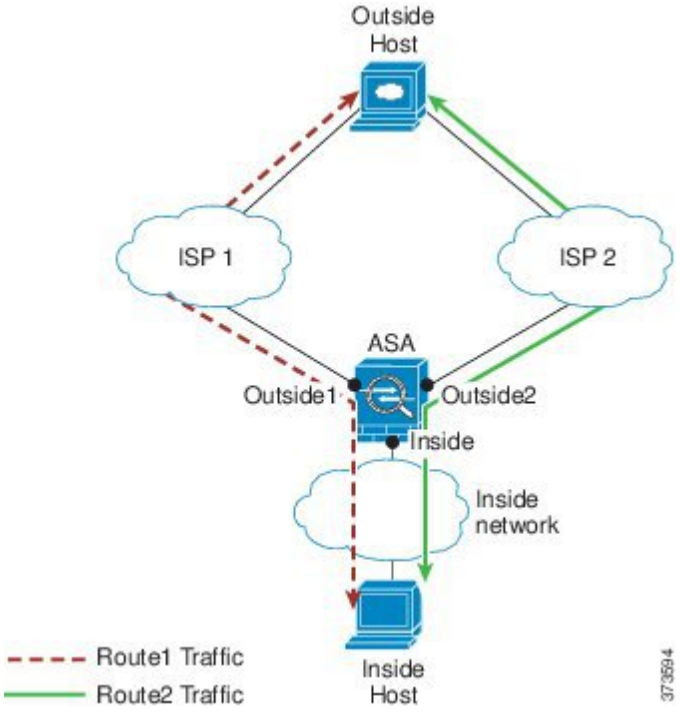


ゾーン分割されていない場合の問題：内部ホストと外部ホスト間の接続が削除されるため、新しい次善のルートを使用して新しい接続を確立する必要があります。UDP の場合、1 つのパケットがドロップダウンすると新しいルートが使用され、UDP がない場合は、新しい接続を再確立する必要があります。

ゾーン分割されたソリューション：ASA は、紛失したルートを検出し、フローを ISP 2 経由の新しいパスに切り替えます。トラフィックは、パケットがドロップすることなくシームレスに転送されます。

ロード バランシング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。2 番目の接続が Outside2 の ISP 2 を経由する等コスト ルートを介して確立されています。



ゾーン分割されていない場合の問題：インターフェイス間でロードバランシングを行うことができません。可能なのは、1つのインターフェイスの等コストルートによるロードバランスだけです。

ゾーン分割されたソリューション：ASAは、ゾーン内のすべてのインターフェイスで最大8つの等コスト ルート間の接続をロードバランスすることができます。

ゾーンごとの接続テーブルおよびルーティング テーブル

ASAは、トラフィックがゾーンのインターフェイスのいずれかに到達できるようにゾーンごとの接続テーブルを保持します。また、ASAは、ECMPサポート用にゾーンごとのルーティングテーブルも保持します。

ECMP ルーティング

ASA では、等コスト マルチパス（ECMP）ルーティングをサポートしています。

ゾーン分割されていない ECMP サポート

ゾーンがない場合は、インターフェイスごとに最大8つの等コストのスタティック ルートタまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスに 3 つのデフォルト ルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
```

```
route outside 0 0 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route outside2 0 0 10.2.1.1
```

ゾーン分割された ECMP サポート

ゾーンがある場合は、ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に 3 つのデフォルト ルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、自動的に等コスト ルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス全体でトラフィックをロードバランスします。

ルートが紛失した場合、ASA はフローをシームレスに別のルートに移動させます。

接続のロード バランス方法

ASA では、パケットの 6 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル、入力インターフェイス）から生成されたハッシュを使用して、等コスト ルート間の接続をロードバランスします。ルートが紛失しない限り、接続は接続期間中、インターフェイスで継続されます。

接続内のパケットは、ルート間でロードバランスされません。接続では、そのルートが紛失しない限り、単一ルートを使用します。

ASA では、ロード バランシング時にインターフェイス帯域幅やその他のパラメータを考慮しません。同じゾーン内のすべてのインターフェイスが MTU、帯域幅などの同じ特性を持つことを確認します。

ロード バランシング アルゴリズムは、ユーザー設定可能ではありません。

別のゾーンのルートへのフォール バック

ルートがインターフェイスで紛失したときにゾーン内で使用可能な他のルートがない場合、ASA では、異なるインターフェイス/ゾーンからのルートを使用します。このバックアップ

ルートを使用した場合、ゾーン分割されていないルーティングのサポートと同様にパケットのドロップが発生することがあります。

インターフェイスベースのセキュリティ ポリシーの設定

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。必須のパラレルインターフェイス設定の詳細については、トラフィック ゾーンの前提条件 （736 ページ）を参照してください。

トラフィック ゾーンでサポートされるサービス

次のサービスがゾーンでサポートされています。

- アクセル ルール
- NAT
- QoS トラフィック ポリシングを除くサービス ルール。
- Routing

完全にゾーン分割されたサポートは利用できませんが、To-the-Box および From-the-Box トラフィック （735 ページ）に示した to-the-box サービスおよび from-the-box サービスを設定することもできます。

トラフィック ゾーンのインターフェイスに他のサービス（VPN、ボットネット トラフィック フィルタなど）を設定しないでください。これらのサービスは、想定どおりに機能または拡張しないことがあります。

（注） セキュリティ ポリシーの設定方法の詳細については、トラフィック ゾーンの前提条件 （736 ページ）を参照してください。

セキュリティ レベル

ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1 つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

フローのプライマリおよび現在のインターフェイス

各接続フローは、最初の入出力インターフェイスに基づいて構築されます。これらのインターフェイスは、プライマリ インターフェイスです。

ルート変更または非対称ルーティングにより、新しい出力インターフェイスが使用されている場合は、新しいインターフェイスが現在のインターフェイスになります。

ゾーンの追加または削除

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

ゾーン内トラフィック

トラフィックがあるインターフェイスに入り、同じゾーンの別のインターフェイスから出ることができるようにするには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Enable traffic between two or more hosts connected to the same interface]をイネーブルにしてトラフィックが同じインターフェイスを出入りできるようにし、さらに、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Enable traffic between two or more interfaces which are configured with same security level]をイネーブルにして same-security インターフェイス間のトラフィックを許可します。このように設定しない場合、フローは同じゾーンの 2 つのインターフェイス間をルーティングできません。

To-the-Box および From-the-Box トラフィック

- management-only インターフェイスまたは management-access インターフェイスをゾーンに追加することはできません。
- ゾーンの通常のインターフェイスでの管理トラフィックでは、既存のフローの非対称ルーティングのみがサポートされます。ECMP サポートはありません。
- 1 つのゾーン インターフェイスにのみ管理サービスを設定できますが、非対称ルーティング サポートを利用するには、すべてのインターフェイスでそれを設定する必要があります。構成がすべてのインターフェイスでパラレルである場合でも、ECMP はサポートされません。
- ASA は、ゾーンで次の To-the-Box および From-the-Box サービスをサポートします。
  - [Telnet]
  - SSH

- HTTPS
- SNMP
- Syslog

ゾーン内の IP アドレスのオーバーラップ

ゾーン分割されていないインターフェイスの場合、ASA では、NAT が正しく設定されていれば、インターフェイスでの IP アドレス ネットワークのオーバーラップをサポートします。ただし、同じゾーンのインターフェイスでは、ネットワークのオーバーラップはサポートされていません。

トラフィック ゾーンの前提条件

- 名前、IPアドレス、およびセキュリティ レベルを含むすべてのインターフェイスパラメータを設定します。ゾーンのすべてのインターフェイスでセキュリティ レベルが一致する必要があることに注意してください。帯域幅および他のレイヤ2のプロパティについては、インターフェイスのようにグループ化する計画を立てる必要があります。
- 次のサービスをゾーンのすべてのインターフェイスで一致するように設定します。
  - アクセス ルール：同じアクセス ルールをゾーンのすべてのメンバー インターフェイスに適用するか、グローバル アクセス ルールを使用します。

    次に例を示します。

    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```

  - NAT：ゾーンのすべてのメンバー インターフェイスで同じ NAT ポリシーを設定するか、グローバル NAT ルールを使用します（つまり、「any」を使用して NAT ルールでゾーンのインターフェイスを表します）。

    インターフェイス PAT はサポートされていません。

    次に例を示します。

    ```
    object network WEBSERVER1
      host 10.9.9.9 255.255.255.255
      nat (inside,any) static 209.165.201.9
    ```

(注) インターフェイス固有の NAT および PAT プールを使用したときに元のインターフェイスの障害が発生した場合、ASA は接続を切り替えることはできません。

インターフェイス固有の PAT プールを使用する場合、同じホストからの複数の接続は、別のインターフェイスにロードバランスし、別のマッピング IP アドレスを使用することがあります。この場合、複数の同時接続を使用するインターネット サービスが正しく機能しないことがあります。

- サービス ルール：グローバル サービス ポリシーを使用するか、ゾーンの各インターフェイスに同じポリシーを割り当てます。

  QoS トラフィック ポリシングはサポートされていません。

  次に例を示します。

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

(注) VoIP インスペクションでは、ゾーンのロード バランシングにより、順序が正しくないパケットが増加する可能性があります。この状況は、異なるパスを通る先行パケットの前に後行パケットが ASA に到達する可能性があるために発生することがあります。順序が正しくないパケットには、次のような症状があります。

  - キューイングを使用した場合に、中間ノード（ファイアウォールと IDS）および受信エンドノードでメモリ使用率が高い。
  - ビデオまたは音声の品質が低い。

  これらの影響を軽減するには、VoIP トラフィックのロード分散にのみ IP アドレスを使用することを推奨します。

- ECMP ゾーン機能を考慮してルーティングを設定します。

トラフィック ゾーンのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードまたはルーテッド モードのブリッジグループ インターフェイスはサポートされません。

フェールオーバー

- フェールオーバー リンクまたはステート リンクをゾーンに追加することはできません。
- アクティブ/アクティブ フェールオーバー モードでは、各コンテキストのインターフェイスを非対称ルーティング（ASR）グループに割り当てることができます。このサービスにより、ピア装置の同様のインターフェイスに戻るトラフィックを元の装置に復元することができます。コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。ASR グループに関する詳細については、非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）（365 ページ）を参照してください。
- 各接続のプライマリ インターフェイスのみがスタンバイ装置に 複製されます。現在のインターフェイスは複製されません。スタンバイ装置がアクティブになると、その装置によって必要に応じて現在の新しいインターフェイスが割り当てられます。

クラスタ

- クラスタ制御リンクをゾーンに追加することはできません。

モデルのガイドライン

Firepower 1010 スイッチポートおよび VLAN インターフェイスをゾーンに追加することはできません。

その他のガイドライン

- 最大 256 ゾーンを作成できます。
- 次のタイプのインターフェイスをゾーンに追加できます。
  - 物理
  - VLAN
  - EtherChannel
  - 冗長

- 次のタイプのインターフェイスは追加できません。
  - 管理専用
  - 管理アクセス
  - フェールオーバーまたはステート リンク
  - クラスタ制御リンク
  - EtherChannel インターフェイスまたは冗長インターフェイスのメンバーインターフェイス
  - VNI（さらに、通常のデータ インターフェイスが nve 専用としてマークされている場合、ゾーンのメンバーにすることはできません）
  - BVI、またはブリッジグループ メンバー インターフェイス。
- 1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。
- ゾーンごとに最大 8 つのインターフェイスを含めることができます。
- ECMP の場合、ゾーンのすべてのインターフェイス間で、ゾーンごとに最大 8 つの等コスト ルートを追加できます。また、8 ルート制限の一部として 1 つのインターフェイスに複数のルートを設定することもできます。
- ゾーンにインターフェイスを追加すると、それらのインターフェイスのすべてのスタティック ルートが削除されます。
- ゾーン内のインターフェイスで DHCP リレー を有効にできません。
- ASA では、個別のインターフェイスにロードバランシングされるフラグメントについて、フラグメント化されたパケットのリアセンブルはサポートしていません。これらのフラグメントはドロップされます。
- PIM/IGMP マルチキャストルーティングは、ゾーン内のインターフェイスではサポートされません。

トラフィック ゾーンの設定

名前を付けたゾーンを設定し、インターフェイスをそのゾーンに割り当てます。

手順

ステップ 1 **[設定（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [ゾーン（Zones）]** の順に選択し、[追加（Add）] をクリックします。

または、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] ダイアログボックスのゾーンにインターフェイスを割り当てることもできます。

ステップ 2 ゾーンに最大 48 文字で名前を付けます。

ステップ 3 1 つ以上のインターフェイスを [メンバー（Member）] 領域に追加します。すべてのインターフェイスのセキュリティ レベルが同じであることを確認します。

ステップ 4 [適用（Apply）] をクリックします。

トラフィック ゾーンのモニターリング

この項では、トラフィック ゾーンをモニターする方法について説明します。

ゾーン情報

- **show zone** [*name*]

  ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

  show zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  インターフェイス名およびゾーン名を表示します。

  show nameif zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show nameif zone
Interface                Name                    zone-name      Security
GigabitEthernet0/0       inside-1                inside-zone     100
GigabitEthernet0/1.21    inside                  inside-zone     100
GigabitEthernet0/1.31    4                                         0
GigabitEthernet0/2       outside                 outside-zone   0
Management0/0            lan                                       0
```

ゾーン接続

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  show conn zone コマンドは、ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリ インターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。

show conn long zone コマンドの次の出力を参照してください。

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  デバッグ目的で高速セキュリティ パス テーブルを表示します。

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  ゾーン内のローカル ホストのネットワーク状態を表示します。

  show local-host zone コマンドについては、次の出力を参照してください。プライマリ インターフェイスが最初に表示され、現在のインターフェイスがカッコに囲まれています。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

ゾーン ルーティング

- **show route zone**

  ゾーン インターフェイスのルートを表示します。

  show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
```

```
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

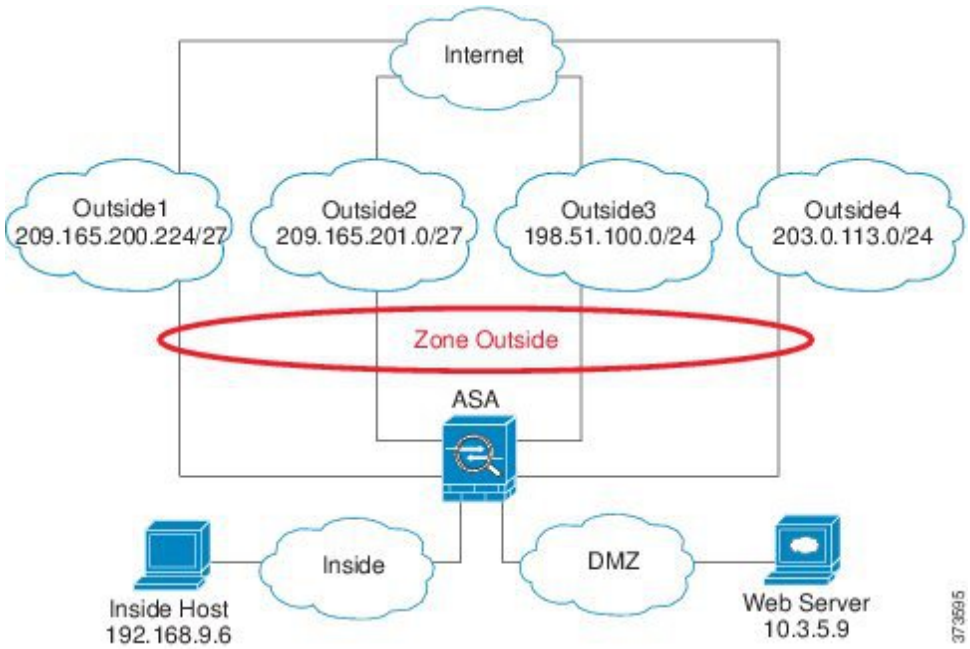
  デバッグ目的で高速セキュリティパステーブルを表示し、各ルートに関連付けられたゾーンを表示します。

  show asp table routing コマンドについては次の出力を参照してください。

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

トラフィック ゾーンの例

次に、4 つの VLAN インターフェイスを外部ゾーンに割り当てて、4 つの等コストのデフォルト ルートを設定する例を示します。PAT は内部インターフェイスに設定され、Web サーバーはスタティック NAT を使用して DMZ インターフェイスで使用できます。




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
```

```
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
```

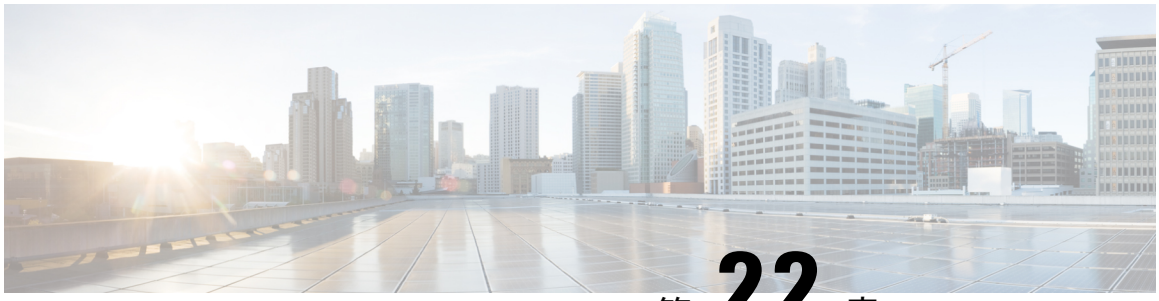
```
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

トラフィック ゾーンの履歴

機能名	プラットフォームリリース	説明
トラフィック ゾーン	9.3(2)	インターフェイスをトラフィック ゾーンにグループ化することで、トラフィックのロードバランシング（等コスト マルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングを実現できます。 （注） 名前付きゾーンにはセキュリティ ポリシーを適用できません。セキュリティポリシーはインターフェイスに基づきます。ゾーン内のインターフェイスが同じアクセスルール、NAT、およびサービス ポリシーを使用して設定されていれば、ロード バランシングおよび非対称ルーティングは正しく動作します。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Interface Parameters] > [Zones]** **[Configuration] > [Device Setup] > [Interface Parameters] > [Interfaces]**。
clear local-host コマンド	9.14(1)	**clear local-host** コマンドおよびそのすべての属性とキーワードが廃止されました。今後のリリースで削除される予定です。

第 IV 部

基本設定



第 22 章

基本設定

この章では、ASA 上でコンフィギュレーションを機能させるために通常必要な基本設定を行う方法について説明します。

ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードを設定するには、次の手順を実行します。

始める前に

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードを設定する前に、次の要件を確認します。

- マルチ コンテキスト モードでは、コンテキスト実行スペースとシステム実行スペースの両方のホスト名とドメイン名を設定できます。
- イネーブル パスワードと Telnet パスワードは、各コンテキストで設定します。システムでは使用できません。

- システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** を選択します。

ステップ 2 ホスト名を入力します。デフォルトのホスト名は「ciscoasa」です。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名は syslog メッセージでも使用されます。

マルチ コンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドラインプロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

ステップ 3 ドメイン名を入力します。デフォルト ドメイン名は default.domain.invalid です。

ASA は、修飾子を持たない名前のサフィックスとして、ドメイン名を追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバーとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

ステップ 4 特権モード（イネーブル）パスワードを変更します。デフォルトのパスワードは空白ですが、CLI で **enable** コマンドを最初に入力したときに変更するように求められます。

enable 認証を設定しない場合、イネーブル パスワードによって特権 EXEC モードが開始されます。HTTP 認証を設定しない場合、イネーブル パスワードによって空のユーザー名で ASDM にログインできます。 ASDM では、CLI アクセスのように、イネーブル パスワードの変更は適用されません。

a) [Change the privileged mode password] チェックボックスをオンにします。
b) 新しいパスワードを入力し、新しいパスワードを確認します。3 から 127 文字のパスワードを設定します。大文字と小文字が区別されます。スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

   パスワードを空白の値にリセットすることはできません。

ステップ 5 Telnet アクセスのためのログイン パスワードを設定します。デフォルトのパスワードはありません。

Telnet 認証を設定しない場合、ログイン パスワードは Telnet アクセスに使用されます。

a) [Change the password to access the console of the security appliance] チェックボックスをオンにします。
b) 古いパスワード（新しい ASA の場合はこのフィールドを空白にしておきます）、新しいパスワードを入力し、新しいパスワードを確認します。パスワードには最大 16 文字の長さを使用できます。スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

ステップ 6 [Apply] をクリックして変更内容を保存します。

日時の設定

（注） Firepower 2100（プラットフォームモード）、4100、または 9300 の日時を設定しないでください。ASA はシャーシから日時の設定を受信します。

NTP サーバーを使用した日付と時刻の設定

NTP を使用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバーを設定できます。ASA は、データ信頼度の尺度となる一番下のストラタムのサーバーを選択します。

手動で設定した時刻はすべて、NTP サーバーから取得された時刻によって上書きされます。

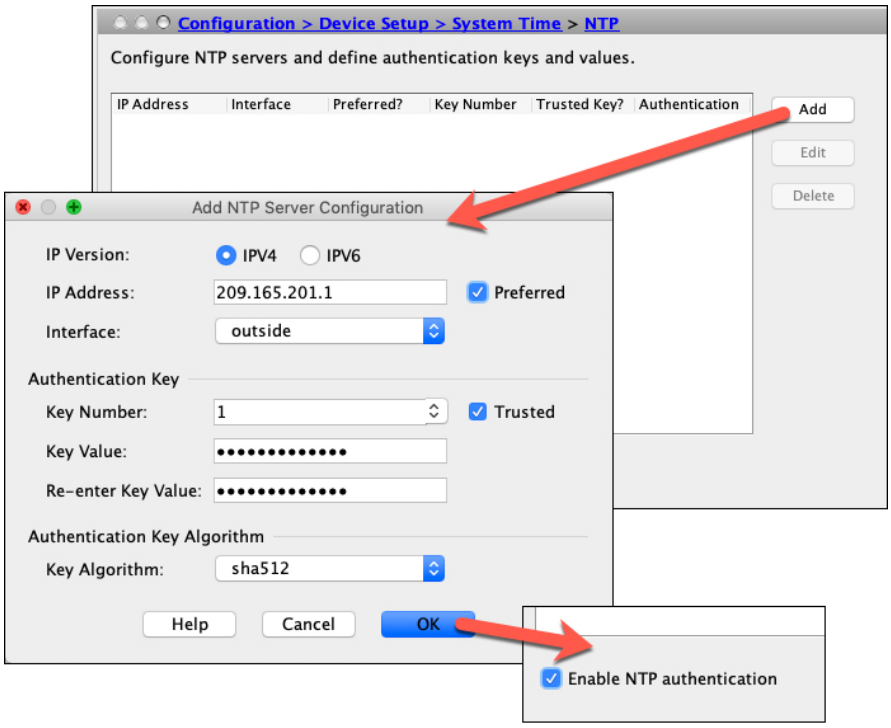
ASA は NTPv4 をサポートします。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[System Time]** > **[NTP]** を選択します。



ステップ 2 [Add] をクリックして、[Add NTP Server Configuration] ダイアログボックスを表示します。

ステップ 3 NTP サーバーの **IPv4** または **IPv6 IP アドレス**を入力します。

サーバーのホスト名を入力することはできません。ASA は、NTP サーバーの DNS ルックアップをサポートしていません。

ステップ 4 （任意） [Preferred] チェックボックスをオンにして、このサーバーを優先サーバーに設定します。

NTP では、どのサーバーの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバーに同期します。精度が同じ程度であれば、優先サーバーを使用します。ただし、優先サーバーよりも精度が大幅に高いサーバーがある場合、ASA は精度の高いそのサーバーを使用します。

ステップ 5 （任意） ドロップダウンリストから [Interface] を選択します。

この設定では、NTP パケットの発信インターフェイスが指定されます。インターフェイスが空白の場合、ASA が使用するデフォルトの管理コンテキストインターフェイスは、管理ルーティングテーブルによって決まります。

ステップ 6 （任意） NTP 認証を設定します。

a) 1 ～ 4294967295 の間の**キー番号**を入力するか、または、再利用する別の NTP サーバーのキーを以前に作成した場合は、ドロップダウンリストから既存のキー番号を選択します。

この設定では、この認証キーのキー ID を指定します。これにより、認証を使用して NTP サーバーと通信できます。NTP サーバーのパケットも、常にこのキー ID を使用する必要があります。

b) [Trusted] チェックボックスをオンにします。
c) [Key Value] を入力します。これは、最大 32 文字の文字列です。その後、キー値を再入力します。
d) ドロップダウンリストから [Key Algorithm] を選択します。
e) [OK] をクリックします。

ステップ 7 [Enable NTP authentication] チェックボックスをオンにして、NTP 認証を有効にします。

ステップ 8 [Apply] をクリックして変更内容を保存します。

手動での日時の設定

日付と時刻を手動で設定するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[System Time]** > **[Clock]** を選択します。

ステップ 2 ドロップダウン リストからタイム ゾーンを選択します。この設定では、適切な時差を GMT に加えた（または GMT から差し引いた）タイム ゾーンを指定します。[Eastern Time]、[Central Time]、[Mountain Time]、または [Pacific Time] ゾーンを選択すると、3 月の第 2 日曜日の午前 2 時から 11 月の第 1 日曜日の午前 2 時間での時間が自動的に夏時間に調整されます。

（注） ASA の時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

ステップ 3 [Date] ドロップダウン リストをクリックしてカレンダーを表示します。続いて、次の方法を使用して正しい日付を検索します。

- 月の名前をクリックし、月のリストを表示し、次に目的の月をクリックします。カレンダーがその月に変わります。
- 年をクリックして年を変更します。上矢印と下矢印を使用して複数年をスクロールすることも、入力フィールドに年を入力することもできます。
- 年月の左右にある矢印をクリックすると、カレンダーが一度に 1 か月ずつ前後にスクロールします。
- カレンダーの日にちをクリックして日を設定します。

ステップ 4 時刻（時間、分、および秒）を手動で入力します。

ステップ 5 [Update Display Time] をクリックして、ASDM ペインの右下に表示される時刻を更新します。現在時刻は 10 秒ごとに自動更新されます。

Precision Time Protocol の設定（ISA 3000）

高精度時間プロトコル（PTP）は、パケットベース ネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。それらのデバイスクロックは、一般的に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせによる、分散型のネットワークシステムです。PTP デバイスには、オーディナリ クロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、ネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

ASA デバイスは、トランスペアレントクロックとして設定できます。ASA デバイスは、自身のクロックを PTP クロックと同期しません。ASA デバイスは、PTP クロックで定義されている PTP のデフォルトプロファイルを使用します。

PTP デバイスを設定する場合は、連携させるデバイスのドメイン番号を定義します。したがって、複数の PTP ドメインを設定し、特定の 1 つのドメインに PTP クロックを使用するように PTP 以外の各デバイスを設定できます。

（注） PTP トラフィックが検査のために ASA FirePOWER モジュールに送信されないようにするために、ASA のデフォルト設定に以下のコマンドが追加されています。既存の導入がある場合は、次のコマンドを手動で追加する必要があります。

```
object-group service bypass_sfr_inspect
service-object udp destination range 319 320
access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any
```

始める前に

- この機能は、ISA 3000 のみで使用できます。
- PTP の使用は、シングルコンテキストモードでのみサポートされます。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。
- デフォルトでは、トランスペアレントモードのすべての ISA 3000 インターフェイスで PTP がイネーブルになっています。ルーテッドモードでは、PTP パケットがデバイスを通過できるようにするために必要な設定を追加する必要があります。
- PTP は IPv6 ネットワークではなく、IPv4 ネットワークでのみ使用できます。

- PTP設定は、スタンドアロンかブリッジグループメンバーかを問わず、物理イーサネットインターフェイスでサポートされます。次のものではサポートされません。
  - 管理インターフェイス。
  - サブインターフェイス、EtherChannel、BVI、その他の仮想インターフェイス。
- VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。
- PTPパケットが確実にデバイスを通過できるようにする必要があります。トランスペアレントファイアウォールモードでは、PTPトラフィックを許可するアクセスリストがデフォルトで設定されています。PTP トラフィックは UDP ポート 319 と 320、および宛先 IP アドレス 224.0.1.129 によって識別されます。そのためルーテッド ファイアウォール モードでは、このトラフィックを許可するすべての ACL が受け入れられます。
- さらにルーテッド ファイアウォール モードでは、PTP マルチキャストグループ用のマルチキャストルーティングを次のようにイネーブルにする必要もあります。
  - グローバル コンフィギュレーション モードのコマンド **multicast-routing** を入力します。
  - また、ブリッジグループメンバーではなく、PTPが有効になっているインターフェイスごとに、インターフェイス コンフィギュレーション コマンド **igmp join-group 224.0.1.129** を入力して、PTP マルチキャスト グループ メンバーシップを静的に有効にします。このコマンドは、ブリッジグループメンバーに対してはサポートされておらず、必要もありません。

手順

ステップ 1 **[Configuration]** > **[Device Management** > **PTP]** を選択します。

ステップ 2 **Domain value** を入力します。

これは、デバイスのすべてのポートのドメイン番号です。異なるドメインで受信されたパケットは、通常のマルチキャストパケットのように扱われるため、PTP処理は行われません。この値の範囲は 0 ～ 255、デフォルト値は 0 です。ネットワーク内の PTP デバイスに設定されているドメイン番号を入力します。

ステップ 3 （オプション）**Enable End-to-End Transparent Clock Mode** を選択し、PTPがイネーブルになっているすべてのインターフェイスでエンドツーエンド トランスペアレント モードをイネーブルにします。

トランスペアレント クロックは、滞留時間を測定し、PTP パケット内の `correctionField` を更新することによって遅延を修正するクロックです。

ステップ 4 インターフェイスを選択し、[Enable] または [Disable] をクリックして、1 つ以上のデバイスインターフェイスで PTP を有効にします。

システムが設定ドメイン内のPTPクロックに接続できる各インターフェイスで、PTPを有効にします。

ステップ 5 [Apply] をクリックします。

次のタスク

[Monitoring] > **[Properties]** > **[PTP]** を選択し、PTP クロックとインターフェイス/ポート情報を表示します。

マスター パスフレーズの設定

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスターパスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバー
- Logging
- 共有ライセンス

マスター パスフレーズの追加または変更

マスター パスフレーズを追加または変更するには、次の手順を実行します。

始める前に

- この手順を実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。
- フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

[Configuration] > [Device Management] > [High Availability] > [Failover] の順に選択し、[Shared Key] フィールドに任意の文字を入力するか、またはフェールオーバー 16 進キーを選択している場合はバックスペースを除く 32 の 16 進数（0-9A-Fa-f）を入力します。次に、[Apply] をクリックします。

- アクティブ/スタンバイ フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行されます。これは、アクティブな構成をスタンバイ ユニットに複製します。この複製が行われない場合、スタンバイ ユニットの暗号化されたパスワードは、同じパスフレーズを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、アクティブ/アクティブ モードでトラフィックの中断を引き起こす場合があります。これは、新しい構成が同期される前に、セカンダリ ユニットで構成が消去されるためです。**failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、**write standby** を入力してから、**no failover active group 2** コマンドを使用してセカンダリ ユニットにグループ 2 コンテキストを復元する必要があります。

手順

ステップ 1 次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] を選択します。

ステップ 2 [Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスター パスフレーズがない場合は、[Apply] をクリックすると警告メッセージが表示されます。[OK] または [Cancel] をクリックして続行できます。

後からパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードはいずれも変更されず、マスターパスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3 [Change the encryption master passphrase] チェックボックスをオンにして、新しいマスター パスフレーズを入力および確認できるようにします。デフォルトでは、これらはディセーブルです。

新しいマスター パスフレーズの長さは 8 ～ 128 文字にする必要があります。

既存のパスフレーズを変更する場合は、新しいパスフレーズを入力する前に、古いパスフレーズを入力する必要があります。

マスター パスフレーズを削除するには [New] および [Confirm master passphrase] フィールドを空白のままにします。

ステップ 4 [適用（Apply）] をクリックします。

マスター パスフレーズの無効化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキストパスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェアバージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

始める前に

- ディセーブルにする現在のマスター パスフレーズがわかっていなければなりません。
- この手順が機能するのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュアセッションだけです。

  マスター パスフレーズをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- シングル コンテキスト モードで、[Configuration] > [Device Management] > [Advanced] > [Master Passphrase] を選択します。
- マルチ コンテキスト モードで、[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase] を選択します。

ステップ 2 [Advanced Encryption Standard (AES) password encryption] チェックボックスをオンにします。

有効なマスターパスフレーズがない場合は、[Apply] をクリックすると警告文が表示されます。[OK] または [Cancel] をクリックして続行します。

ステップ 3 [Change the encryption master passphrase] チェックボックスをオンにします。

ステップ 4 [Old master passphrase] フィールドに、古いマスターパスフレーズを入力します。ディセーブルにする古いマスター パスフレーズを指定する必要があります。

ステップ 5 [Newmaster master passphrase] フィールドと [Confirm master passphrase] フィールドを空白のままにします。

ステップ 6 [Apply] をクリックします。

DNS サーバーの設定

DNS サーバーを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するように、DNS サーバーを設定する必要があります。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバーと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

（注） ASA では、機能に応じて DNS サーバーの使用が限定的にサポートされます。

始める前に

DNS ドメイン ルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングおよびアクセス ルールを設定し、DNS サーバーに到達できるようにしてください。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** の順に選択します。

ステップ 2 [DNS Setup] 領域で、次のいずれかのオプションを選択します。

- Configure one DNS server group：このオプションは DefaultDNS グループにサーバーを定義します。
- Configure multiple DNS server groups：このオプションでも、DefaultDNS グループは設定する必要があります。FQDN ネットワーク オブジェクトの名前解決に使用されるのは DefaultDNS グループのみです。DefaultDNS はアクティブ グループのままにします。ただし、リモート アクセス SSL VPN グループ ポリシーで使用する追加のグループを作成することもできます。DefaultDNS グループのみを設定したとしても、グループで使用するタイムアウトやその他の特性を変更する場合は、このオプションを選択する必要があります。

ステップ 3 [Configure one DNS server group] を選択した場合は、DefaultDNS グループにサーバーを設定します。

a) [Primary DNS Server] に、可能な限り使用する必要がある DNS サーバーの IP アドレスを入力します。必要に応じて、このサーバーと各セカンダリ サーバーに対し、ASA がサーバーとの接続に使用する *interface_name* を指定します。インターフェイスを指定しなかった場合、ASA はデータ ルーティング テーブルを確認し、一致するものが見つからなければ、管理専用ルーティング テーブルを確認します。

b) [Add] をクリックして、セカンダリ DNS サーバーを追加します。

最大 6 個の DNS サーバーを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[Move Up]/[Move Down] ボタンを使用して、サーバーを優先度の順に並べます。

c) ホスト名に追加する DNS ドメイン名を入力します（完全修飾されていない場合）。

ステップ 4 [Configure multiple DNS server groups] を選択した場合は、サーバー グループのプロパティを定義します。

a) [Add] をクリックして新しいグループを作成するか、グループを選択して [Edit] をクリックします。

DefaultDNS グループは常にリストに表示されます。

b) グループ プロパティを設定します。

- [Server IP Address to Add]、[Source Interface]：DNS サーバーの IP アドレスを入力し、[Add>>] をクリックします。各サーバーについて、必要に応じて ASA がサーバーとの通信に使用する *interface_name* を指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

  最大 6 個の DNS サーバーを追加できます。ASA では、応答を受信するまで各 DNS サーバを順に試します。[Move Up]/[Move Down] ボタンを使用して、サーバーを優先度の順に並べます。

- [タイムアウト（Timeout）]：次の DNS サーバーを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。ASA がサーバーのリストを再試行するたびに、このタイムアウトは倍増します。

- [Retries]：ASA が応答を受信しないときに、DNS サーバーのリストを再試行する回数（0 ～ 10）。

- [Expire Entry Timer]（DefaultDNS またはアクティブ グループのみ）：DNS エントリの期限が切れた（TTL が経過した）後、そのエントリが DNS ルックアップ テーブルから削除されるまでの分数。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です（つまり、TTL が経過してから 1 分後にエントリが削除されます）。指定できる範囲は 1 ～ 65535 分です。このオプションは、FQDN ネットワーク オブジェクトの解決時にのみ使用されます。

- [Poll Timer]（DefaultDNS またはアクティブ グループのみ）：FQDN ネットワーク/ホスト オブジェクトを IP アドレスに解決するために使用されるポーリング サイクルの時間（分単位）。FQDN オブジェクトはファイアウォール ポリシーで使用される場合にのみ解決されます。タイマーによって解決間隔の最大時間が決まります。IP アドレス解決に対して更新するタイミングの決定には DNS エントリの存続可能時間（TTL）値も使用されるため、個々の FQDN がポーリング サイクルよりも頻繁に解決される場合があります。デフォルトは 240（4 時間）です。指定できる範囲は 1 ～ 65535 分です。

• [Domain Name]：ホスト名に追加するドメイン名（完全修飾されていない場合）。

c) [OK] をクリックします。
d) 複数のグループがある場合は、DNS 要求に使用するグループを選択して [Set Active] をクリックすれば変更できます。

ステップ 5 DNSルックアップが少なくとも1つのインターフェイスでイネーブルになっていることを確認します。DNS サーバー グループの表の下にある [DNS lookup] インターフェイス リストで、[DNS Enabled] カラムをクリックして [True] を選択し、インターフェイスでのルックアップを有効化します。

インターフェイスで DNS ルックアップを有効にしないと、DNS サーバーの [Source Interface] またはルーティング テーブルを使用して検出したインターフェイスを使用できません。

ステップ 6 （任意）クエリーごとに 1 つの DNS 応答を強制するには、[Enable DNS Guard on all interfaces] チェックボックスをオンにします。

DNS インスペクションを設定するときに、DNS ガードも設定できます。特定のインターフェイスでは、DNS インスペクションで設定されている DNS ガードの設定がこのグローバル設定より優先されます。デフォルトでは、DNSインスペクションはDNSガードがイネーブルになっているすべてのインターフェイスでイネーブルになっています。

ステップ 7 [Apply] をクリックして変更内容を保存します。

ハードウェア バイパスおよびデュアル電源（Cisco ISA 3000）の設定

ハードウェア バイパスを有効化して、停電時にもインターフェイス ペア間のトラフィックのフローを継続することができます。サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。ハードウェア バイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。次のハードウェア バイパスのガイドラインを参照してください。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- 光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。
- ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのはサポートされているインターフェイス ペアだけになります。つまり、デフォルトの設定を使用している場合、inside1 と inside2 間および outside1 と outside2 間は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。
- シスコでは、TCP シーケンスのランダム化を無効にすることを推奨しています（下記の手順を参照）。ランダム化が有効化されている場合（デフォルト）、ハードウェア バイパス

を有効化するときにTCPセッションを再確立する必要があります。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェアバイパスが有効化されると、ISA 3000 はデータ パスに存在しなくなり、シーケンス番号を変換しません。受信するクライアントは予期しないシーケンス番号を受信し、接続をドロップします。TCP シーケンスのランダム化が無効になっていても、スイッチオーバーの際に一時的にダウンしたリンクのために、一部の TCP 接続は再確立される必要があります。

- ハードウェアのバイパス インターフェイスでの Cisco TrustSec の接続は、ハードウェアのバイパスが有効化されているときにはドロップされます。ISA 3000 の電源がオンになり、ハードウェアのバイパスが非アクティブ化されている場合、接続は再ネゴシエートされます。
- ハードウェア バイパスを非アクティブ化し、トラフィックが ISA 3000 のデータ パスを経由することを再開した場合、スイッチオーバー時に一時的にダウンしたリンクがあるために、既存の TCP セッションの一部を再確立する必要があります。
- ハードウェア バイパスをアクティブにすると、イーサネット PHY が切断され、ASA はインターフェイスのステータスを判断できなくなります。インターフェイスはダウン状態であるかのように表示されます。

ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。

始める前に

- ハードウェア バイパス インターフェイスはスイッチのアクセス ポートに接続する必要があります。トランク ポートには接続しないでください。

手順

ステップ 1 ハードウェア バイパスを設定するには、**[Configuration]** > **[Device Management]** > **[Hardware Bypass]** の順に選択します。

ステップ 2 [Enable Bypass during Power Down] チェックボックスをオンにして、各インターフェイス ペアのハードウェア バイパスを有効化するように設定します。

ステップ 3 （任意） **[Stay in Bypass after Power Up]** チェック ボックスをオンにして、電源が回復してアプライアンスが起動した後にハードウェア バイパス モードの状態に維持されるように、各インターフェイス ペアを設定します。

ハードウェア バイパスを非アクティブ化すると、ASA がフローを引き継ぐため、接続が短時間中断されます。この場合、準備が整った時点でハードウェアバイパスを手動でオフにする必要があります。このオプションを使用すると、短時間の割り込みがいつ発生するかを制御できます。

ステップ 4 インターフェイス ペアに対しては、[Bypass Immediately] チェックボックスをオン/オフして、手動でハードウェア バイパスを有効化または非アクティブ化します。

ステップ 5 （任意） **[Stay in Bypass Mode until after the ASA Firepower Module Boots Up]** チェック ボックスをオンにして、ASA Firepower モジュールの起動後までハードウェア バイパスがアクティブであり続けるように設定します。

ブート遅延が動作するには、[Stay in Bypass after Power Up] オプションを使用せずにハードウェア バイパスを有効化する必要があります。このオプションを使用しないと、ASA FirePOWER モジュールが起動を完了する前にハードウェア バイパスが非アクティブになる可能性があります。たとえば、モジュールをフェールクローズに設定していた場合、このような状況では、トラフィックがドロップされる可能性があります。

ステップ 6 [Apply] をクリックします。

ステップ 7 TCP のランダム化を無効化します。この例では、デフォルト設定に設定を追加することによって、すべてのトラフィックのランダム化を無効化する方法を示します。

a) **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択します。
b) **sfrclass** ルールを選択して [Edit] をクリックします。
c) [Rule Actions] に続いて、[Connection Settings] をクリックします。
d) [Randomize Sequence Number] チェック ボックスをオフにします。
e) [OK]、続いて [Apply] をクリックします。

ステップ 8 予期する構成としてデュアル電源を設定するには、**[Configuration]** > **[Device Management]** > **[Power Supply]** の順に選択し、[Enable Redundant Power Supply] チェック ボックスをオンにして、[Apply] をクリックします。

この画面は利用可能な電源も表示します。

ステップ 9 [保存（Save）] をクリックします。

システムがオンラインになった後のハードウェアバイパスの動作は、スタートアップ コンフィギュレーションの設定によって決定されるため、実行コンフィギュレーションを保存する必要があります。

ASP（高速セキュリティ パス）のパフォーマンスと動作の調整

ASP はポリシーおよび設定を利用可能にする実装レイヤです。Cisco Technical Assistance Center とのトラブルシューティング時以外は直接影響することはありません。ただし、パフォーマンスと信頼性に関連するいくつかの動作を調節することができます。

ルール エンジンのトランザクション コミット モデルの選択

デフォルトでは、ルールベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性によりパフォーマンスにわずかな負担がかかります。パフォーマンス コストは、1秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しながら、25,000 個のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルール エンジンがルールをコンパイルするためです。デフォルトでは、システムは接続試行の評価時にコンパイルされていないルールも検索して、新しいルールが適用されるようにします。ルールがコンパイルされていないため、検索に時間がかかります。

この動作を変更して、ルール エンジンがトランザクション モデルを使用してルールの変更を導入し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクション モデルを使用することで、ルールのコンパイル中にパフォーマンスが落ちることはありません。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールに一致します。	新しいルールに一致します （接続数/秒のレートは減少します）。	新しいルールに一致します。
トランザクション	古いルールに一致します。	古いルールに一致します （接続数/秒のレートは影響を受けません）。	新しいルールに一致します。

トランザクション モデルのその他のメリットには、インターフェイス上の ACL を交換するときに、古い ACL を削除して新しいポリシーを適用するまでに時間差がないことがあります。この機能により受け入れ可能な接続が操作中にドロップされる可能性が削減されます。

ヒント ルール タイプのトランザクション モデルをイネーブルにする場合、コンパイルの先頭と末尾をマークする Syslog が生成されます。これらの Syslog には 780001 ～ 780004 までの番号が付けられます。

ルール エンジンのトランザクション コミット モデルを有効にするには、次の手順を使用します。

手順

[Configuration] > [Device Management] > [Advanced] > [Rule Engine] の順に選択し、目的のオプションを選択します。

- **Access group**：グローバルにまたはインターフェイスに適用されるアクセス ルール。
- **NAT**：ネットワーク アドレス変換ルール。

ASP ロード バランシングの有効化

ASP のロード バランシング機能によって、次の問題を回避しやすくなります。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングル コアでは負荷を維持できません）

ASP ロードバランシングにより、1 つのインターフェイス受信リングから受信したパケットを複数のコアが同時に処理できます。システムがパケットをドロップし、**show cpu** コマンドの出力が 100% を大きく下回る場合、互いに関連のない多数の接続にパケットが属しているのであれば、この機能によってスループットが向上することがあります。

（注） ASP ロード バランシングは、ASAv で無効になっています。DPDK（データプレーン開発キット）を ASAv の高速セキュリティ パス（ASP）に統合すると、ASAv でこの機能を無効にしたときのパフォーマンスが向上します。

手順

ステップ 1 ASP ロード バランシングの自動切り替えをイネーブルまたはディセーブルにするには、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[ASP Load Balancing]** の順に選択して、[Dynamically enable or disable ASP load balancing based on traffic monitoring] チェックボックスをオンにします。

ステップ 2 手動で ASP ロード バランシングをイネーブルまたはディセーブルにするには、[Enable ASP load balancing] チェックボックスをオンまたはオフにします。

手動で ASP ロード バランシングをイネーブルにすると、動的オプションをイネーブルにした場合でも、手動でディセーブルにするまではイネーブル状態となります。手動で ASP ロード バランシングをイネーブルにした場合にのみ、ASP ロード バランシングの手動ディセーブル

化が適用されます。動的オプションもまたイネーブルにすると、システムは ASP ロード バランシングの自動イネーブル/ディセーブル化に戻ります。

DNS キャッシュのモニターリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカルキャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバーに DNS クエリーが送信されます。外部 DNS サーバーによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカルキャッシュに格納されます。

DNS キャッシュのモニターリングについては、次のコマンドを参照してください。

- **show dns-hosts**

  DNS キャッシュを表示します。これには、DNS サーバーからダイナミックに学習したエントリと name コマンドを使用して手動で入力された名前および IP アドレスが含まれます。

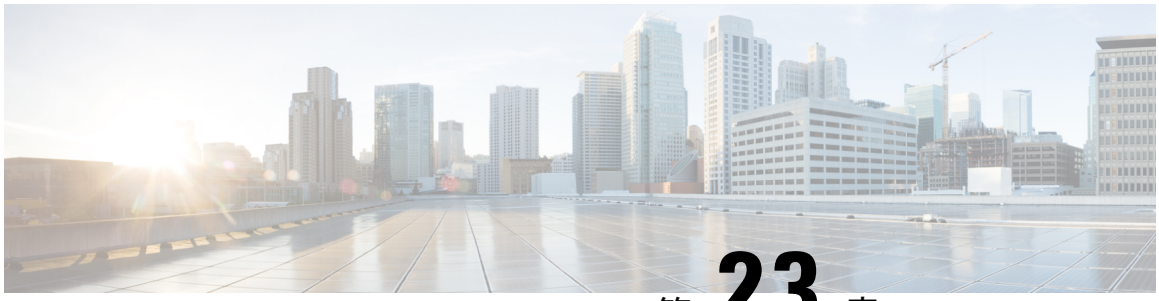
基本設定の履歴

機能名	プラットフォームリリース	説明
NTPv4 のサポート	9.14(1)	ASA が NTPv4 をサポートするようになりました。 変更された画面はありません。

機能名	プラットフォームリリース	説明
追加の NTP 認証アルゴリズム	9.13(1)	以前は、NTP 認証では MD5 だけがサポートされていました。ASA は、次のアルゴリズムをサポートするようになりました。 • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC 新しい/変更された画面： **[構成（Configuration）] > [デバイス設定（Device Setup）] > [システム時間（System Time）] > [NTP] > [追加（Add）]**ボタン > [NTPサーバ構成の追加（Add NTP Server Configuration）] ダイアログボックス > [キーアルゴリズム（Key Algorithm）] ドロップダウンリスト
IPv6 での NTP サポート	9.12(1)	NTP サーバーに IPv6 アドレスを指定できるようになりました。 新しい/変更された画面： **[Configuration] > [Device Setup] > [System Time] > [NTP] > [Add]** ボタン > [Add NTP Server Configuration] ダイアログボックス
enable ログイン時のパスワードの変更が必須に	9.12(1)	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 ～ 127 文字の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブルパスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 変更された画面はありません。
ASP ロードバランシングは、ASAv で無効になっています。	9.10(1)	DPDK（データプレーン開発キット）の ASAv の高速セキュリティ パス（ASP）への最近の統合により、ASAv でこの機能を無効にしたときのパフォーマンスが向上します。

機能名	プラットフォームリリース	説明
自動 ASP ロード バランシングが ASAv でサポートされるようになりました。	9.8(1)	以前は、ASP ロード バランシングは手動でのみ有効または無効にできました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	9.7(1)	長さ制限内のすべてのローカル **username** および **enable** パスワードは、SHA-512 を使用する PBKDF2（パスワードベースキー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザーが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**
ISA 3000 のデュアル電源サポート	9.6(1)	ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。 次の画面が導入されました。**[Configuration] > [Device Management] > [Power Supply]**
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**
ISA 3000 ハードウェア バイパス	9.4(1.225)	ISA 3000 は、トラフィックが電源喪失時にアプライアンスを通過し続けるようにするハードウェア バイパス機能をサポートします。 次の画面が導入されました。**[Configuration] > [Device Management] > [Hardware Bypass]** この機能は、バージョン *9.5(1)* では使用できません。

機能名	プラットフォームリリース	説明
自動 ASP ロード バランシング	9.3(2)	ASP ロードバランシング機能の自動切替を有効または無効に設定できるようになりました。 （注） 自動機能は ASAv ではサポートされません。手動による有効化または無効化のみがサポートされます。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [ASP Load Balancing]。
デフォルトの Telnet パスワードの削除	9.0(2)、9.1(2)	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。 （注） ログイン パスワードが使用されるのは、Telnet ユーザー認証を設定しない場合の Telnet に対してのみです。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元していました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 変更された ASDM 画面はありません。
パスワード暗号化の可視性	8.4(1)	**show password encryption** コマンドが変更されました。
マスターパスフレーズ	8.3(1)	この機能が導入されました。マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。 次の画面が導入されました。 **[Configuration] > [Device Management] > [Advanced] > [Master Passphrase]**。 **[Configuration] > [Device Management] > [Device Administration] > [Master Passphrase]**。



第 23 章

DHCP サービスと DDNS サービス

この章では、ダイナミック DNS（DDNS）のアップデート方式のほか、DHCP サーバーまたは DHCP リレーを設定する方法について説明します。

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。Secure Firewall ASA は、Secure Firewall ASA インターフェイスに接続されている DHCP クライアントに、DHCP サーバーを提供します。DHCP サーバは、ネットワーク構成パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたア

イテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 では、デフォルト ルートが設定されます。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションにより、DNS、WINS、ドメイン名のパラメータを DHCP クライアントに提供できます。DNS ドメイン サフィックスには DHCP オプション 15 が使用されます。これらの値は DHCP 自動構成設定を使用して取得するか、または手動で定義できます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動構成設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動構成を有効にできます。DHCP 自動構成によって、DNS サーバーおよび WINS サーバーとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバー名および WINS サーバー名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCPv6 ステートレス サーバーについて

ステートレス アドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6 プレフィックス委任クライアントの有効化（694 ページ））については、これらのクライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER

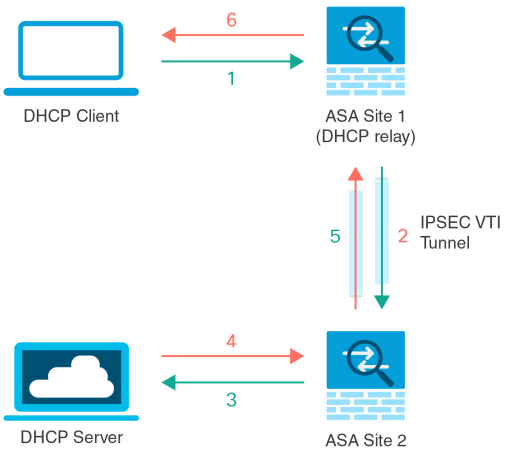
メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワークセグメントにクライアントがある場合、Secure Firewall ASA はブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェントを使用して、ブロードキャストを受信している Secure Firewall ASA のインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定できます。

VTI での DHCP リレーサーバーのサポート

DHCP クライアントと DHCP サーバーの間で DHCP メッセージを受信して転送するように、ASA インターフェイスで DHCP リレーエージェントを設定できます。ただし、論理インターフェイスを介してメッセージを転送する DHCP リレーサーバーはサポートされていませんでした。

次の図は、VTI VPN 経由の DHCP リレーを使用した DHCP クライアントと DHCP サーバーの DISCOVER プロセスを示しています。ASA サイト 1 の VTI インターフェイスに設定された DHCP リレーエージェントは、DHCP クライアントから DHCPDISCOVER パケットを受信し、VTI トンネルを介してパケットを送信します。ASA サイト 2 は DHCPDISCOVER パケットを DHCP サーバーに転送します。DHCP サーバーは ASA サイト 2 に DHCPOFFER で応答します。この応答が ASA サイト 2 から DHCP リレー（ASA サイト 1）に転送され、そこから DHCP クライアントに転送されます。

図 *62 : VTI* を介した *DHCP* リレーサーバー



DHCPREQUEST および DHCPACK/NACK の要件についても同じ手順に従います。

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCP および DDNS サービスを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モード

- DHCPv6 ステートレス サーバは、マルチ コンテキスト モードではサポートされません。

ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。
- DHCP サーバーは、ブリッジ グループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。 ルーテッド モードでは、DHCP サーバーは BVI インターフェイスでサポートされますが、ブリッジ グループ メンバー インターフェイスではサポートされません。DHCP サーバーを動作させるために、BVI には名前が必要です。
- DDNS は、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。
- DHCPv6 ステートレス サーバーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。

クラスタリング

- DHCPv6 ステートレス サーバは、クラスタリングではサポートされません。

IPv6

DHCP ステートレス サーバーの IPv6 と DHCP リレーをサポートします。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバー、ドメイン名、オプション、ping のタイムアウト、WINS サーバーなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバーによって使用されます。
- インターフェイスで DHCP サーバーも有効になっている場合、そのインターフェイスを DHCP クライアントとして設定することはできません。スタティック IP アドレスを使用する必要があります。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。

- インターフェイスの DHCP アドレスを予約できます。ASA で、クライアントの MAC アドレスに基づいて、アドレスプールから DHCP クライアントに特定のアドレスが割り当てられます。
- Secure Firewall ASA は、QIP DHCP サーバと DHCP プロキシ サービスとの併用をサポートしません。
- DHCP サーバーは、BOOTP 要求をサポートしていません。

DHCPv6 サーバ

DHCPv6 ステートレス サーバは、DHCPv6 アドレス、プレフィックス委任クライアントまたは DHCPv6 リレーが設定されているインターフェイス上で設定できません。

DHCP リレー

- シングルモードとコンテキストごとに、グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。
- シングル モードとコンテキストごとに、10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバーはサポートされません。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- DHCP リレー サービスは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスでは利用できません。ただし、アクセス ルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答が Secure Firewall ASA を通過できるようにするには、2 つのアクセス ルールを設定する必要があります。1 つは内部インターフェイスから外部（UDP 宛先ポート 67）への DCHP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバーからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 Secure Firewall ASA に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、Secure Firewall ASA は別のリレー サーバーからのパケットをサポートします。
- DHCP クライアントは、Secure Firewall ASA が要求をリレーする DHCP サーバーとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DHCP サーバーの設定

ここでは、ASA の DHCP サーバーを設定する方法について説明します。

手順

ステップ 1 DHCPv4 サーバーの有効化 （776 ページ）。
ステップ 2 高度な DHCPv4 オプションの設定 （778 ページ）。
ステップ 3 DHCPv6 ステートレス サーバーの設定 （779 ページ）。

DHCPv4 サーバーの有効化

ASA のインターフェイスで DHCP サーバーをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Server]** の順に選択します。
ステップ 2 インターフェイスを選択し、[Edit] をクリックします。

トランスペアレント モードでは、ブリッジ グループ メンバー インターフェイスを選択します。 ルーテッド モードでは、ルーテッド インターフェイスまたは BVI を選択します。ブリッジ グループ メンバー インターフェイスは選択しないでください。

a) 選択したインターフェイス上で DHCP サーバーをイネーブルにするには、[Enable DHCP Server] チェックボックスをオンにします。
b) [DHCP Address Pool] フィールドに、DHCP サーバーが使用する最下位から最上位の IP アドレスの範囲を入力します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
c) [Optional Parameters] 領域で、次の項目を設定します。

- インターフェイスに設定された DNS サーバー（1 および 2）。
- インターフェイスに設定された WINS サーバー（プライマリおよびセカンダリ）。
- インターフェイスのドメイン名。
- インターフェイス上で ASA が ICMP ping の応答を待つ時間（ミリ秒単位）。
- インターフェイス上に設定された DHCP サーバーが、割り当てた IP アドレスの使用を DHCP クライアントに許可する時間。
- 指定のインターフェイス（通常は外側）上で ASA が DHCP クライアントとして動作している場合に、自動コンフィギュレーションのための DNS、WINS、ドメイン名情報を提供する DHCP クライアントのインターフェイス。
- より多くの DHCP オプションを設定するには、[Advanced] をクリックして [Advanced DHCP Options] ダイアログボックスを表示します。詳細については、「高度な DHCPv4 オプションの設定 （778 ページ）」を参照してください。

d) [Dynamic Settings for DHCP Server] 領域の [Update DNS Clients] チェックボックスをオンにして、クライアントの PTR リソース レコードを更新するデフォルトのアクションに加えて、選択した DHCP サーバーでの次の更新アクションの実行を指定します。

- [Update Both Records] チェックボックスをオンにして、DHCP サーバーが A レコードと PTR RR の両方を更新するように指定します。
- [Override Client Settings] チェックボックスをオンにして、DHCP サーバーのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定します。

e) [OK] をクリックして、[Edit DHCP Server] ダイアログボックスを閉じます。

ステップ 3 （任意）（ルーテッド モード）指定したインターフェイス（通常は外側）で ASA が DHCP クライアントとして動作している場合に限り、DHCP 自動コンフィギュレーションをイネーブルにするには、DHCP サーバー テーブルの下にある [Global DHCP Options] 領域の [Enable Auto-configuration from interface] チェックボックスをオンにします。

DHCP 自動コンフィギュレーションでは、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバー、ドメイン名、および WINS サーバーの情報が、DHCP サーバーから DHCP クライアントに提供されます。自動コンフィギュレーションを介して取得された情報が、[Global DHCP Options] 領域でも手動で指定されている場合、検出された情報よりも手動で指定した情報の方が優先されます。

ステップ 4 ドロップダウン リストから [auto-configuration interface] を選択します。

ステップ 5 インターフェイスの DHCP または PPPoE クライアントの WINS パラメータを VPN クライアントのパラメータで上書きするには、[Allow VPN override] チェックボックスをオンにします。

ステップ 6 [DNS Server 1] フィールドに、DHCP クライアント用のプライマリ DNS サーバーの IP アドレスを入力します。

ステップ 7 [DNS Server 2] フィールドに、DHCP クライアント用の代替 DNS サーバーの IP アドレスを入力します。

ステップ 8 [Domain Name] フィールドに、DHCP クライアント用の DNS ドメイン名（たとえば、example.com）を入力します。

ステップ 9 [Lease Length] フィールドに、リースが期限切れになるまでにクライアントが割り当てられた IP アドレスを使用可能な時間を秒数で入力します。有効な値の範囲は、300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。

ステップ 10 [Primary WINS Server] フィールドに、DHCP クライアント用のプライマリ WINS サーバーの IP アドレスを入力します。

ステップ 11 [Secondary WINS Server] フィールドに、DHCP クライアント用の代替 WINS サーバーの IP アドレスを入力します。

ステップ 12 アドレスの衝突を避けるために、ASA は 1 つのアドレスに 2 つの ICMP ping パケットを送信してから、そのアドレスを DHCP クライアントに割り当てます。[Ping Timeout] フィールドに、ASA が DHCP ping の試行のタイムアウトを待つ時間をミリ秒単位で入力します。有効値の範囲は 10 ～ 10000 ミリ秒です。デフォルト値は、50 ミリ秒です。

ステップ 13 追加の DHCP オプションとパラメータを指定するには、[Advanced] をクリックして [Configuring Advanced DHCP Options] ダイアログボックスを表示します。詳細については、高度な DHCPv4 オプションの設定 （778 ページ）を参照してください。

ステップ 14 [Dynamic DNS Settings for DHCP Server] 領域で、DHCP サーバー用の DDNS 更新設定を設定します。[Update DNS Clients] チェックボックスをオンにして、クライアントの PTR リソース レコードを更新するデフォルトのアクションに加えて、選択した DHCP サーバーが次の更新アクションも実行するように指定します。

- [Update Both Records] チェックボックスをオンにして、DHCP サーバーが A レコードと PTR RR の両方を更新するように指定します。
- [Override Client Settings] チェックボックスをオンにして、DHCP サーバーのアクションが、DHCP クライアントによって要求された更新アクションを上書きするように指定します。

ステップ 15 [Apply] をクリックして変更内容を保存します。

高度な DHCPv4 オプションの設定

ASA は、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（1 ～ 255）がサポートされています。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Server]** の順に選択し、[Advanced] をクリックします。

ステップ 2 ドロップダウン リストからオプション コードを選択します。

ステップ 3 設定するオプションを選択します。一部のオプションは標準です。標準オプションの場合、オプション名がオプション番号の後のカッコ内に表示され、オプション番号およびオプション パラメータは、オプションでサポートされるものに制限されます。他のすべてのオプションにはオプション番号だけが表示され、オプションに指定する適切なパラメータを選択する必要があります。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、このオプションに入力できるのは 16 進数値だけです。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できますが、適切なものを選択する必要があります。

ステップ 4 [Option Data] 領域に、このオプションによって DHCP クライアントに返す情報のタイプを指定します。標準 DHCP オプションの場合、サポートされるオプションの値タイプだけが使用可能です。他のすべての DHCP オプションでは、すべてのオプション値タイプを使用できます。[Add] をクリックして、オプションを DHCP オプション リストに追加します。[Delete] をクリックして、オプションを DHCP オプション リストから削除します。

- [IP Address] をクリックして、IP アドレスが DHCP クライアントに返されることを示します。IP アドレスは最大 2 つまで指定できます。IP アドレス 1 および IP アドレス 2 は、ドット付き 10 進数表記の IP アドレスを示します。

（注） 関連付けられた [IP Address] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 3（ルーター）を選択した場合、フィールド名は [Router 1] および [Router 2] に変わります。

- [ASCII] をクリックして、ASCII 値が DHCP クライアントに返されることを指定します。[Data] フィールドに ASCII 文字列を入力します。文字列にスペースを含めることはできません。

  （注） 関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 14（ダンプ ファイル名）を選択した場合、関連付けられた [Data] フィールドの名前は [File Name] に変わります。

- [Hex] をクリックして、16 進数値が DHCP クライアントに返されることを指定します。[Data] フィールドに、偶数個の数字（スペースを含まない）から成る 16 進数文字列を入力します。0x プレフィックスを使用する必要はありません。

  （注） 関連付けられた [Data] フィールドの名前は、選択した DHCP オプションに基づいて変わります。たとえば、DHCP オプション 2（タイム オフセット）を選択した場合、関連付けられた [Data] フィールドは [Offset] フィールドになります。

ステップ 5 [OK] をクリックして、[Advanced DHCP Options] ダイアログボックスを閉じます。

ステップ 6 [Apply] をクリックして変更内容を保存します。

DHCPv6 ステートレス サーバーの設定

ステートレス アドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6 プレフィックス委任クライアントの有効化（694 ページ））については、これらのクライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

始める前に

この機能は、シングル ルーテッド モードでのみサポートされます。この機能は、クラスタリングではサポートされていません。

手順

ステップ 1 DHCPv6 サーバーに提供させる情報が含まれる IPv6 DHCP プールを設定します。

a) **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Pool]** の順に選択し、[Add] をクリックします。

b) [TCP Map Name] フィールドに TCP マップ名を入力します。

c) 各タブのパラメータごとに、[Import] チェックボックスをオンにするか、フィールドに手動で値を入力して [Add] をクリックします。

[Import] オプションを指定すると、プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバーから取得した 1 つ以上のパラメータが使用されます。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じパラメータを手動で設定し、かつ [Import] を指定してインポートすることはできません。

d) [OK]、続いて [Apply] をクリックします。

ステップ 2 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 3 インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 4 [IPv6] タブをクリックします。

ステップ 5 [Interface IPv6 DHCP] 領域で、[Server DHCP Pool Name] オプション ボタンをクリックし、IPv6 DHCP プール名を入力します。

ステップ 6 [Hosts should use DHCP for non-address config] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。

このフラグは、DHCPv6 から DNS サーバー アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

ステップ 7 [OK] をクリックします。

[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] ペインに戻ります。

ステップ 8 [適用（Apply）] をクリックします。

DHCP リレー エージェントの設定

インターフェイスに DHCP 要求が届くと、ユーザーの設定に基づいて、ASA からその要求がリレーされる DHCP サーバーが決定されます。設定できるサーバーのタイプは次のとおりです。

- インターフェイス固有の DHCP サーバー：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバーにだけリレーします。
- グローバル DHCP サーバー：インターフェイス固有のサーバーが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバル サーバーは使用されません。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Relay]** の順に選択します。

ステップ 2 [DHCP Relay Agent] 領域で、各インターフェイスに必要なサービスのチェックボックスをオンにします。

- [IPv4] > [DHCP Relay Enabled]。
- [IPv4] > [Set Route]：サーバーからの DHCP メッセージのデフォルト ゲートウェイ アドレスを、元の DHCP 要求をリレーした DHCP クライアントに最も近い ASA インターフェイスのアドレスに変更します。このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバーで異なるルータが指定されている場合でも、ASA をポイントすることができます。パケット内にデフォルトのルータ オプションがなければ、ASA は、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。
- [IPv6] > [DHCP Relay Enabled]。
- [Trusted Interface]：信頼する DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。[Set dhcp relay information as trusted on all interfaces] チェックボックスをオンにして、すべてのインターフェイスを信頼することもできます。

ステップ 3 [Global DHCP Relay Servers] 領域に、DHCP 要求をリレーする 1 つまたは複数の DHCP サーバーを追加します。

a) [Add] をクリックします。[Add Global DHCP Relay Server] ダイアログボックスが表示されます。
b) [DHCP Server] フィールドに、DHCP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。
c) [Interface] ドロップダウン リストから、指定した DHCP サーバーが接続されているインターフェイスを選択します。
d) [OK] をクリックします。

新たに追加されたグローバル DHCP リレー サーバーが、[Global DHCP Relay Servers] リストに表示されます。

ステップ 4 （オプション）[IPv4 Timeout] フィールドに、DHCPv4 アドレス処理のために許容する時間を秒数で入力します。有効な値の範囲は、1 ～ 3600 秒です。デフォルト値は 60 秒です。

ステップ 5 （オプション）[IPv6 Timeout] フィールドに、DHCPv6 アドレス処理のために許容する時間を秒数で入力します。有効な値の範囲は、1 ～ 3600 秒です。デフォルト値は 60 秒です。

ステップ 6 [DHCP Relay Interface Servers] 領域で、特定のインターフェイスの DHCP 要求がリレーされるインターフェイス固有の DHCP サーバーを 1 台以上追加します。

a) [Add] をクリックします。[Add DHCP Relay Server] ダイアログボックスが表示されます。
b) [Interface] ドロップダウンリストから、DHCP クライアントが接続されているインターフェイスを選択します。グローバル DHCP サーバーの場合とは異なり、要求の出力インターフェイスを指定しないことに注意してください。代わりに、ASA はルーティング テーブルを使用して出力インターフェイスを決定します。
c) [Server to] フィールドに DHCP サーバーの IPv4 アドレスを入力し、[Add] をクリックします。サーバーが右側のリストに追加されます。全体の最大数に余裕があれば、4 台までサーバーを追加します。インターフェイス固有のサーバーでは、IPv6 はサポートされていません。
d) [OK] をクリックします。

新しく追加したインターフェイスの DHCP リレー サーバーが、[DHCP Relay Interface Server] リストに表示されます。

ステップ 7 すべてのインターフェイスを信頼するインターフェイスとして設定するには、[Set dhcp relay information as trusted on all interfaces] チェックボックスをオンにします。あるいは、個々のインターフェイスを信頼することもできます。

ステップ 8 [Apply] をクリックして設定値を保存します。

ダイナミック DNS の設定

インターフェイスで DHCP IP アドレッシングを使用している場合、DHCP リースが更新されると、割り当てられた IP アドレスが変更されることがあります。完全修飾ドメイン名（FQDN）を使用してインターフェイスに到達できる必要がある場合、この IP アドレスの変更が原因で DNS サーバーのリソースレコード（RR）が古くなる可能性があります。ダイナミック DNS（DDNS）は、IP アドレスまたはホスト名が変更されるたびに DNS の RR を更新するメカニズムです。DDNS はスタティックまたは PPPoE IP アドレッシングにも使用できます。

DDNS では DNS サーバーの A RR と PTR RR を更新します。A RR には名前から IP アドレスへのマッピングが含まれ、PTR RR でアドレスが名前にマッピングされます。

ASA では、RFC 2136 で定義されている DDNS 更新方式をサポートしています。Web 更新方式はサポートされていません。この方式では、ASA と DHCP サーバーで DNS 要求を使用して DNS の RR を更新します。ASA または DHCP サーバーは、ローカル DNS サーバーにホスト名に関する情報を求める DNS 要求を送信し、その応答に基づいて RR を所有するメイン DNS サーバーを特定します。その後、ASA または DHCP サーバーからメイン DNS サーバーに更新要求が直接送信されます。一般的なシナリオを次に示します。

- ASA で A RR を更新し、DHCP サーバーで PTR RR を更新する。

  通常、ASA が A RR を「所有」し、DHCP サーバーが PTR RR を「所有」するため、両方のエンティティで個別に更新を要求する必要があります。IP アドレスまたはホスト名が変更されると、ASA から DHCP サーバーに DHCP 要求が送信され、PTR RR の更新を要求する必要があることが通知されます。

- DHCP サーバーで A RR と PTR RR の両方を更新する。

  このシナリオは、ASA に A RR を更新する権限がない場合に使用します。IP アドレスまたはホスト名が変更されると、ASA から DHCP サーバーに DHCP 要求が送信され、A RR と PTR RR の更新を要求する必要があることが通知されます。

セキュリティのニーズやメイン DNS サーバーの要件に応じて、異なる所有権を設定できます。たとえば、スタティックアドレスの場合、ASA で両方のレコードの更新を所有します。

（注） DDNS は BVI またはブリッジグループのメンバーインターフェイスではサポートされません。

始める前に

- **[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** で DNS サーバーを設定します。「DNS サーバーの設定 （759 ページ）」を参照してください。
- **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** でデバイスのホスト名とドメイン名を設定します。「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （749 ページ）」を参照してください。インターフェイスごとにホスト名を指定しない場合は、デバイスのホスト名が使用されます。FQDN を指定しない場合、スタティックまたは PPPoE IP アドレッシングにおいては、システムのドメイン名または DNS サーバーのドメイン名がホスト名に追加されます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[DNS]** > **[Dynamic DNS]** の順に選択します。

ステップ 2 ASA からの DNS 要求を有効にするように DDNS 更新方式を設定します。

すべての要求を DHCP サーバーで実行する場合は、DDNS 更新方式を設定する必要はありません。

a) [Update Methods] 領域で、[Add] をクリックします。
b) [Name] で、このメソッドの名前を指定します。
c) （任意） [Update Interval] で、DNS 要求の更新間隔を設定します。デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、[Days]（0 ～ 364）、[Hours]、[Minutes]、[Seconds] で間隔を設定します。
d) [Records to Update] で、ASA で更新する標準の DDNS レコードを指定します。

   この設定は、ASA から直接更新するレコードにのみ影響します。 DHCP サーバーで更新するレコードを指定するには、インターフェイスごとまたはグローバルに DHCP クライアント設定を行います。ステップ 3 （784 ページ）を参照してください。

- [Both (PTR and A records)]：ASA で A RR と PTR RR の両方を更新するように設定します。スタティックまたは PPPoE IP アドレッシングには、このオプションを使用します。
- [A records only]：ASA で A RR のみを更新するように設定します。DHCP サーバーで PTR RR を更新する場合は、このオプションを使用します。

e) [OK] をクリックします。
f) この方式をステップ 3 （784 ページ）でインターフェイスに割り当てます。

ステップ 3 DDNS のインターフェイス設定として、このインターフェイスの更新方式、DHCP クライアント設定、ホスト名などを設定します。

a) [Dynamic DNS Interface Settings] 領域で、[Add] をクリックします。
b) ドロップダウンリストから [Interface] を選択します。
c) [Method Name] で、[Update Methods] 領域で作成した方式の名前を選択します。

すべての更新を DHCP サーバで実行する場合は、方式を割り当てる必要はありません。

d) [Hostname] で、このインターフェイスのホスト名を設定します。

ホスト名を設定しない場合は、デバイスのホスト名が使用されます。FQDN を指定しない場合、システムのドメイン名または DNS サーバーグループのデフォルトのドメイン（スタティックまたは PPPoE IP アドレッシングの場合）、または DHCP サーバーのドメイン名（DHCP IP アドレッシングの場合）が追加されます。

e) [DHCP Server Record Updates] で、DHCP サーバで更新するレコードを指定します。

ASA から DHCP サーバーに DHCP クライアント要求が送信されます。DHCP サーバーも DDNS をサポートするように設定する必要があることに注意してください。サーバーはクライアント要求を受け入れるように設定できるほか、クライアントをオーバーライドすることもできます（この場合、サーバーで実行している更新をクライアントで実行しないようにクライアントに応答します）。クライアントで DDNS 更新を要求しなくても、DHCP サーバーから更新を送信するように設定できます。

スタティックまたは PPPoE IP アドレッシングの場合、これらの設定は無視されます。

（注） これらの値は、メインの [Dynamic DNS] ページで、すべてのインターフェイスに対してグローバルに設定することもできます。インターフェイスごとの設定は、グローバル設定よりも優先されます。

- [Default (PTR Records)]：DHCP サーバで PTR RR の更新を実行するように要求します。この設定は、[A Records] を有効にした DDNS 更新方式と連携して機能します。
- [Both (PTR Records and A Records)]：DHCP サーバーで A RR と PTR RR の両方の更新を実行するように要求します。この設定では、DDNS 更新方式をインターフェイスに関連付ける必要はありません。
- [None]：DHCP サーバで更新を実行しないように要求します。この設定は、[Both A and PTR Records] を有効にした DDNS 更新方式と連携して機能します。

f) [OK] をクリックします。

ステップ 4 変更を保存するには [Apply] をクリックし、変更を破棄して新しく入力するには [Reset] をクリックします。

DHCP および DDNS サービスのモニターリング

この項では、DHCP および DDNS の両方のサービスをモニターする手順について説明します。

DHCP サービスのモニターリング

- [Monitoring] > [Interfaces] > [DHCP] > [DHCP Client Lease Information]

  このペインには、設定されている DHCP クライアントの IP アドレスが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table]**

  このペインには、設定されている動的な DHCP クライアントの IP アドレスが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Statistics]**

  このペインには、DHCPv4 メッセージのタイプ、カウンタ、値、方向、受信メッセージ数、および送信メッセージ数が表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Relay Statistics]**

  このペインには、DHCPv6 Relay メッセージのタイプ、カウンタ、値、方向、受信メッセージ数、および送信メッセージ数が表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Relay Binding]**

  このペインには、DHCPv6 Relay バインディングが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Interface Statistics]**

  この画面は、すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバー構成用に設定されている場合（DHCPv6 ステートレス サーバーの設定 （779 ページ） を参照）、この画面はサーバーによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、この画面は各クライアントの状態とサーバーから受信した値を表示します。この画面は、DHCP サーバーまたはクライアントのメッセージの統計情報も表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP HA Statistics]**

  この画面は、DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバー ユニット間のトランザクションの統計情報を表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Server Statistics]**

この画面は、DHCPv6 ステートレス サーバーの統計情報を表示します。

DDNS ステータスのモニターリング

DDNS ステータスのモニタリングについては、次のコマンドを参照してください。[Tools] > [Command Line Interface] でコマンドを入力します。

- **show ddns update** { **interface** *if_name* | **method** [*name*]}

  このコマンドは、DDNS 更新ステータスを表示します。

  次の例は、DDNS 更新方式の詳細を示しています。

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  次の例は、DDNS インターフェイスに関する情報を示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

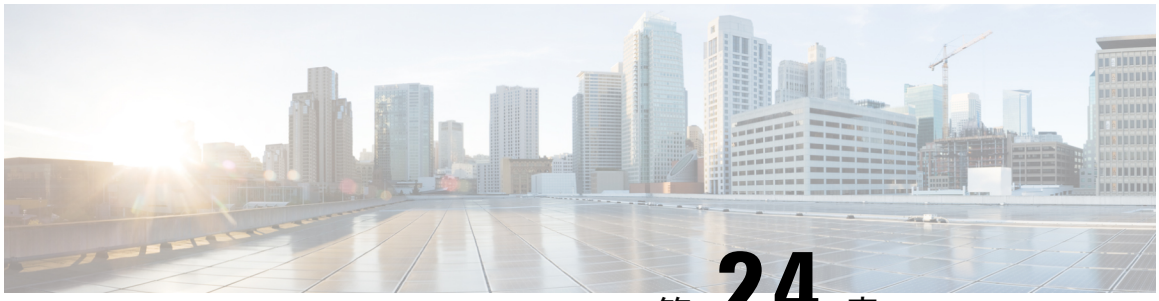
DHCP および DDNS サービスの履歴

機能名	プラットフォームリリース	説明
VTI での DHCP リレーサーバーのサポート	9.14(1)	ASA でインターフェイスを接続する DHCP リレーサーバーとして VTI インターフェイスがサポートされます。 DHCP リレーに VTI インターフェイスを選択できるように次の画面が変更されました。 **[Configuration] > [Device Management] > [DHCP] > [DHCP Relay] > [DHCP Relay Interface Servers]**
DHCP の予約	9.13(1)	ASA で DHCP の予約がサポートされます。DHCP サーバーで、クライアントの MAC アドレスに基づいて、定義されたアドレスプールから DHCP クライアントにスタティック IP アドレスが割り当てられます。 変更された ASDM 画面はありません。

機能名	プラットフォームリリース	説明
IPv6 DHCP	9.6(2)	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバーから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバー：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次の画面が追加または変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [IPv6]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Pool]** **[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] > [Networks]** **[Monitoring] > [interfaces] > [DHCP]**
DHCPv6 モニターリング	9.4(1)	IPv6 の DHCP 統計情報および IPv6 の DHCP バインディングをモニターできます。 次の画面が導入されました。[DHCPv6 monitoring] [Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Statistics, Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Binding]。
DHCP リレー サーバーは、応答用の DHCP サーバー識別子を確認します。	9.2(4)/ 9.3(3)	ASA DHCP リレー サーバーが不適切な DHCP サーバーから応答を受信すると、応答を処理する前に、その応答が適切なサーバーからのものであることを確認するようになりました。導入または変更されたコマンドはありません。変更された ASDM 画面はありません。 変更された ASDM 画面はありません。

機能名	プラットフォームリリース	説明
DHCP 再バインド機能	9.1(4)	DHCP 再バインド フェーズに、クライアントはトンネル グループ リスト内の他の DHCP サーバーへの再バインドを試みるようになりました。このリリース以前には、DHCP リースの更新に失敗した場合、クライアントは代替サーバーへ再バインドしませんでした。 変更された ASDM 画面はありません。
DHCP の信頼できるインターフェイス	9.1(2)	DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
インターフェイスごとの DHCP リレー サーバー（IPv4 のみ）	9.1(2)	DHCP リレー サーバーをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサーバーに対してのみリレーされます。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
DHCP relay for IPv6 (DHCPv6)	9.0(1)	DHCP リレーに IPv6 サポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。
DDNS	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [DNS] > [DNS Client] [Configuration] > [Device Management] > [DNS] > [Dynamic DNS]

機能名	プラットフォームリリース	説明
DHCP	7.0(1)	ASA は、DHCP サーバーまたは DHCP リレー サービスを ASA のインターフェイスに接続されている DHCP クライアントに提供することができます。 次の画面が導入されました。 [Configuration] > [Device Management] > [DHCP] > [DHCP Relay]。 [Configuration] > [Device Management] > [DHCP] > [DHCP Server]



第 24 章

デジタル証明書

この章では、デジタル証明書の設定方法について説明します。

デジタル証明書の概要

デジタル証明書は、認証に使用されるデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。CA は、証明書要求の管理とデジタル証明書の発行を行います。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。

デジタル証明書には、ユーザーまたはデバイスの公開キーのコピーも含まれています。CA は、信頼できるサードパーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。ASA では CRL（認証局の失効リストとも呼ばれます）に照らしてサードパーティの証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

- ID証明書は、特定のシステムまたはホストの証明書です。この証明書もCAにより発行されます。
- コード署名者証明書は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。

ローカルCAは、ASAの独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Web サイトのログイン ページからユーザー登録を行う場合には、ローカル CA により実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。

（注） CA 証明書および ID 証明書は、サイトツーサイト VPN 接続およびリモート アクセス VPN 接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUI でリモート アクセス VPN を使用する場合の手順です。

ヒント 証明書コンフィギュレーションおよびロード バランシングの例は、次の URL を参照してください。https://supportforums.cisco.com/docs/DOC-5964

公開キー暗号化

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザーを認証する手段です。RSA 暗号化システムなどの Public Key Cryptography では、各ユーザーは、公開キーと秘密キーの両方を含むキーペアを使用します。これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号できます。

簡単に言えば、データが秘密キーで暗号化されたとき、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPsec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

証明書のスケーラビリティ

デジタル証明書がない場合、通信するピアごとに各 IPsec ピアを手動で設定する必要があります。そのため、ネットワークにピアを新たに追加するたびに、安全に通信するために各ピアで設定変更を行わなければなりません。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPSec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモート ピアに証明書を送り、公開キー暗号化を実行することによって、そのリモート ピアに対して自分自身を認証します。各ピアから、CA によって発行された固有の証明書が送信されます。このプロセスが機能を果たすのは、関連付けられているピアの公開キーが各証明書にカプセル化され、各証明書が CA によって認証され、参加しているすべてのピアによって CA が認証権限者として認識されるためです。このプロセスは、RSA 署名付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPSec セッションに対して、および複数の IPSec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPSec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CA の中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバーであるため、CA が使用できないときも CA 機能は継続しています。

キーペア

キー ペアは、RSA または楕円曲線署名アルゴリズム（ECDSA）キーであり、次の特性があります。

- RSA キーは SSH や SSL に使用できます。
- SCEP 登録は、RSA キーの証明書をサポートしています。
- RSA キー サイズの最大値は 4096 で、デフォルトは 2048 です。
- ECDSA キー長の最大値は 521 で、デフォルトは 384 です。
- 署名にも暗号化にも使用できる汎用 RSA キー ペアを生成することも、署名用と暗号化用に別々の RSA キー ペアを生成することもできます。SSL では署名用ではなく暗号化用のキーが使用されるので、署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。ただし、IKE では暗号化用ではなく署名用のキーが使用されます。キーを用途別に分けることで、キーの公開頻度が最小化されます。

トラストポイント

トラストポイントを使用すると、CA と証明書の管理およびトラックを行えます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。

（注） Cisco ASA に同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザー証明書の検証に使用できるのは 1 つだけです。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザー証明書を検証するかを制御するには、**support-user-cert-validation** コマンドを使用します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があり、また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

認証登録

ASA は、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティ アプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、ASA には署名用と暗号化用の 2 つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は 1 つだけです。

ASA は、SCEP を使用した自動登録と、base-64-encoded 証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイト VPN の場合は、各 ASA を登録する必要があります。リモート アクセス VPN の場合は、各 ASA と各リモート アクセス VPN クライアントを登録する必要があります。

SCEP 要求のプロキシ

ASA は、AnyConnect とサードパーティ CA 間の SCEP 要求のプロキシとして動作することができます。プロキシとして動作する場合に必要なのは CA が ASA からアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザーが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA は、AnyConnect SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、Cisco IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠 CA をサポートしています。

クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）はサポートしていません。

ASA は、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

失効チェック

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効確認を有効にすることにより、CA が認証にその証明書を使用するたびに、その証明書が無効にされていないかどうか、ASA によってチェックされます。

失効確認を有効にすると、PKI 証明書検証プロセス時に ASA によって証明書の失効ステータスがチェックされます。これには、CRL チェック、OCSP、またはその両方が使用されます。OCSP は、最初の方式がエラーを返した場合に限り使用されます（たとえば、サーバーが使用不可であることを示すエラー）。

CRL チェックを使用すると、ASA によって、無効になった（および失効解除された）証明書とその証明書シリアル番号がすべてリストされている CRL が取得、解析、およびキャッシュされます。ASA は CRL（認証局の失効リストとも呼ばれます）に基づいて証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

OCSP は、検証局に特定の証明書のステータスを問い合わせ、チェックを検証局が扱う範囲に限定するため、よりスケーラブルな方法を提供します。

サポート対象の CA サーバー

ASA は次の CA サーバーをサポートしています。

Cisco IOS CS、ASA ローカル CA、およびサードパーティの X.509 準拠 CA ベンダー（次のベンダーが含まれますが、これらに限定はされません）。

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon

- Thawte
- VeriSign

CRL

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための1つの方法です。CRLコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

証明書を認証するときに必ず **revocation-check crl** コマンドを使用して CRL チェックを行うように、ASA を設定できます。また、**revocation-check crl none** コマンドを使用して、CRL チェックをオプションにすることもできます。オプションにすると、更新された CRL データが CA から提供されない場合でも、証明書認証は成功します。

（注） **revocation-check crl none** は削除されました。

ASA は HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な時間だけキャッシュされます。

（注） CRL サーバは HTTP フラグ「Connection: Keep-alive」で応答して永続的な接続を示しますが、ASA は永続的な接続のサポートを要求しません。リストの送信時に「Connection: Close」と応答するように、CRL サーバの設定を変更します。

CRL のキャッシュに設定された時間を超過して ASA にキャッシュされている CRL がある場合、ASA はその CRL を、古すぎて信頼できない、つまり「失効した」と見なします。ASA は、次回の証明書認証で失効した CRL のチェックが必要な場合に、より新しいバージョンの CRL を取得しようとします。

CRL の 16 MB のサイズ制限を超えると、ユーザー接続/証明書で失効チェックエラーが表示されることがあります。

ASA によって CRL がキャッシュされる時間は、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。
- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。ASA が NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

ASA では、これらの 2 つの要素が次のように使用されます。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、ASA は CRL に失効のマークを付けます。

- NextUpdate フィールドが必要な場合、ASA は、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、**cache-time** コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、ASA は 70 分後に CRL に失効のマークを付けます。

ASA がメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。大規模な CRL では、解析に大量の計算オーバーヘッドが必要です。したがって、パフォーマンスを向上させるには、少数の大規模な CRL ではなく、小さいサイズの CRL を多数使用するか、または OCSP を使用することを推奨します。

キャッシュサイズは次のとおりです。

- シングルコンテキストモード：128 MB
- マルチコンテキストモード：コンテキストあたり 16 MB

OCSP

OCSP は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。OCSP のコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

OCSP によって、証明書のステータスをチェックする範囲が検証局（OCSP サーバー、応答側とも呼ばれます）に限定され、ASA によって検証局に特定の証明書のステータスに関する問い合わせが行われます。これは、CRL チェックよりもスケーラブルで、最新の失効ステータスを確認できる方法です。この方法は、PKI の導入規模が大きい場合に便利で、安全なネットワークを拡大できます。

（注） ASA では、OCSP 応答に 5 秒間のスキューを許可します。

証明書を認証するときに必ず **revocation-check ocsp** コマンドを使用して OCSP チェックを行うように、ASA を設定できます。また、**revocation-check ocsp none** コマンドを使用して、OCSP チェックをオプションにすることもできます。オプションにすると、更新された OCSP データが検証局から提供されない場合でも、証明書認証は成功します。

（注） **revocation-check ocsp none** は削除されました。

OCSP を利用すると、OCSP サーバーの URL を 3 つの方法で定義できます。ASA は、これらのサーバーを次の順に使用します。

1. **match certificate** コマンドの使用による証明書の照合の上書きルールで定義されている OCSP サーバーの URL
2. **ocsp url** コマンドを使用して設定されている OCSP サーバーの URL

3. クライアント証明書の AIA フィールド

（注） トラストポイントでOCSPの応答側の自己署名した証明書を検証するように設定するには、信頼できるCA証明書として、この自己署名した応答側の証明書をそのトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSP の応答側の自己署名された証明書を含むトラストポイントを使用するようにします。クライアント証明書の検証パスの外部にある応答側の証明書を検証する場合も、同じ手順で設定します。

通常、OCSP サーバー（応答側）の証明書によって、OCSP 応答が署名されます。ASA が応答を受け取ると、応答側の証明書を検証しようとします。通常、CA は、侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。ただし、この拡張がない場合、ASAはトラストポイントで指定されている方法で失効ステータスをチェックします。応答側の証明書を検証できない場合、失効ステータスをチェックできなくなります。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。

証明書とユーザー ログイン クレデンシャル

この項では、認証と認可に証明書およびユーザー ログイン クレデンシャル（ユーザー名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPSec、AnyConnect、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP認可では、パスワードをクレデンシャルとして使用しません。RADIUS認可では、すべてのユーザーの共通パスワードまたはユーザー名のいずれかを、パスワードとして使用します。

ユーザー ログイン クレデンシャル

認証および認可のデフォルトの方法では、ユーザー ログイン クレデンシャルを使用します。

- 認証
  - トンネル グループ（ASDM接続プロファイルとも呼ばれます）の認証サーバー グループ設定によりイネーブルにされます。
  - ユーザー名とパスワードをクレデンシャルとして使用します。
- 認証
  - トンネル グループ（ASDM接続プロファイルとも呼ばれます）の認可サーバー グループ設定によりイネーブルにされます。
  - ユーザー名をクレデンシャルとして使用します。

証明書

ユーザーデジタル証明書が設定されている場合、ASAによって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザー名として使用されません。

認証と認可の両方がイネーブルになっている場合、ASAによって、ユーザーの認証と認可の両方にユーザー ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバー グループ設定によってイネーブルにされます。
  - ユーザー名とパスワードをクレデンシャルとして使用します。
- 認証
  - 認可サーバー グループ設定によってイネーブルにされます。
  - ユーザー名をクレデンシャルとして使用します。

認証がディセーブルで認可がイネーブルになっている場合、ASA によって認可にプライマリ DN のフィールドが使用されます。

- 認証
  - 認証サーバー グループ設定によってディセーブル（[None] に設定）になります。
  - クレデンシャルは使用されません。
- 認証
  - 認可サーバー グループ設定によってイネーブルにされます。
  - 証明書のプライマリ DN フィールドのユーザー名の値をクレデンシャルとして使用します。

（注） 証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンデリ DN のフィールド値が認可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザー証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA（電子メール アドレス）およびセカンデリ DN = CN（一般名）の場合、許可要求で使われるユーザー名は anyuser@example.com になります。

デジタル証明書のガイドライン

この項では、デジタル証明書を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

- サードパーティ CA ではシングル コンテキスト モードでのみサポートされています。

フェールオーバーのガイドライン

- ステートフル フェールオーバーではセッションの複製はサポートされません。
- ローカル CA のフェールオーバーはサポートされません。
- ステートフル フェールオーバーを設定すると、証明書は自動的にスタンバイユニットにコピーされます。証明書がない場合は、アクティブユニットで **write standby** コマンドを使用します。

IPv6 のガイドライン

IPv6 はサポートされません。

ローカル CA 証明書

- 証明書をサポートするように ASA が正しく設定されていることを確認します。ASA の設定が正しくないと、登録に失敗したり、不正確な情報を含む証明書が要求されたりする可能性があります。
- ASA のホスト名とドメイン名が正しく設定されていることを確認します。現在設定されているホスト名とドメイン名を表示するには、**show running-config** コマンドを入力します。
- CA を設定する前に、ASA のクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。ASA が CA に登録して証明書を取得するとき、ASA は現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。
- ローカル CA 証明書の有効期限の 30 日前に、ロールオーバー代替証明書が生成され、syslog メッセージ情報で管理者にローカル CA のロールオーバーの時期であることが知らされます。新しいローカル CA 証明書は、現在の証明書が有効期限に達する前に、必要なすべてのデバイスにインポートする必要があります。管理者が、新しいローカル CA 証明書としてロールオーバー証明書をインストールして応答しない場合、検証が失敗する可能性があります。
- ローカル CA 証明書は、同じキーペアを使用して期限満了後に自動的にロールオーバーします。ロールオーバー証明書は、base 64 形式でエクスポートに使用できます。

  次に、base 64 で符号化されたローカル CA 証明書の例を示します。

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP プロキシ サポート

- ASA と Cisco ISE ポリシー ノードが、同じ NTP サーバーを使用して同期されていることを確認します。
- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- グループ ポリシーの接続プロファイルで設定される認証方式は、AAA 認証と証明書認証の両方を使用するように設定する必要があります。
- SSL ポートが、IKEv2 VPN 接続用に開いている必要があります。
- CA は、自動許可モードになっている必要があります。

その他のガイドライン

- 使用できる証明書のタイプは、証明書を使用するアプリケーションでサポートされている証明書タイプによって制約されます。RSA 証明書は通常、証明書を使用するすべてのアプリケーションでサポートされます。ただし、EDDSA 証明書は、ワークステーションのオペレーティングシステム、ブラウザ、ASDM、または AnyConnect ではサポートされない場合があります。たとえば、リモートアクセス VPN の ID および認証には RSA 証明書を使用する必要があります。ASA が証明書を使用するアプリケーションであるサイト間 VPN の場合は、EDDSA がサポートされます。
- ASA が CA サーバーまたはクライアントとして設定されている場合、推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期を制限してください。このガイドラインは、サードパーティ ベンダーからインポートした証明書にも適用されます。
- ASA は、次の認定条件のいずれかが満たされている場合にのみ LDAP/SSL 接続を確立します。
  - LDAP サーバー証明書が信頼されていて（トラストポイントまたは ASA トラストプールに存在する）、有効であること。
  - チェーンを発行しているサーバーからの CA 証明書が信頼されていて（トラストポイントまたは ASA トラストプールに存在する）、チェーン内のすべての下位 CA 証明書が完全かつ有効であること。

- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。キー サイズは 2048 以上を使用することをお勧めします。
- 管理インターフェイスへの ASDM トラフィックと HTTPS トラフィックを保護するために、アイデンティティ証明書を使用するよう ASA を設定する必要があります。SCEP により自動的に生成される ID 証明書はリブートのたびに再生成されるため、必ず独自の ID 証明書を手動でインストールしてください。SSL のみに適用されるこのプロシージャの例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA および AnyConnect クライアントで検証できるのは、[X520Serialnumber] フィールド（[Subject Name] のシリアル番号）が PrintableString 形式である証明書のみです。シリアル番号の形式に UTF8 などのエンコーディングが使用されている場合、証明書認証は失敗します。
- ASA でのインポート時は、有効な文字と値だけを証明書パラメータに使用してください。ASA では、これらの証明書が復号化されて内部データ構造に組み込まれます。空白のフィールドがある証明書は、復号化標準に準拠していないと解釈されるため、インストールの検証は失敗します。
- ワイルドカード（*）記号を使用するには、文字列値でこの文字を使用できるエンコードを CA サーバーで使用していることを確認してください。RFC 5280 では UTF8String または PrintableString を使用することを推奨していますが、PrintableString ではこのワイルドカード文字を有効であると認識しないため UTF8String を使用する必要があります。ASA は、インポート中に無効な文字または値が見つかると、インポートした証明書を拒否します。次に例を示します。

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

デジタル証明書の設定

ここでは、デジタル証明書の設定方法について説明します。

参照 ID の設定

ASA が TLS クライアントとして動作する場合、ASA は RFC 6125 で定義されているアプリケーション サーバーの ID の検証ルールをサポートします。この RFC では、参照 ID を表現（ASA 上で設定）し、（アプリケーション サーバーから送信）提示された ID に対して参照 ID を照合する手順を示しています。提示された ID が設定済みの参照 ID と一致しなければ、接続は確立されず、エラーがログに記録されます。

接続の確立中、サーバーは自身の ID を提示するために、1 つ以上の識別子を含めたサーバー証明書を ASA に提示します。ASA で設定される参照 ID は、接続の確立中にサーバー証明書で提示される ID と比較されます。これらの ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。4 つの ID タイプは次のとおりです。

- CN_ID：証明書のサブジェクト フィールドに設定される、共通名（CN）タイプの 1 つの属性タイプと値のペアだけが含まれる相対識別名（RDN）。この値は、完全な形のドメイン名と一致します。CN 値は自由形式のテキストにすることはできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
- DNS-ID：dNSName タイプの subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
- SRV-ID：RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。
- URI-ID：uniformResourceIdentifier タイプの subjectAltName エントリ。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。

参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

始める前に

- 参照 ID は、syslog サーバーおよびスマート ライセンス サーバーへの接続時にのみ使用されます。その他の ASA SSL クライアント モードの接続では、現時点では、参照 ID の設定や使用はサポートされていません。
- 対話式クライアントの固定証明書およびフォールバックを除き、ASA は RFC 6125 で説明されている ID と一致させるためのすべてのルールを実装します。

- 証明書を固定する機能は実装されません。したがって、「No Match Found, Pinned Certificate」メッセージが発生することはありません。また、シスコで実装するクライアントは対話式クライアントではないため、一致が見つからない場合にユーザーが証明書を固定することもできません。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Advanced] > [Reference Identity] に移動します。

設定済みの参照 ID がリストされます。新しい参照 ID を追加するには [Add] をクリックします。既存の参照 ID を編集するには、対象の参照 ID を選択してから [Edit] をクリックします。既存の参照 ID を削除するには、対象の参照 ID を選択してから [Delete] をクリックします。使用中の参照 ID を削除することはできません。

ステップ 2 参照 ID を作成または変更するには、それぞれ [Add]、[Edit] をクリックします。

[Add Reference Identity] または [Edit Reference Identity] ダイアログボックスを使用して、参照 ID を選択および指定します。

- 参照 ID には、任意のタイプの複数の参照 ID を追加できます。
- 参照 ID を設定した後に、その名前を変更することはできません。名前を変更するには、参照 ID を削除してから作成し直す必要があります。

次のタスク

設定した参照 ID は、syslog および Smart Call Home サーバー接続を設定する際に使用します。

特定の証明書タイプの設定方法

信頼できる証明書を確立すると、アイデンティティ証明書の確立などの基本的なタスクや、ローカル CA 証明書やコード署名証明書の確立などのさらに高度な設定を行なえるようになります。

始める前に

デジタル証明書情報に目を通し、信頼できる証明書を確立します。秘密キーが設定されていない CA 証明書は、すべての VPN プロトコルと webvpn で使用され、トラストポイントで着信クライアント証明書を検証するように設定されています。また、トラストポイントとは、HTTPS サーバーにプロキシ接続された接続を検証し、smart-call-home 証明書を検証する、webvpn 機能によって使用される信頼できる証明書の一覧のことです。

手順

ステップ 1 アイデンティティ証明書は、対応する秘密キーとともに ASA に設定される証明書です。これは、SSL サービスや IPsec サービスを確立する際のアウトバウンドの暗号化またはシグネチャの生成に使用され、トラストポイントを登録することによって取得されます。アイデンティティ証明書を設定するには、ID 証明書 （805 ページ） を参照してください。

ステップ 2 ローカル CA を設定すると、VPN クライアントが ASA から証明書を直接登録できるようになります。この高度な設定により、ASA は CA に変換されます。CA を設定するには、CA 証明書 （812 ページ） を参照してください。

ステップ 3 WebVPN Java コード署名機能の一部としてアイデンティティ証明書を使用する場合は、コード署名者証明書 （818 ページ） を参照してください。

次のタスク

証明書の有効期限にアラートを設定するか、デジタル証明書や証明書の管理履歴をモニターします。

ID 証明書

アイデンティティ証明書は、ASA 内の VPN アクセスの認証に使用できます。

[Identity Certificates Authentication] ペインでは、次のタスクを実行できます。

- アイデンティティ証明書の追加またはインポート （805 ページ）。
- CA からの要求として CMPv2 登録の有効化
- ID 証明書の詳細を表示する。
- 既存の ID 証明書を削除する。
- アイデンティティ証明書のエクスポート （810 ページ）。
- 証明書有効期限のアラートを設定する。
- Etrust でアイデンティティ証明書を登録する証明書署名要求の生成 （810 ページ）。

アイデンティティ証明書の追加またはインポート

新しい ID 証明書コンフィギュレーションを追加またはインポートするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[Identity Certificates]** の順に選択します。

ステップ 2 [Add] をクリックします。

選択されたトラストポイント名が上部に示された [Add Identity Certificate] ダイアログボックスが表示されます。

ステップ 3 [Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)] オプション ボタンをクリックして、既存のファイルから ID 証明書をインポートします。

ステップ 4 PKCS12 ファイルの復号化に使用するパスフレーズを入力します。

ステップ 5 ファイルのパス名を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示します。証明書ファイルを見つけて、[Import ID Certificate File] をクリックします。

ステップ 6 [Add a new Global Controller] オプション ボタンをクリックして、新しい ID 証明書を追加します。

ステップ 7 [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。

ステップ 8 **RSA** または **ECDSA** キーのタイプを選択します。

ステップ 9 [Use default keypair name] オプション ボタンをクリックして、デフォルトのキー ペア名を使用します。

ステップ 10 [Enter a new key pair name] オプション ボタンをクリックして、新しい名前を入力します。

ステップ 11 ドロップダウン リストから係数サイズを選択します。係数サイズが不明な場合は、Entrust にお問い合わせください。

ステップ 12 [General purpose] オプション ボタン（デフォルト）または [Special] オプション ボタンをクリックして、キー ペアの用途を選択します。[Special] オプション ボタンを選択すると、ASA により署名用と暗号化用の 2 つのキー ペアが生成されます。この選択は、対応する識別用に 2 つの証明書が必要なことを示します。

ステップ 13 [Generate Now] をクリックして新しいキー ペアを作成し、[Show] をクリックして [Key Pair Details] ダイアログボックスを表示します。ここには、次の表示専用の情報が示されます。

- 公開キーが認証の対象となるキー ペアの名前。
- キー ペアの生成日時。
- RSA キー ペアの用途。
- キーペアのモジュラスサイズ（512、768、1024、2048、および 4096 ビット）。デフォルトは 2048 です。
- テキスト形式の特定のキー データを含むキー データ。

ステップ 14 完了したら、[OK] をクリックします。

ステップ 15 ID 証明書で DN を形成するための証明書サブジェクト DN を選択します。その後、[選択（Select）] をクリックして [証明書件名DN（Certificate Subject DN）] ダイアログボックスを表示します。

ステップ 16 ドロップダウンリストから追加する DN 属性を 1 つ以上選択し、値を入力し、[Add] をクリックします。証明書サブジェクト DN の使用可能な X.500 属性は、次のとおりです。

- **Common Name（CN）**

- **Department（OU）**
- **Company Name（O）**
- **Country（C）**
- **State/Province（ST）**
- **Location（L）**
- **E-mail Address（EA）**

ステップ 17 完了したら、[OK] をクリックします。

ステップ 18 自己署名証明書を作成するには、[Generate self-signed certificate] チェック ボックスをオンにします。

ステップ 19 アイデンティティ証明書をローカル CA として機能させるには、[Act as local certificate authority and issue dynamic certificates to TLS proxy] チェックボックスをオンにします。

ステップ 20 追加のアイデンティティ証明書設定を行うには、[Advanced] をクリックします。

[Certificate Parameters]、[Enrollment Mode]、および [SCEP Challenge Password] の 3 つのタブを持つ [Advanced Options] ダイアログボックスが表示されます。

（注） 登録モード設定と SCEP チャレンジ パスワードは自己署名証明書では使用できません。

ステップ 21 [Certificate Parameters] タブをクリックし、次の情報を入力します。

- DNS ツリー階層内のノードの位置を示す FQDN（完全修飾ドメイン名）。
- ID 証明書に関連付けられている電子メール アドレス。
- 4 分割ドット付き 10 進表記の、ネットワーク上の ASA IP アドレス。
- [Include serial number of the device] チェックボックスをオンにして、ASA のシリアル番号を証明書パラメータに追加します。

ステップ 22 [Enrollment Mode] タブをクリックし、次の情報を入力します。

- [Request by manual enrollment] オプション ボタンまたは [Request from a CA] オプション ボタンをクリックして、登録方式を選択します。[Request from a CA] を選択して CMPV2 登録を有効にする場合は、CA からの要求としての CMPv2 登録の有効化 （808 ページ）を参照してください。
- SCEP を介して自動的にインストールされる証明書の登録 URL。
- ID 証明書のインストールに許可される最大再試行分数。デフォルトは 1 分です。
- ID 証明書のインストールに許可される最大再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 23 [SCEP Challenge Password] タブをクリックし、次の情報を入力します。

- SCEP パスワード
- SCEP パスワードを確認のために再入力

ステップ 24 完了したら、[OK] をクリックします。

ステップ 25 この証明書で他の証明書に署名できるようにする場合は、[Enable CA flag in basic constraints extension] をオンにします。

基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。このオプションをオンのままにしておいても、特に問題はありません。

ステップ 26 [Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificates] リストに新しい ID 証明書が表示されます。

ステップ 27 [Apply] をクリックし、新しい ID 証明書コンフィギュレーションを保存します。

ステップ 28 [Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ステップ 29 ID証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA からの要求としての CMPv2 登録の有効化

LTE ワイヤレス ネットワークでセキュリティ ゲートウェイ デバイスとして機能するために、ASA は Certificate Management Protocol（CMPv2）を使用していくつかの証明書管理機能をサポートします。ASA デバイス証明書の登録に CMPv2 を使用することで、CMPv2 が有効な CA からの最初の証明書とセカンダリ証明書を手動登録したり、同じキーペアを使用する以前に発行済みの証明書を差し替えるための証明書を手動更新したりできます。受信した証明書は従来の設定の外部に保存され、証明書が有効になっている IPsec の設定で使用されます。

（注） ASA では CMPv2 のすべての機能を利用できるわけではありません。

最初の要求で CA との信頼を確立し、最初の証明書を取得します。CA 証明書はトラストポイントで事前に設定される必要があります。インストール中の証明書のフィンガープリントを認知すると、認証が実行されます。

[Advanced Options] ウィンドウの [Enrollment Mode] タブ上で [Request from a CA] をクリックした後、CMPv2 登録のために以下の手順を実行します。

始める前に

アイデンティティ証明書の追加またはインポート （805 ページ） の手順を実行します。

手順

ステップ 1 CMP を登録プロトコルとして選択し、http:// 領域に CMP URL を入力します。

ステップ 2 すべての CMP 手動/自動登録用に自動的に新しいキー ペアを生成するには、[RSA] または [EDCSA] を選択します。

[RSA] を選択した場合、[Modulus] ドロップダウン メニューから値を選択します。[EDCSA] を選択した場合、楕円曲線のドロップダウン メニューから値を選択します。

ステップ 3 （オプション）証明書の更新中、あるいは登録要求の作成前にキー ペアを生成するには、[Regenerate the key pair] をクリックします。

ステップ 4 [Shared Key] をクリックし、CA によってアウトオブバンド提供された値を入力します。この値は、CA および ASA が交換するメッセージの信頼性および整合性を確認するために使用されます。

ステップ 5 [Signing Trustpoint] をクリックし、CMP 登録要求に署名する際に使用された発行済みデバイス証明書を含むトラストポイントの名前を入力します。

これらのオプションは、トラストポイント登録プロトコルが CMP に設定されているときにのみ使用できます。CMP トラストポイントが設定されている場合、共有秘密または署名証明書のいずれかを指定ができますが、両方は指定できません。

ステップ 6 CA 証明書を指定するには [Browse Certificate] をクリックします。

ステップ 7 （オプション）CMPv2 の自動登録を起動するには、[Auto Enroll] チェックボックスをオンにします。

ステップ 8 [Auto Enroll Lifetime] フィールドには、自動登録が必要になるまでの、証明書の絶対的な有効期間のパーセンテージを入力します。

ステップ 9 証明書の更新中に新しいキーを生成するには、[Auto Enroll Regenerate Key] をクリックします。

アイデンティティ証明書のエクスポート

ID 証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 [Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2 証明書コンフィギュレーションをエクスポートするときに使用するPKCS12形式ファイルの名前を入力します。または、[Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 3 [PKCS12 Format] オプション ボタンまたは [PEM Format] オプション ボタンをクリックして、証明書の形式を選択します。

ステップ 4 PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを入力します。

ステップ 5 暗号化パスフレーズを確認のために再入力します。

ステップ 6 [Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

情報ダイアログボックスが表示され、証明書コンフィギュレーション ファイルが指定の場所に正常にエクスポートされたことが示されます。

証明書署名要求の生成

Entrust に送信する証明書署名要求を生成するには、次の手順を実行します。

手順

ステップ 1 [Enroll ASA SSL VPN with Entrust] をクリックして、[Generate Certificate Signing Request] ダイアログボックスを表示します。

ステップ 2 [Key Pair] 領域で次の手順を実行します。

a) ドロップダウン リストから、設定されたキー ペアのいずれかを選択します。

b) [Show] をクリックして [Key Details] ダイアログボックスを表示します。ここには、選択されたキー ペアの生成日時、用途（一般的または特殊な用途）、係数サイズ、およびキーデータといった情報が示されます。

c) 完了したら、[OK] をクリックします。

d) [New] をクリックして、[Add Key Pair] ダイアログボックスを表示します。生成したキーペアを ASA に送信するか、ファイルに保存することができます。

ステップ 3 [Certificate Subject DN] 領域に次の情報を入力します。

a) ASA の FQDN または IP アドレス。

b) 会社の名前。

c) 2 文字の国番号。

ステップ 4 [Optional Parameters] 領域で次の手順を実行します。

a) [Select] をクリックして、[Additional DN Attributes] ダイアログボックスを表示します。
b) ドロップダウンリストから追加する属性を選択し、値を入力します。
c) [Add] をクリックして、各属性を [attribute] テーブルに追加します。
d) [Delete] をクリックして、[attribute] テーブルから属性を削除します。
e) 完了したら、[OK] をクリックします。

[Additional DN Attributes] フィールドに追加された属性が表示されます。

ステップ 5 CA から要求された場合は、完全修飾ドメイン名情報を追加で入力します。

ステップ 6 [Generate Request] をクリックして、証明書署名要求を生成します。これを Entrust に送信することも、ファイルに保存して後で送信することもできます。

CSR が示された [Enroll with Entrust] ダイアログボックスが表示されます。

ステップ 7 [request a certificate from Entrust] リンクをクリックして、登録プロセスを完了します。その後、示された CSR をコピーして貼り付け、それを Entrust Web フォーム（http://www.entrust.net/cisco/）を使用して送信します。後で登録する場合は、生成された CSR をファイルに保存し、[Identity Certificates] ペインで [enroll with Entrust] リンクをクリックします。

ステップ 8 Entrust により、要求の認証が確認された後、証明書が発行されます。これには数分かかる場合があります。次に、[Identity Certificate] ペインで保留中の要求を選択し、[Install] をクリックして、証明書をインストールする必要があります。

ステップ 9 [Close] をクリックして、[Enroll with Entrust] ダイアログボックスを閉じます。

アイデンティティ証明書のインストール

新しい ID 証明書をインストールするには、次の手順を実行します。

手順

ステップ 1 [Identity Certificates] ペインで [Add] をクリックし、[Add Identity Certificate] ダイアログボックスを表示します。

ステップ 2 [Add a new identity certificate] オプション ボタンをクリックします。

ステップ 3 キー ペアを変更するか、新しいキー ペアを作成します。キー ペアは必須です。

ステップ 4 証明書サブジェクト DN 情報を入力し、[Select] をクリックして、[Certificate Subject DN] ダイアログボックスを表示します。

ステップ 5 関係する CA で必要なサブジェクト DN 属性をすべて指定し、[OK] をクリックして [Certificate Subject DN] ダイアログボックスを閉じます。

ステップ 6 [Add Identity Certificate] ダイアログボックスで、[Advanced] をクリックして [Advanced Options] ダイアログボックスを表示します。

ステップ 7 以降の手順については、アイデンティティ証明書の追加またはインポート（805 ページ）の手順 17 ～ 23 を参照してください。

ステップ 8 [Add Identity Certificate] ダイアログボックスで、[Add Certificate] をクリックします。

[Identity Certificate Request] ダイアログボックスが表示されます。

ステップ 9 テキスト タイプの CSR ファイル名（c:\verisign-csr.txt など）を入力し、[OK] をクリックします。

ステップ 10 CSR テキスト ファイルを CA に送信します。送信する代わりに、CA の Web サイトにある CSR 登録ページにテキスト ファイルを貼り付けることもできます。

ステップ 11 CA から ID 証明書が返されたら、[Identity Certificates] ペインに移動し、保留中の証明書エントリを選択して、[Install] をクリックします。

[Install Identity Certificate] ダイアログボックスが表示されます。

ステップ 12 該当するオプション ボタンをクリックして、次のいずれかのオプションを選択します。

- Install from a file

  または、[Browse] をクリックし、ファイルを検索します。

- Paste the certificate data in base-64 format

  コピーした証明書データを指定された領域に貼り付けます。

ステップ 13 [Install Certificate] をクリックします。

ステップ 14 [Apply] をクリックし、新しくインストールした証明書とその ASA コンフィギュレーションを保存します。

ステップ 15 選択した ID 証明書に関する詳細情報を表示するには、[Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

[General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。

[Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。

[Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

ステップ 16 コード署名者証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Import] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

CA 証明書

このページで、CA 証明書を管理します。次のトピックでは、実行できることについて説明します。

CA 証明書の追加またはインストール

CA 証明書を追加またはインストールするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Remote Access VPN]** > **[Certificate Management]** > **[CA Certificates]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Install Certificate] ダイアログボックスが表示されます。

ステップ 3 [Install from a file] オプション ボタンをクリックして、既存のファイルから証明書設定を追加します（これがデフォルト設定です）。

ステップ 4 パスおよびファイル名を入力するか、または [Browse] をクリックしてファイルを検索します。次に、[Install Certificate] をクリックします。

ステップ 5 [Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 6 [Paste certificate in PEM format] オプション ボタンをクリックして、手動で登録します。

ステップ 7 PEM 形式（base64 または 16 進数）の証明書をコピーして、指定の領域に貼り付け、[Install Certificate] をクリックします。

ステップ 8 [Certificate Installation] ダイアログボックスが表示され、証明書が正常にインストールされたことを示す確認メッセージが示されます。[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 9 [Use SCEP] オプション ボタンをクリックして、自動で登録します。ASA が、SCEP を使用して CA に接続し、証明書を取得して、証明書をデバイスにインストールします。SCEP を使用するには、インターネットを介して、SCEP をサポートする CA に登録する必要があります。SCEP を使用した自動登録では、ユーザーは次の情報を入力する必要があります。

- 自動インストールする証明書のパスとファイル名。
- 証明書のインストールの最大再試行分数。デフォルトは 1 分です。
- 証明書のインストールの再試行回数。デフォルトは 0 です。この場合は、再試行時間内であれば何度でも再試行できます。

ステップ 10 新規および既存の証明書のその他のコンフィギュレーション オプションを表示するには、[More Options] をクリックします。

[Configuration Options for CA Certificates] ペインが表示されます。

ステップ 11 既存の CA 証明書コンフィギュレーションを変更するには、コンフィギュレーションを選択し、[Edit] をクリックします。

ステップ 12 CA 証明書コンフィギュレーションを削除するには、コンフィギュレーションを選択し、[Delete] をクリックします。

（注） 証明書コンフィギュレーションを削除すると、復元できなくなります。削除した証明書を再作成するには、[Add] をクリックして、証明書コンフィギュレーションの情報をすべて再入力します。

ステップ 13 [Show Details] をクリックして、次の 3 つの表示専用タブが含まれる [Certificate Details] ダイアログボックスを表示します。

- [General] タブには、タイプ、シリアル番号、ステータス、用途、公開キー タイプ、CRL 分散ポイント、証明書の有効期間、および関連付けられているトラストポイントの値が表示されます。これらの値は、[Available] と [Pending] の両方のステータスに適用されます。
- [Issued to] タブには、サブジェクト DN または証明書所有者の X.500 フィールドとその値が表示されます。これらの値は、[Available] ステータスのみに適用されます。
- [Issued by] タブには、証明書を付与したエンティティの X.500 フィールドが表示されます。これらの値は、[Available] ステータスのみに適用されます。

失効に関する CA 証明書の設定

失効に関して CA 証明書を設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Revocation Check] タブをクリックします。

ステップ 3 証明書の失効チェックをディセーブルにするには、[Do not check certificates for revocation] オプション ボタンをクリックします。

ステップ 4 1 つ以上の失効チェック方式（CRL または OCSP）を選択するには、[Check certificates for revocation] オプション ボタンをクリックします。

ステップ 5 [Add] をクリックして失効方式を右側に移動すると、その方式が使用可能になります。[Move Up] または [Move Down] をクリックして、方式の順序を変更します。

選択した方式は、追加した順序で実装されます。方式からエラーが返された場合は、その次の失効チェック方式がアクティブになります。

ステップ 6 証明書の検証中に失効チェックのエラーを無視するには、[**Consider certificate valid if revocation checking returns errors**] チェックボックスをオンにします。

ステップ 7 [OK] をクリックして、[Revocation Check] タブを閉じます。

CRL 取得ポリシーの設定

CRL 取得ポリシーを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Use CRL Distribution Point from the certificate] チェックボックスをオンにして、チェック対象の証明書から CRL 分散ポイントに失効チェックを転送します。

ステップ 3 [Use Static URLs configured below] チェックボックスをオンにして、CRL の取得に使用する特定の URL を一覧表示します。選択した URL は、追加した順序で実装されます。指定した URL でエラーが発生した場合は、その次の URL が使用されます。

ステップ 4 [Static Configuration] 領域の [Add] をクリックします。

[Add Static URL] ダイアログボックスが表示されます。

ステップ 5 CRL の分散に使用するスタティック URL を入力して、[OK] をクリックします。

入力した URL が [Static URLs] リストに表示されます。

ステップ 6 [OK] をクリックして、このダイアログボックスを閉じます。

CRL 取得方式の設定

CRL 取得方式を設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [CRL Retrieval Methods] タブをクリックします。

ステップ 3 次の 3 つの取得方式のいずれかを選択します。

- CRL の取得で LDAP をイネーブルにするには、[Enable Lightweight Directory Access Protocol (LDAP)] チェックボックスをオンにします。LDAP を使用して CRL を取得する場合は、指定した LDAP サーバーにパスワードを使用して接続することで、LDAP セッションが開始されます。デフォルトの場合、この接続には TCP ポート 389 を使用されます。次の必須パラメータを入力します。
  - **Name**

- **Password**
- **Confirm Password**
- **デフォルト サーバー**（サーバー名）
- **デフォルト ポート**（389）

- CRL の取得で HTTP をイネーブルにするには、[Enable HTTP] チェックボックスをオンにします。

ステップ 4 [OK] をクリックして、このタブを閉じます。

OCSP ルールの設定

X.509 デジタル証明書の失効ステータスを取得するための OCSP ルールを設定するには、次の手順を実行します。

始める前に

OCSP ルールを追加する前に、必ず証明書マップを設定しておいてください。証明書マップが設定されていない場合、エラー メッセージが表示されます。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [OCSP Rules] タブをクリックします。

ステップ 3 この OCSP ルールと一致する証明書マップを選択します。証明書マップにより、ユーザー権限と、証明書の特定のフィールドとの照合が行われます。[Certificate] フィールドに、ASA において応答側の証明書の検証に使用される CA の名前が表示されます。[Index] フィールドに、ルールのプライオリティ番号が表示されます。[URL] フィールドに、この証明書の OCSP サーバーの URL が表示されます。

ステップ 4 [Add] をクリックします。

[Add OCSP Rule] ダイアログボックスが表示されます。

ステップ 5 使用する証明書マップをドロップダウン リストから選択します。

ステップ 6 使用する証明書をドロップダウン リストから選択します。

ステップ 7 ルールのプライオリティ番号を入力します。

ステップ 8 この証明書の OCSP サーバーの URL を入力します。

ステップ 9 完了したら、[OK] をクリックして、このダイアログボックスを閉じます。

新しく追加された OCSP ルールがリストに表示されます。

ステップ 10 [OK] をクリックして、このタブを閉じます。

高度な CRL および OCSP の設定

CRL および OCSP の追加設定を行うには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Site-to-Site VPN]** > **[Certificate Management]** > **[CA Certificates]** > **[Add]** の順に選択して、[Install Certificates] ダイアログボックスを表示します。次に、[More Options] をクリックします。

ステップ 2 [Configuration Options for CA Certificates] ペインで [Advanced] タブをクリックします。

ステップ 3 [CRL Options] 領域にキャッシュの更新間隔を分数で入力します。デフォルトは 60 分です。範囲は 1 ～ 1440 分です。CA から同じ CRL を何度も受け取る必要のないように、ASA では、取得した CRL をローカルで保存できます。これを CRL キャッシングと呼びます。CRL キャッシュの容量はプラットフォームによって異なり、すべてのコンテキストについて累積されます。新たに取得した CRL をキャッシュすることで、保存制限を超える可能性がある場合は、ASA により使用頻度が最も低い CRL が削除され、使用可能な空き容量が確保されます。

ステップ 4 [Enforce next CRL update] チェックボックスをオンにして、Next Update 値の有効期限が切れていない CRL に限り、有効な CRL として使用できるようにします。[Enforce next CRL update] チェックボックスをオフにすると、Next Update 値がない場合や、Next Update 値の有効期限が切れている場合でも有効な CRL として使用できます。

ステップ 5 [OCSP Options] 領域に OCSP サーバーの URL を入力します。ASA で使用される OCSP サーバーは、次の順で選択されます。

a) 一致証明書上書きルールの OCSP URL に対応するサーバー
b) 選択された [OCSP Options] 属性に設定した OCSP URL に対応するサーバー
c) ユーザー証明書の AIA フィールド

ステップ 6 デフォルトでは、[Disable nonce extension] チェックボックスがオンになっています。この設定では、暗号化によって要求を応答にバインドし、リプレイアタックを回避します。このプロセスでは、要求と応答との間でそれぞれのナンス拡張を照合し、両者が同一であることを確認することで、リプレイアタックを防ぐことができます。ただし、事前に生成した応答には、各要求と一致するナンス拡張は含まれていません。そのため、使用している OCSP サーバーから、事前に生成した応答を送信する場合は、[Disable nonce extension] チェックボックスをオフにしてください。

ステップ 7 [Other Options] 領域で、次のいずれかのオプションを選択します。

- 指定した CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by this CA] チェックボックスをオンにします。
- 下位 CA の証明書を ASA で受け入れるようにするには、[Accept certificates issued by the subordinate CAs of this CA] チェックボックスをオンにします。

ステップ 8 [OK] をクリックしてこのタブを閉じ、[Apply] をクリックしてコンフィギュレーションの変更を保存します。

CA サーバー管理

コード署名者証明書

コード署名者証明書のインポート

コード署名者証明書をインポートするには、次の手順を実行します。

手順

ステップ 1 [Code Signer] ペインで、[Import] をクリックし、[Import Certificate] ダイアログボックスを表示します。

ステップ 2 PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 3 インポートするファイルの名前を入力するか、[Browse] をクリックして [Import ID Certificate File] ダイアログボックスを表示し、ファイルを検索します。

ステップ 4 インポートするファイルを選択し、[Import ID Certificate File] をクリックします。

[Import Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 5 [Import Certificate] をクリックします。

[Code Signer] ペインにインポートされた証明書が表示されます。

ステップ 6 [Apply] をクリックし、新しくインポートしたコード署名者証明書コンフィギュレーションを保存します。

コード署名者証明書のエクスポート

コード署名者証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 [Code Signer] ペインで、[Export] をクリックし、[Export Certificate] ダイアログボックスを表示します。

ステップ 2 証明書コンフィギュレーションをエクスポートするときに使用する PKCS12 形式ファイルの名前を入力します。

ステップ 3 公開キー暗号化標準（base64 エンコードまたは 16 進数形式を使用できます）を使用するには、[Certificate Format] 領域で [PKCS12 format] オプション ボタンをクリックします。使用しない場合は、[PEM format] オプション ボタンをクリックします。

ステップ 4 [Browse] をクリックして [Export ID Certificate File] ダイアログボックスを表示し、証明書コンフィギュレーションをエクスポートするファイルを探します。

ステップ 5 ファイルを選択し、[Export ID Certificate File] をクリックします。

[Export Certificate] ダイアログボックスに、選択した証明書ファイルが表示されます。

ステップ 6 エクスポート用の PKCS12 形式ファイルの復号化に使用するパスフレーズを入力します。

ステップ 7 復号化パスフレーズを確認のために再入力します。

ステップ 8 [Export Certificate] をクリックして、証明書コンフィギュレーションをエクスポートします。

証明書の有効期限アラートの設定（ID 証明書または CA 証明書用）

ASA は、トラストポイントの CA 証明書および ID 証明書について有効期限を24時間ごとに 1 回チェックします。証明書の有効期限がまもなく終了する場合、syslog がアラートとして発行されます。

更新リマインダに加え、コンフィギュレーションに期限が切れた証明書が見つかった場合、その証明書を更新するか、または削除することで、コンフィギュレーションを修正するために syslog が毎日 1 回生成されます。

たとえば、有効期限アラートが 60 日に開始され、その後 6 日ごとに繰り返すように設定されているとします。ASAが 40 日に再起動されると、アラートはその日に送信され、次のアラートは 36 日目に送信されます。

（注） 有効期限チェックは、トラストプールの証明書では実行されません。ローカルCA トラストポイントは、有効期限チェックの通常のトラストポイントとしても扱われます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificate/CA Certificate]** を参照します。

ステップ 2 [Enable Certificate Expiration Alert] チェックボックスをオンにします。

ステップ 3 目的の日数を入力します。

- [Repeat the alert for]：最初のアラートが発行される有効期限までの日数（1 ～ 90）を設定します。

- [Repeat the alert for]：証明書が更新されない場合のアラート頻度（1 ～ 14 日）を設定します。デフォルトでは、最初のアラートは有効期限の 60 日前に送信され、その後は証明書が更新または削除されるまで毎週 1 回送信されます。また、アラートは有効期限日に送信され、その後は毎日 1 回送信され、アラートの設定に関係なく、有効期限の直前の週はアラートが毎日送信されます。

デジタル証明書のモニターリング

デジタル証明書ステータスのモニターリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [CRL]**

  このペインには、CRL の詳細が表示されます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

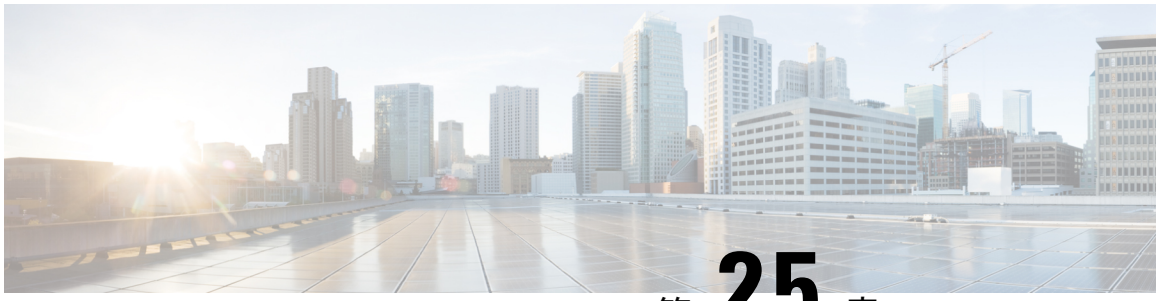
証明書管理の履歴

表 *32 :* 証明書管理の履歴

機能名	プラットフォームリリース	説明
証明書管理	7.0(1)	デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、またはIPアドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。 次の画面が導入されました。 [Configuration] > [Remote Access VPN] > [Certificate Management Configuration] > [Site-to-Site VPN] > [Certificate Management]。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [CA Certificates Configuration] > [Device Management] > [Certificate Management] > [CA Certificates]。
証明書管理	7.2(1)	
証明書管理	8.0(2)	
SCEP プロキシ	8.4(1)	サードパーティ CA からのデバイス証明書を安全に構成できる機能を導入しました。

機能名	プラットフォームリリース	説明
参照 ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 確認は syslog サーバーとスマートライセンスサーバーへの TLS 接続の PKI 確認中に行われます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次の画面を変更しました。[Configuration] > [Remote Access VPN] > [Advanced Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add/Edit Configuration] > [Device Management] > [Smart Call Home]。
ローカル CA サーバー	9.12(1)	ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、crypto ca server の smpt モードに追加されます。 We deprecated Local CA Server and will be removing in a later release—When ASA is configured as local CA server, it is enabled to issue digital certificates, publish Certificate Revocation Lists（CRLs), and securely revoke issued certificates. この機能は古くなったため、crypto ca server コマンドは廃止されています。
ローカル CA サーバー	9.13(1)	ローカル CA サーバーのサポートが削除されました。したがって、**crypto ca server** コマンドとそのサブコマンドは削除されています。 **crypto ca server** コマンドとそのすべてのサブコマンドが削除されました。

機能名	プラットフォームリリース	説明
CRL 分散ポイント コマンドの変更	9.13(1)	スタティック CDP URL コンフィギュレーション コマンドが削除され、match certificate コマンドに移行しました。 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[CA Certificates]**
CRL キャッシュサイズの拡張	9.13(1)	大規模な CRL ダウンロードの失敗を防ぐため、キャッシュサイズを拡張し、また、個別の CRL 内のエントリ数の制限を取り除きました。 • マルチ コンテキスト モードの場合、コンテキストごとの合計CRL キャッシュサイズが 16 MB に増加しました。 • シングル コンテキスト モードの場合、合計 CRL キャッシュサイズが 128 MB に増加しました。



第 25 章

ARP インスペクションおよび MAC アドレス テーブル

この章では、MACアドレステーブルのカスタマイズ方法、およびブリッジグループのARPインスペクションの設定方法について説明します。

ARP インスペクションと MAC アドレス テーブルについて

ブリッジ グループのインターフェイスでは、ARP インスペクションは「中間者」攻撃を防止します。他の ARP の設定をカスタマイズすることも可能です。ブリッジ グループの MAC アドレス テーブルのカスタマイズができます。これには、MAC スプーフィングに対する防御としてのスタティック ARP エントリの追加が含まれます。

ブリッジグループ トラフィックの ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションを有効にします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイルータはゲートウェイルータのMACアドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答

をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、Secure Firewall ASAは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Secure Firewall ASAはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにSecure Firewall ASAを設定できます。

注 専用の Management インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジ グループを使用する場合、ASA は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、ASA が MAC アドレスをアドレス テーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、ASAは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには ASA セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに元のパケットを ASA がフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモートデバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：ASA は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモート デバイスへのパケット：ASA は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

ルーテッドモードでは、すべてのインターフェイスで非 IP パケットのフラッディングをオプションで有効にできます。

デフォルト設定

- ARP インスペクションを有効にした場合、デフォルト設定では、一致しないパケットはフラッディングします。
- ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、Secure Firewall ASAは対応するエントリを MAC アドレス テーブルに追加します。

注 Secure Firewall ASA はリセットパケットを生成し、ステートフル検査エンジンによって拒否された接続をリセットします。リセットパケットでは、パケットの宛先 MAC アドレスが ARP テーブルのルックアップに基づいて決定されるのではなく、拒否されるパケット（接続）から直接取得されます。

ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジ グループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジ グループでのみサポートされます。

ARP インスペクションとその他の ARP パラメータの設定

ブリッジ グループでは、ARP インスペクションをイネーブルにすることができます。その他の ARP パラメータは、ブリッジ グループとルーテッド モードのインターフェイスの両方で設定できます。

手順

ステップ 1 スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ（828 ページ）に従って、スタティック ARP エントリを追加します。ARP インスペクションは ARP パケットを

ARP テーブルのスタティック ARP エントリと比較するので、この機能にはスタティック ARP エントリが必要です。その他の ARP パラメータも設定できます。

ステップ 2 ARP インスペクションの有効化 （829 ページ）に従って ARP インスペクションを有効にします。

スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ

ブリッジグループのデフォルトでは、ブリッジ グループ メンバー インターフェイス間の ARP パケットはすべて許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの ASA との間のトラフィックに、ASA は ARP テーブルのダイナミック ARP エントリのみを使用します。

ARP タイムアウトなどの ARP 動作を設定することもできます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Advanced]** > **[ARP]** > **[ARP Static Table]** の順に選択します。

ステップ 2 [Add] をクリックして、スタティック ARP エントリを追加します。

[Add ARP Static Configuration] ダイアログボックスが表示されます。

a) [Interface] ドロップダウンリストから、ホスト ネットワークに接続されているインターフェイスを選択します。
b) [IP Address] フィールドにホストの IP アドレスを入力します。
c) [MAC Address] フィールドにホストの MAC アドレスを入力します（00e0.1e4e.3d8b など）。

d) このアドレスでプロキシ ARP を実行するには、[Proxy ARP] チェック ボックスをオンにします。

ASA は、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

e) [OK] をクリックします。

ステップ 3 ダイナミック ARP エントリの ARP タイムアウトを設定するには、[ARP Timeout] フィールドに値を入力します。

このフィールドでは、ASA が ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは14400秒です。ARPテーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

ステップ 4 非接続サブネットを使用するには、[Allow non-connected subnets] チェックボックスをオンにします。ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。ARPキャッシュをイネーブルにして、間接接続されたサブネットを含めることもできます。セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASAに対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンデリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

ステップ 5 すべてのインターフェイスの 1 秒あたりの ARP パケット数を制御するには、[ARP Rate-Limit] フィールドに値を入力します。

10 ～ 32768 の範囲で値を入力します。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。

ステップ 6 [Apply] をクリックします。

ARP インスペクションの有効化

この項では、ブリッジ グループ用に ARP インスペクションをイネーブルにする方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Advanced]** > **[ARP]** > **[ARP Inspection]** ペインの順に選択します。

ステップ 2 ARP インスペクションをイネーブルにするインターフェイス行を選択し、[Edit] をクリックします。

[Edit ARP Inspection] ダイアログボックスが表示されます。

ステップ 3 ARPインスペクションをイネーブルにするには、[Enable ARP Inspection] チェック ボックスをオンにします。

ステップ 4 （任意）一致しない ARP パケットをフラッディングするには、[Flood ARP Packets] チェックボックスをオンにします。

デフォルトでは、スタティック ARP エントリのどの要素にも一致しないパケットが、送信元のインターフェイスを除くすべてのインターフェイスからフラッドされます。MACアドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。

このチェックボックスをオフにすると、一致しないパケットはすべてドロップされます。これにより、スタティック エントリにある ARP だけが ASA を通過するように制限されます。

（注） Management 0/0 または 0/1 インターフェイスあるいはサブインターフェイスがある場合、これらのインターフェイスは、このパラメータがフラッドに設定されていてもパケットをフラッドしません。

ステップ 5 [OK]、続いて [Apply] をクリックします。

トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルの

ここでは、ブリッジグループの MAC アドレス テーブルをカスタマイズする方法について説明します。

ブリッジ グループのスタティック MAC アドレスの追加

通常、MACアドレスは、特定のMACアドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティックエントリに一致しないインターフェイスにトラフィックを送信しようとした場合、ASA はトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ （828 ページ）を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

MAC アドレス テーブルにスタティック MAC アドレスを追加するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Bridging]** > **[MAC Address Table]** ペインを選択します。

ステップ 2 （オプション）MAC アドレス エントリがタイムアウトするまで MAC アドレス テーブル内に留まる時間を設定するには、[Dynamic Entry Timeout] フィールドに値を入力します。

この値は、5 ～ 720 分（12 時間）の範囲で指定します。5 分がデフォルトです。

ステップ 3 [Add] をクリックします。

[Add MAC Address Entry] ダイアログボックスが表示されます。

ステップ 4 [Interface Name] ドロップダウンリストから、MAC アドレスに関連付けられている送信元インターフェイスを選択します。

ステップ 5 [MAC Address] フィールドに MAC アドレスを入力します。

ステップ 6 [OK]、続いて [Apply] をクリックします。

MAC アドレスラーニングの設定

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MACアドレスをテーブルにスタティックに追加しないと、トラフィックが ASA を通過できなくなります。ルーテッドモードでは、すべてのインターフェイスで非 IP パケットのフラッディングを有効にできます。

MAC アドレスラーニングを設定にするには、次の手順を実行します。

手順

ステップ 1 **[構成（Configuration）]** > **[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ブリッジング（Bridging）]** > **[MACラーニング（MAC Learning）]**の順に選択します。

ステップ 2 MAC ラーニングをディセーブルにするには、インターフェイス行を選択して、[Disable] をクリックします。

ステップ 3 MAC ラーニングを再度イネーブルにするには、[Enable] をクリックします。

ステップ 4 非IPパケットのフラッディングを有効にするには、[非IPv4-IPv6パケットの不明なMACアドレスのフラッディングを有効にする（Enable flooding for unknown MAC address for non IPv4-IPv6 packets）] をオンにします。

ステップ 5 [Apply] をクリックします。

ARP インスペクションと MAC アドレス テーブルの履歴

機能名	プラットフォームリリース	機能情報
ARP インスペクション	7.0(1)	ARP インスペクションは、すべての ARP パケットの MAC アドレス、IP アドレス、および送信元インターフェイスを、ARP テーブルのスタティック エントリと比較します。この機能は、トランスペアレント ファイアウォール モード、および 9.7(1) で始まるトランスペアレントモードとルーテッドモードのブリッジグループのインターフェイスで利用できます。 **arp**、**arp-inspection**、および **show arp-inspection** コマンドが導入されました。
MAC アドレス テーブル	7.0(1)	トランスペアレント モード、および 9.7(1) で始まるトランスペアレントモードとルーテッドモードのブリッジグループのインターフェイスの MAC アドレステーブルをカスタマイズすることもできます。 **mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable**、および **show mac-address-table** コマンドが導入されました。

機能名	プラットフォームリリース	機能情報
間接接続されたサブネットの ARP キャッシュの追加	8.4(5)/9.1(2)	ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。また、ARP キャッシュに間接接続されたサブネットを含めることができるようになりました。セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。 次の機能を使用する場合は、この機能を使用する必要がある可能性があります。 • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced]> [ARP] > [ARP Static Table]。
カスタマイズ可能な ARP レート制限	9.6(2)	1 秒あたり許可される ARP パケットの最大数を設定できます。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。 次の画面が変更されました。**[Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table]**

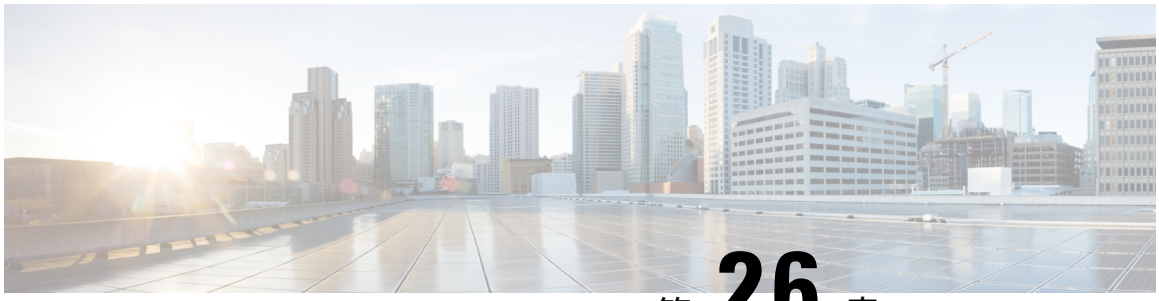
機能名	プラットフォームリリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	

機能名	プラットフォームリリース	機能情報
		Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジグループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定するASA上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVIは名前付きインターフェイスとなり、アクセスルールやDHCPサーバーなどの一部の機能に、メンバーインターフェイスとは個別に参加できます。 トランスペアレントモードでサポートされるマルチ コンテキスト モードやASAクラスタリングの各機能は、ルーテッド モードではサポートされません。マルチキャストルーティングとダイナミック ルーティングの機能も、

機能名	プラットフォームリリース	機能情報
		BVI ではサポートされません。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** **[Configuration]** > **[Device Management]** > **[DHCP]** > **[DHCP Server]** **[Configuration]** > **[Firewall]** > **[Access Rules]** **[Configuration]** > **[Firewall]** > **[EtherType Rules]**

第 V 部

IP ルーティング



第 26 章

ルーティングの概要

この章では、ASA 内でのルーティングの動作について説明します。

パスの決定

ルーティング プロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティング アルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティング アルゴリズムは、ルート情報が格納されるルーティング テーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデート

を他のすべてのルータから分析することで、ルータはネットワークトポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワークトポロジの全体像の構築に使用できます。

（注） 非対称ルーティングがサポートされるのは、マルチ コンテキスト モードでのアクティブ/アクティブ フェールオーバーに対してのみです。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。Secure Firewall ASA では、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは、実はネットワーク管理者が確立したテーブル マップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパス アルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティング アルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティング システムでは、一部のルータが実質的なルーティング バックボーンを形成します。バックボーン以外のルータからのパケットはバックボーン ルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーン ルータから、1 つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織を模倣しているため、そのトラフィック パターンを適切にサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティング アルゴリズムを簡素化できます。また、使用しているルーティング アルゴリズムに応じて、ルーティング アップデート トラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステート アルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステート アルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティング テーブル全体または一部を送信するように要求されます。つまり、リンクステート アルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ルーティングでサポートされるインターネットプロトコル

Secure Firewall ASA は、ルーティングに対してさまざまなインターネット プロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol（EIGRP）

  EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First（OSPF）

  OSPF は、インターネット プロトコル（IP）ネットワーク向けに、インターネット技術特別調査委員会（IETF）の Interior Gateway Protocol（IGP）作業部会によって開発されたルーティング プロトコルです。OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- Routing Information Protocol（RIP）

  RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol（IGP）です。つまり、1 つの自律システム内部でルーティングを実行します。

- ボーダー ゲートウェイ プロトコル（BGP）

  BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。顧客は ISP に接続し、ISP は BGP を使用して顧客のルートと ISP のルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

- Intermediate System to Intermediate System（IS-IS）

  IS-IS はリンクステート内部ゲートウェイ プロトコル（IGP）です。リンクステート プロトコルは、各参加ルータで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。

Routing Table

ASA はデータ トラフィック（デバイスを介して）および管理トラフィック（デバイスから）に別々のルーティング テーブルを使用します。ここでは、ルーティング テーブルの仕組みについて説明します。管理ルーティング テーブルの詳細については、管理トラフィック用ルーティングテーブル （850 ページ）も参照してください。

ルーティング テーブルへの入力方法

ASA のルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。ASA は、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティング プロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への 2 つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2 つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティング テーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネット マスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- ASA が、1 つのルーティング プロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティング プロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティング プロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティング テーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- ASA が、ある宛先へのルーティング プロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2 つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブ ディスタンスが小さい方のルートがルーティング テーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、Secure Firewall ASAが最適なパスの選択に使用するルート パラメータです。ルーティング プロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への 2 つのルートについて常にベスト パスを判定できるわけではありません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、Secure Firewall ASAでサポートされているルーティングプロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 *33*：サポートされるルーティング プロトコルのデフォルト アドミニストレーティブ ディスタンス

ルートの送信元	デフォルト アドミニストレーティブ ディスタンス
接続されているインターフェイス	[0]
スタティック ルート	1
EIGRP 集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、Secure Firewall ASAが OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、

OSPF ルーティング プロセスの方が優先度が高いため、Secure Firewall ASAは OSPF ルートを選択します。この場合、ルータはOSPFバージョンのルートをルーティングテーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、Secure Firewall ASA は、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された Secure Firewall ASA のルーティング テーブルにだけ影響します。アドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIPルーティングプロセスは、のルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルートとフローティング スタティック ルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされているためにインストールできなかった場合、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先ルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティング スタティック ルートとは、単に、Secure Firewall ASA で動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブ ディスタンスが設定されているスタティック ルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。

- 宛先が、ルーティング テーブル内の複数のエントリと一致し、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

（注） ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

ダイナミック ルーティングおよび フェールオーバー

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 フェールオーバー ペアでアクティブになると、ルートはフェールオーバー バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

ダイナミック ルーティングおよびクラスタリング

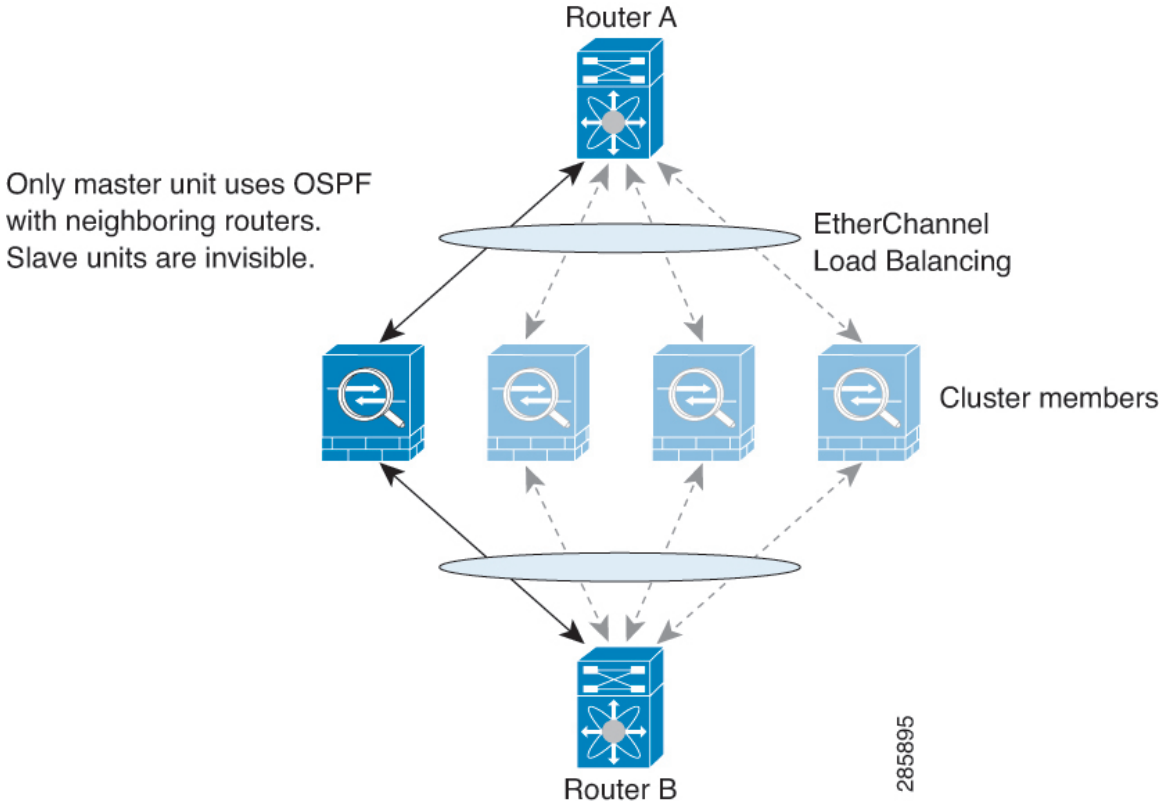
ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

（注） IS-IS は、スパンド EtherChannel モードではサポートされていません。

スパンド EtherChannel モード：ルーティング プロセスは制御ノードでのみ実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティング パケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *63* : スパンド *EtherChannel* モードでのダイナミック ルーティング



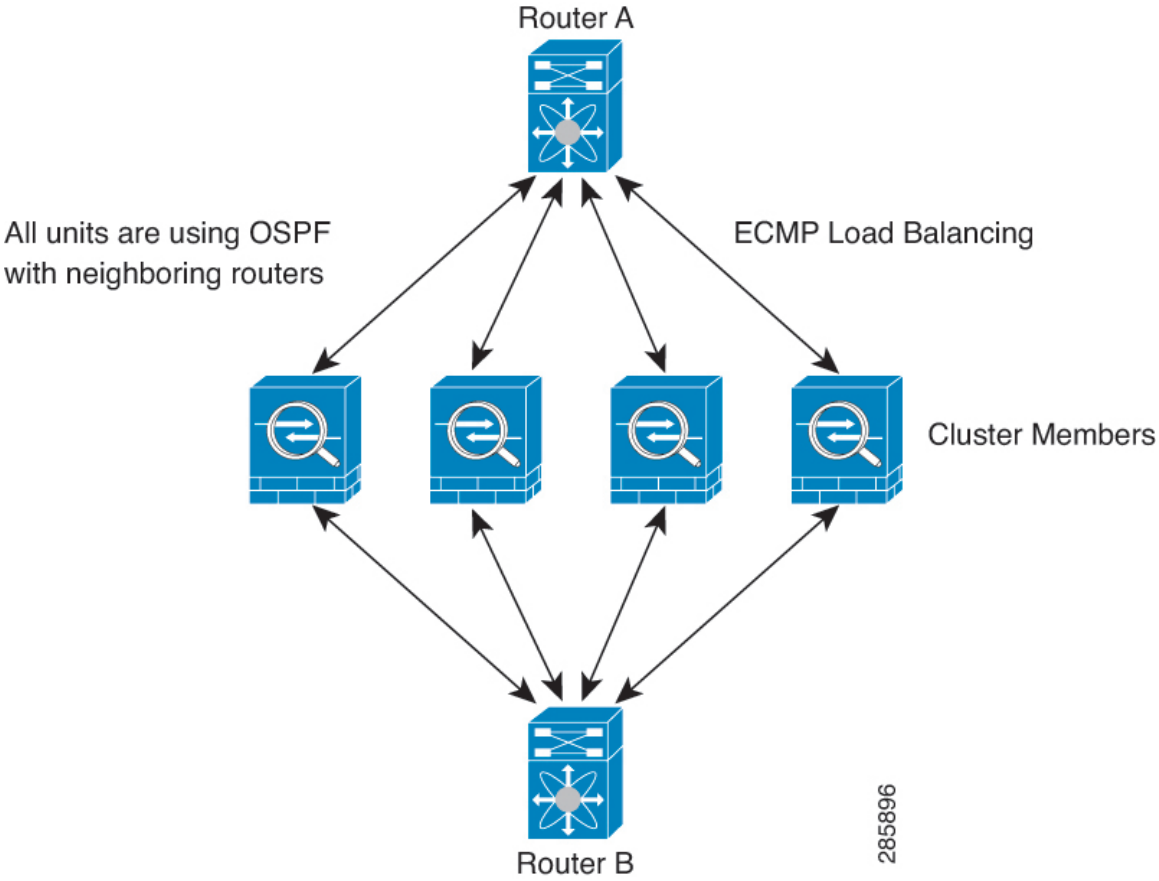
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *64 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コスト パスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタプールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性確保のためにクラスタが同一ルータに対して複数の隣接関係を持つ場合、非対称ルーティングが原因で許容できないトラフィック損失が発生する場合があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべての ASA インターフェイスをまとめます。トラフィック ゾーンの設定 （739 ページ）を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 およびEIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキスト モードでは、ルーテッド モードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティング アップデートをフィルタリングするためにOSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルートマップ とプレフィックスのリスト
コンテキストごとに 1 つのインスタンスがサポートされます。	コンテキストごとに 2 つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし
2つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングルモードで使用可能なすべてのCLI はマルチコンテキストモードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える1つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルトクラスは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル（接続、スタティック、OSPF、EIGRP、および RIP）のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ対策として、多くの場合、（デバイスからの）管理トラフィックをデータトラフィックから分離する必要があります。この分離を実現するために、ASA は管理専用トラフィックとデータ トラフィックに個別のルーティング テーブルを使用します。個別のルーティングテーブルを使用することで、データと管理用に別のデフォルトルートを作成できます。

各ルーティングテーブルのトラフィックのタイプ

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス発信トラフィックでは、タイプに応じて、デフォルトで管理専用ルーティングテーブルまたはデータルーティングテーブルが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

- 管理専用テーブルのデバイス発信トラフィックには、HTTP、SCP、TFTP、**copy** コマンド、スマートライセンス、Smart Call Home、**trustpoint**、**trustpool** などを使用してリモートファイルを開く機能が含まれています。
- データテーブルのデバイス発信トラフィックには、ping、DNS、DHCP などの他のすべての機能が含まれます。

管理専用ルーティングテーブルに含まれるインターフェイス

管理専用インターフェイスには、すべてのManagement x/x インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。

他のルーティングテーブルへのフォールバック

デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デフォルト以外のルーティングテーブルの使用

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。ASA は、指定されたインターフェイスのルートのみをチェックします。たとえば、管理専用インターフェイスから ping を送信する必要がある場合は、ping 機能でインターフェイスを指定します。他方、データルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、管理ルーティングテーブルにフォールバックすることは決してありません。

ダイナミック ルーティング

管理専用ルーティングテーブルは、データ インターフェイス ルーティング テーブルから分離したダイナミックルーティングをサポートします。ダイナミック ルーティング プロセスは管理専用インターフェイスまたはデータ インターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。分離した管理ルーティングテーブルが含まれていない以前のリリースからアップグレードする際、データインターフェイスと管理インターフェイスが混在し、同じダイナミック ルーティング プロセスを使用している場合、管理インターフェイスは破棄されます。

VPN 要件の管理アクセス機能

VPN を使用している際に ASA で参加したインターフェイス以外のインターフェイスに管理アクセスを許可する管理アクセス機能を設定した場合、分離した管理およびデータ ルーティング テーブルに関するルーティングの配慮のために、VPN 終端インターフェイスと管理アクセスインターフェイスは同じタイプである必要があります。両方とも管理専用インターフェイスまたは通常のデータ インターフェイスである必要があります。

管理インターフェイスの識別

management-only で設定されたインターフェイスは、管理インターフェイスと見なされます。

次の設定では、GigabitEthernet0/0 と Management0/0 の両インターフェイスは、管理インターフェイスと見なされます。

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

等コスト マルチパス（ECMP）ルーティング

Secure Firewall ASA は、等コスト マルチパス（ECMP）ルーティングをサポートしています。

インターフェイスごとに最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
```

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

トラフィックゾーンを使用した複数のインターフェイス間の ECMP

インターフェイスのグループを含むようにトラフィックゾーンを設定する場合、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、自動的に等コスト ルートを設定できます。Secure Firewall ASAでは、より堅牢なロードバランシング メカニズムを使用してインターフェイス間でトラフィックをロード バランスします。

ルートが紛失した場合、デバイスはフローをシームレスに別のルートに移動させます。

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分の MAC アドレスで応答するときに使用されます。NAT を設定し、ASA インターフェイスと同じネットワーク上のマッピング アドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できる唯一の方法は、ASA でプロキシ ARP が使用されている場合、MAC アドレスが宛先マッピング アドレスに割り当てられていると主張することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、ASA はデフォルトで、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Proxy ARP/Neighbor Discovery]** の順に選択します。

[Interface] フィールドにインターフェイス名が一覧表示されます。[Enabled] フィールドには、NAT グローバル アドレスに対してプロキシ ARP/ネイバー探索がイネーブルか（Yes）ディセーブルか（No）が表示されます。

ステップ 2 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をイネーブルにするには、[Enable] をクリックします。デフォルトでは、プロキシ ARP/ネイバー探索はすべてのインターフェイスに対してイネーブルです。

ステップ 3 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をディセーブルにするには、[Disable] をクリックします。

ステップ 4 [Apply] をクリックして設定を実行コンフィギュレーションに保存します。

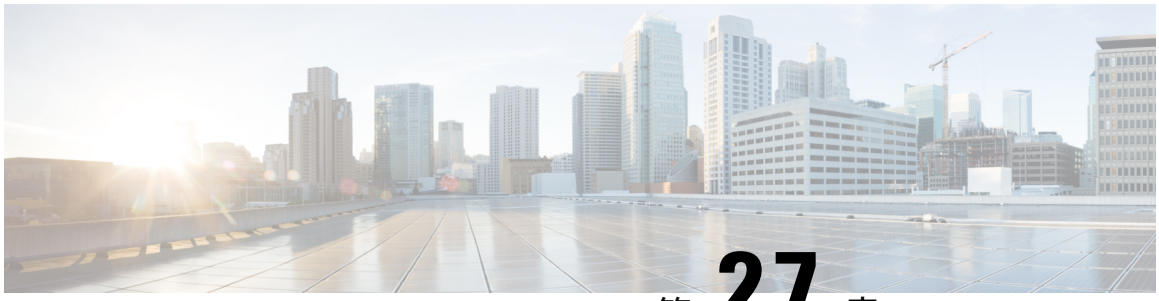
ルーティング テーブルの表示

ルーティング テーブルにある ASDM のすべてのルートを表示するには、**[Monitoring]** > **[Routing]** > **[Routes]** の順に選択します。各行は 1 つのルートを表します。

ルート概要の履歴

表 *34 :* ルート概要の履歴

機能名	プラットフォームリリース	機能情報
管理インターフェイス用のルーティング テーブル	9.5(1)	データ トラフィックから管理トラフィックを区別して分離するため、管理トラフィック専用のルーティング テーブルが追加されました。管理とデータそれぞれの専用ルーティング テーブルは IPv4 と Ipv6 の両方に対して、ASA の各コンテキストごとに作成されます。さらに、ASA の各コンテキストに対して、RIB と FIB の両方に 2 つの予備のルーティング テーブルが追加されます。 次の画面が更新されました。



第 27 章

スタティック ルートとデフォルト ルート

この章では、Cisco ASA でスタティック ルートとデフォルト ルートを設定する方法について説明します。

スタティック ルートとデフォルト ルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。通常は、少なくとも 1 つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクスト ホップ ルータ）を設定する必要があります。

Default Route

最も単純なオプションは、すべてのトラフィックをアップストリームルータに送信するようにデフォルトスタティックルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、ASAが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0（IPv4）または ::/0（IPv6）が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

ASA はデータトラフィックと管理トラフィックに別々のルーティングテーブルを使用するため、必要に応じて、データトラフィック用のデフォルトルートと管理トラフィック用の別のデフォルトルートを設定できます。デバイス間トラフィックでは、タイプに応じてデフォルトで

管理専用またはデータルーティングテーブルが使用されます（管理トラフィック用ルーティングテーブル（850ページ）を参照）。ただし、ルートが見つからない場合は、他のルーティングテーブルにフォールバックします。デフォルトルートは常にトラフィックに一致するため、他のルーティングテーブルへのフォールバックが妨げられます。この場合、インターフェイスがデフォルトのルーティングテーブルになければ、出力トラフィックに使用するインターフェイスを指定する必要があります。

スタティック ルート

次の場合は、スタティック ルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、ASA に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

不要なトラフィックをドロップするための null0 インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセス ルールを補完するソリューションです。null0 ルートを使用して不要なトラフィックや望ましくないトラフィックを転送することで、トラフィックをドロップできます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティング ループを回避することもできます。BGP では、リモート トリガ型ブラック ホール ルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブディスタンスによってプライオリティが決まります。スタティックルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。

- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、等コスト マルチパス（ECMP）ルーティング （851 ページ）を参照してください。
- [トンネル化（Tunneled）] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルト ルートをすべてオーバーライドします。

トランスペアレント ファイアウォール モードおよびブリッジ グループのルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう Secure Firewall ASA で発信されるトラフィックの場合、Secure Firewall ASA がどのブリッジ グループ メンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。Secure Firewall ASA で発信されるトラフィックには、syslog サーバーまたは SNMP サーバーへの通信が含まれることもあります。1つのデフォルト ルートで到達できないサーバーがある場合、スタティック ルートを設定する必要があります。トランスペアレント モードの場合、ゲートウェイ インターフェイスにBVIを指定できません。メンバーインターフェイスのみが使用できます。ルーテッド モードのブリッジ グループの場合、スタティック ルートにBVIを指定する必要があります。メンバー インターフェイスを指定することはできません。詳細については、#unique_1015を参照してください。

スタティック ルート トラッキング

スタティック ルートの問題の1つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、Secure Firewall ASA 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

Secure Firewall ASA では、Secure Firewall ASA が ICMP エコー要求を使用してモニターする宛先ネットワーク上でモニターリング対象スタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象がICMPエコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクストホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- Secure Firewall ASA が通信を行う必要のある対象ネットワーク上のサーバー（syslog サーバーなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけを有効化することができます。

スタティックルートとデフォルトルートのガイドライン

ファイアウォール モードとブリッジ グループ

- トランスペアレント モードでは、スタティック ルートはブリッジ グループ メンバー インターフェイスをゲートウェイとして使用する必要があります。BVI を指定することはできません。
- ルーテッド モードでは、BVI をゲートウェイとして指定する必要があります。メンバー インターフェイスを指定することはできません。
- スタティック ルート トラッキングは、ブリッジ グループ メンバー インターフェイスまたは BVI ではサポートされません。

サポートされるネットワークアドレス

- IPv6 では、スタティック ルート トラッキングはサポートされません。
- ASA はクラスEルーティングをサポートしていません。したがって、クラスEネットワークはスタティックルートとしてルーティングできません。

クラスタリングとマルチコンテキストモード

- クラスタリングでは、スタティック ルート トラッキングはプライマリユニットでのみサポートされます。

- スタティック ルート トラッキングはマルチコンテキストモードではサポートされません。

デフォルト ルートおよびスタティック ルートの設定

少なくとも 1 つのデフォルト ルートを設定する必要があります。また、スタティック ルートの設定が必要になる場合があります。このセクションでは、デフォルト ルートの設定、スタティック ルートの設定、スタティック ルートの追跡を行います。

デフォルト ルートの設定

デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。この手順に従って手動で設定するか、DHCP サーバーや他のルーティング プロトコルから取得するかに関わらず、デフォルト ルートは必ず設定する必要があります。

始める前に

[Tunneled] オプションについては、次のガイドラインを参照してください。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPFを有効にしないでください。この設定を行うと、セッションでエラーが発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- これらのインスペクション エンジンはトンネル ルートを無視するため、トンネル ルートで VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンを使用しないでください。
- tunneled オプションで複数のデフォルト ルートを定義することはできません。
- トンネル トラフィックの ECMP はサポートされません。
- トンネルルートは、通過トラフィックの VPN 終端をサポートしないブリッジグループではサポートされません。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** を選択し、**[Add]** をクリックします。

ステップ 2 [IP Address Type]、[IPv4]、または [IPv6] を選択します。

ステップ 3 特定のトラフィックの送信を行う**インターフェイス**を選択します。

トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。 ブリッジ グループでルーテッド モードを使用する場合は、BVI 名を指定します。

ステップ 4 **ネットワーク**の場合は、そのタイプに応じて **any4** または **any6** を入力します。

ステップ 5 トラフィックを送信する**ゲートウェイ IP** を入力します。

ステップ 6 **メトリック**を設定して、ルートのアドミニストレーティブ ディスタンスを設定します。

デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 7 （オプション） [Options] 領域で、以下を設定します。

- [Tunneled]：VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。tunneled オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。このオプションは、ブリッジグループではサポートされません。
- [Tracked]：（IPv4 のみ）ルートのトラッキングについては、スタティック ルート トラッキングの設定 （861 ページ）を参照してください。

ステップ 8 [OK] をクリックします。

スタティック ルートの設定

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** を選択し、**[Add]** をクリックします。

ステップ 2 [IP Address Type]、[IPv4]、または [IPv6] を選択します。

ステップ 3 特定のトラフィックの送信を行う**インターフェイス**を選択します。

不要なトラフィックをドロップするには、[Null0]インターフェイスを選択します。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。 ブリッジ グループでルーテッド モードを使用する場合は、BVI 名を指定します。

ステップ 4 **ネットワーク**の場合は、トラフィックをルーティングする宛先ネットワークを入力します。

ステップ 5 トラフィックを送信する**ゲートウェイ IP** を入力します。

ステップ 6 **メトリック**を設定して、ルートのアドミニストレーティブ ディスタンスを設定します。

デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

ステップ 7 （オプション） [Options] 領域で、以下を設定します。

- [Tunneled]：VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。tunneled オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。
- [Tracked]：（IPv4 のみ）ルートのトラッキングについては、スタティック ルート トラッキングの設定 （861 ページ）を参照してください。

ステップ 8 [OK] をクリックします。

スタティック ルート トラッキングの設定

スタティック ルート トラッキングを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Static Routes]** の順に選択し、スタティック ルートの設定 （860 ページ）に従ってスタティック ルートを追加または編集します。

ステップ 2 [Options] 領域で [Tracked] オプション ボタンをクリックします。

ステップ 3 [Track ID] フィールドに、ルート トラッキング プロセスの固有識別子を入力します。

ステップ 4 [Track IP Address/DNS Name] フィールドに、追跡対象の IP アドレスまたはホスト名を入力します。これは通常、このルートのネクスト ホップ ゲートウェイの IP アドレスになりますが、そのインターフェイスから利用できる任意のネットワーク オブジェクトとすることもできます。

ステップ 5 [SLA ID] フィールドに、SLA モニターリング プロセスの固有識別子を入力します。

ステップ 6 （任意）[Monitoring Options] をクリックします。

[Route Monitoring Options] ダイアログボックスが表示されます。ここから、次のトラッキング オブジェクトのモニターリング プロパティを変更します。

- [Frequency]：追跡対象の存在を ASA がテストする頻度を秒数で設定します。有効な値の範囲は、1 ～ 604800 秒です。デフォルト値は 60 秒です。
- [Threshold]：しきい値を超えたイベントを示す時間をミリ秒数で設定します。この値に、タイムアウト値より大きい値は指定できません。
- [Timeout]：ルート監視操作が要求パケットからの応答を待つ時間をミリ秒数で設定します。有効な値の範囲は、0 ～ 604800000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
- [Data Size]：エコー要求パケットで使用するデータ ペイロードのサイズを設定します。デフォルト値は 28 です。有効値の範囲は 0 ～ 16384 です。

  （注） この設定では、ペイロードのサイズだけが指定されます。パケット全体のサイズは指定されません。

- [ToS]：エコー要求の IP ヘッダーにあるサービス バイトのタイプの値を設定します。有効な値は、0 ～ 255 です。デフォルト値は 0 です
- [Number of Packets]：各テストに送信されるエコー要求の数を設定します。有効値の範囲は 1 ～ 100 です。デフォルト値は 1 です。

[OK] をクリックします。

ステップ 7 [OK] をクリックしてルートを保存してから、[Apply] をクリックします。

追跡するルートを適用するとすぐに、モニターリング プロセスが開始されます。

ステップ 8 追跡対象外のバックアップ ルートを作成します。

バックアップ ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブ ディスタンス（メトリック）に割り当てる必要があります。

スタティックルートまたはデフォルトルートのモニターリング

- [Monitoring] > [Routing] > [Routes]

[Routes] ペインでは、それぞれの行が 1 つのルートを表しています。IPv4 接続、IPv6 接続、またはその両方でフィルタリングできます。ルーティング情報には、プロトコル、ルートタイプ、宛先IPアドレス、ネットマスクまたはプレフィックスの長さ、ゲートウェイ IP アドレス、ルートに接続するときに経由するインターフェイス、およびアドミニストレーティブ ディスタンスが含まれています。

スタティック ルートまたはデフォルト ルートの例

次の例は、スタティック ルートの作成方法を示します。スタティック ルートは、宛先が 10.1.1.0/24 のトラフィックすべてを内部インターフェイスに接続されているルータ（10.1.2.45）に送信します。また、dmz インターフェイスで 3 つの異なるゲートウェイにトラフィックを誘導する 3 つの等コスト スタティック ルートを定義し、トンネル トラフィックのデフォルト ルートと通常のトラフィックのデフォルト ルートを追加します。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

スタティック ルートおよびデフォルト ルートの履歴

表 *35 :* スタティック ルートおよびデフォルト ルートの機能履歴

機能名	プラットフォームリリース	機能情報
スタティック ルート トラッキング	7.2(1)	スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。 次の画面が導入または変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] [Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] > [Route Monitoring Options]**

機能名	プラットフォームリリース	機能情報
スタティック null0 ルートによるトラフィックのドロップ	9.2(1)	トラフィックを null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route]**

第 28 章

ポリシーベースルーティング

この章では、ポリシーベース ルーティング（PBR）をサポートするように Cisco ASA を設定する方法について説明します。この項では、ポリシーベース ルーティング、PBR のガイドライン PBR の設定について説明します。

ポリシーベース ルーティングについて

従来のルーティングは宛先ベースであり、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティング システムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベース ルーティング（PBR）では、宛先ネットワークではなく条件に基づいてルーティングを定義できます。PBR では、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル、またはこれらの組み合わせに基づいてトラフィックをルーティングできます。

ポリシーベース ルーティング：

- 区別したトラフィックに Quality of Service（QoS）を提供できます。
- 低帯域幅、低コストの永続パスと、高帯域幅、高コストのスイッチドパスに、インタラクティブ トラフィックとバッチ トラフィックを分散できます。
- インターネット サービス プロバイダやその他の組織が、さまざまなユーザー セットから発信されるトラフィックを、適切に定義されたインターネット接続を経由してルーティングできます。

ポリシーベース ルーティングには、ネットワーク エッジでトラフィックを分類およびマークし、ネットワーク全体で PBR を使用してマークしたトラフィックを特定のパスに沿ってルーティングすることで、QoS を実装する機能があります。これにより、宛先が同じ場合でも、異なる送信元から送信されるパケットを別のネットワークにルーティングすることができます。これは、複数のプライベート ネットワークを相互接続する場合に役立ちます。

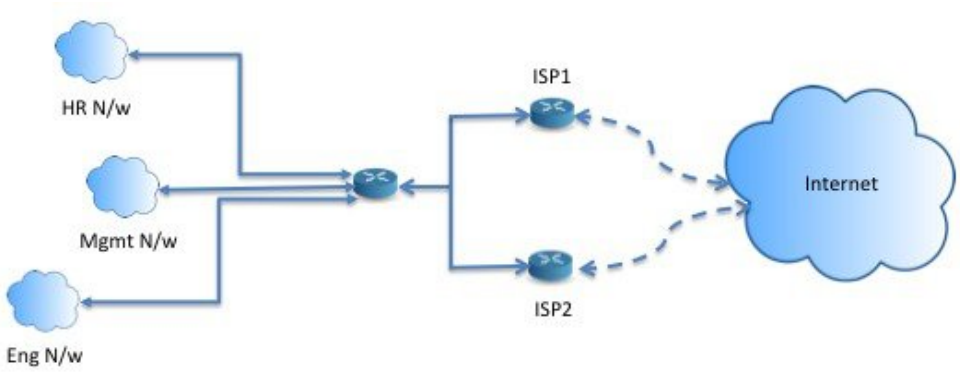
ポリシーベース ルーティングを使用する理由

ロケーション間に 2 つのリンクが導入されている企業を例に説明します。1 つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう 1 つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティング プロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅/遅延の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベース ルーティングの用途のいくつかを以下に示します。

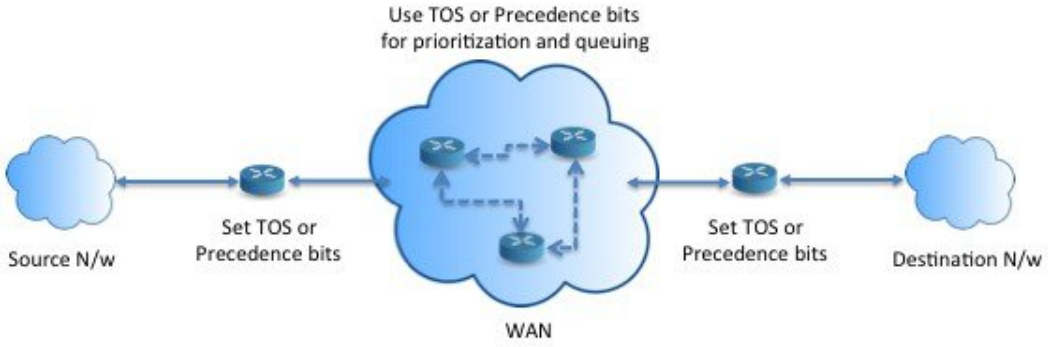
同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックは ISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベース ルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



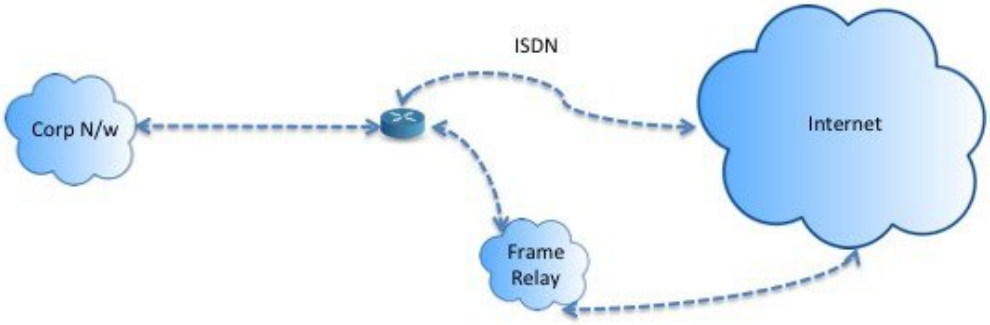
QoS

ネットワーク管理者は、ポリシーベース ルーティングでパケットにタグを付けることにより、ネットワーク トラフィックをネットワーク境界でさまざまなサービス クラスのために分類し、プライオリティ、カスタム、または重み付け均等化のキューイングを使用してそれらのサービス クラスをネットワークのコアに実装できます（下の図を参照）。この設定では、バックボーン ネットワークのコアの各 WAN インターフェイスでトラフィックを明示的に分類する必要がなくなるため、ネットワーク パフォーマンスが向上します。



コスト節約

組織は、特定のアクティビティに関連付けられている一括トラフィックを転送して、帯域幅が高い高コストリンクの使用を短時間にし、さらにここに示すようにトポロジを定義することで帯域幅が低い低コスト リンク上の基本的な接続を継続できます。



ロード シェアリング

ECMP ロード バランシングによって提供されるダイナミックなロード シェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR netto からのトラフィックと ISP2 を経由するエンジニアリング ネットワークからのトラフィックをロード シェアするようにポリシーベース ルーティングを設定できます。

PBR の実装

ASA は、ACL を使用してトラフィックを照合してから、トラフィックのルーティングアクションを実行します。具体的には、照合のために ACL を指定するルート マップを設定し、次にそのトラフィックに対して1つ以上のアクションを指定します。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルートマップを関連付けます。

ポリシーベース ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フロー別のルーティング

ASA はフロー別にルーティングを実行するため、ポリシー ルーティングは最初のパケットに適用され、その結果決定したルーティングが、そのパケットに対して作成されたフローに格納されます。同一接続に属する後続のパケットはすべてこのフローと照合され、適切にルーティングされます。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベース ルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワード レグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用されない場合には、PBR がトリガーされないことに注意してください。

クラスタ

- クラスタリングがサポートされています。
- クラスタのシナリオでは、スタティック ルートまたはダイナミック ルートがない場合、ip-verify-reverse パスを有効にした非対称トラフィックはドロップされる可能性があります。したがって、ip-verify-reverse パスを無効にすることが推奨されます。

IPv6 のサポート

IPv6 はサポートされます。

その他のガイドライン

- ルート マップ関連の既存のすべての設定の制限事項が引き続き適用されます。
- ポリシーベースルーティングには、一致ポリシーリストを含むルートマップを使用しないでください。一致ポリシーリストは BGP にのみ使用されます。

ポリシーベース ルーティングの設定

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と permit 句または deny 句が付加されます。各ルート マップ文には、match コマンドと set コマン

ドが含まれています。match コマンドは、パケット データに適用される一致基準を示します。set コマンドは、パケットに対して実行されるアクションを示します。

- IPv4 と IPv6 の両方の match/set 句でルート マップを設定した場合、または IPv4 および IPv6 トラフィックを照合する統合 ACL を使用した場合、宛先 IP のバージョンに基づいた set アクションが適用されます。
- 複数のネクストホップまたはインターフェイスを set アクションとして設定すると、使用できる有効なオプションが見つかるまですべてのオプションが順に評価されます。設定された複数のオプション間のロード バランシングは実行されません。
- verify-availability オプションは、マルチ コンテキスト モードではサポートされません。

手順

ステップ 1 ASDM で、ポリシーベース ルーティングを実行するトラフィックを特定する 1 つ以上の標準または拡張 ACL を設定します。**[Configuration]** > **[Firewall]** > **[Advanced]** > **[ACL Manager]** を表示します。

ステップ 2 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Route Maps]** の順に選択し、[Add] をクリックします。

[Add Route Map] ダイアログボックスが表示されます。

ステップ 3 ルート マップ名とシーケンス番号を入力します。オプションでルート マップ文を追加する場合は、このルート マップ名と同じ名前を使用します。シーケンス番号は、ASA がルートマップを評価する順序です。

ステップ 4 [Deny] または [Permit] をクリックします。

ACL には、固有の permit および deny 文も含まれます。ルート マップと ACL が permit/permit で一致する場合、ポリシーベース ルーティング処理が続行されます。permit/deny で一致する場合、このルート マップでの処理が終了し、別のルート マップがチェックされます。それでも結果が permit/deny であれば、通常のルーティング テーブルが使用されます。deny/deny で一致する場合、ポリシーベース ルーティング処理が続行されます。

ステップ 5 [Match Clause] タブをクリックし、作成した ACL を確認します。

[IPv4] セクションで、ドロップダウン メニューから [Access List] を選択し、ダイアログボックスで 1 つ以上の標準または拡張 ACL を選択します。

標準 ACL を使用する場合、照合は宛先アドレスに対してのみ行われます。拡張 ACL を使用する場合、送信元、宛先、またはその両方に対して照合を行えます。

IPv4 と IPv6 の両方に [IPv4] セクションを使用します。拡張 ACL では、IPv4、IPv6、アイデンティティ ファイアウォール、または Cisco TrustSec パラメータを指定できます。完全な構文については、ASA コマンド リファレンスを参照してください。

ステップ 6 [Policy Based Routing] タブをクリックし、トラフィック フローのポリシーを定義します。

一致するトラフィック フローに対して実行する set アクションを、次のうちから 1 つ以上選択します。

- [Set PBR next hop address]：IPv4 および IPv6 では、複数のネクストホップ IP アドレスを設定できます。その場合、ルーティングできる有効なネクスト ホップ IP アドレスが見つかるまで、それらのアドレスが指定された順で評価されます。設定済みのネクストホップは、直接接続する必要があります。そうでなければ、set アクションが適用されません。
- [Set default next-hop IP address]：IPv4 および IPv6 では、一致するトラフィックに対する通常のルート ルックアップが失敗した場合、ASA はここで指定されたネクストホップ IP アドレスを使用してトラフィックを転送します。
- [Recursively find and set next-hop IP address]：ネクストホップ アドレスとデフォルトのネクストホップアドレスのいずれでも、直接接続されたサブネット上でネクストホップが検出されることが要件となります。このオプションを指定した場合、ネクストホップアドレスが直接接続されている必要はありません。代わりにネクストホップアドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティングパスに従って、そのルート エントリで使用されているネクストホップに転送されます。
- [Configure Next Hop Verifiability]：ルート マップの次の IPv4 ホップが使用できるかどうかを確認します。ネクストホップの到達可能性を確認するには、SLA モニター追跡オブジェクトを設定できます。[Add] をクリックして、ネクストホップ IP アドレス エントリを追加し、次の情報を指定します。
  - [Sequence Number]：エントリはシーケンス番号を使用して順に評価されます。
  - [IP Address]：ネクスト ホップ IP アドレスを入力します。
  - [Tracking Object ID]：有効な ID を入力します。
- [Set interfaces]:このオプションを使用して、一致するトラフィックを転送するために使用するインターフェイスを設定します。複数のインターフェイスを設定できます。その場合、有効なインターフェイスが見つかるまで、それらのインターフェイスが指定された順で評価されます。**null0** を指定すると、ルート マップと一致するすべてのトラフィックがドロップされます。指定されたインターフェイス（静的または動的のいずれか）経由でルーティングできる宛先のルートが存在している必要があります。
- [Set null0 interface as the default interface]：通常のルート ルックアップが失敗すると、ASA はトラフィックを null0 に転送し、トラフィックがドロップされます。
- [Set do-not-fragment bit to either 1or 0]：適切なオプション ボタンを選択します。
- [Set differential service code point (DSCP) value in QoS bits]：[IPv4] または [IPv6]ドロップダウン リストから値を選択します。

ステップ 7 [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 8 **[構成（Configuration）]>[デバイス設定（Device Setup）]>[インターフェイス設定（Interface Settings）]>[インターフェイス（Interfaces）]**の順に選択し、このルートマップを適用して出力インターフェイスを決定する入力インターフェイスを設定します。

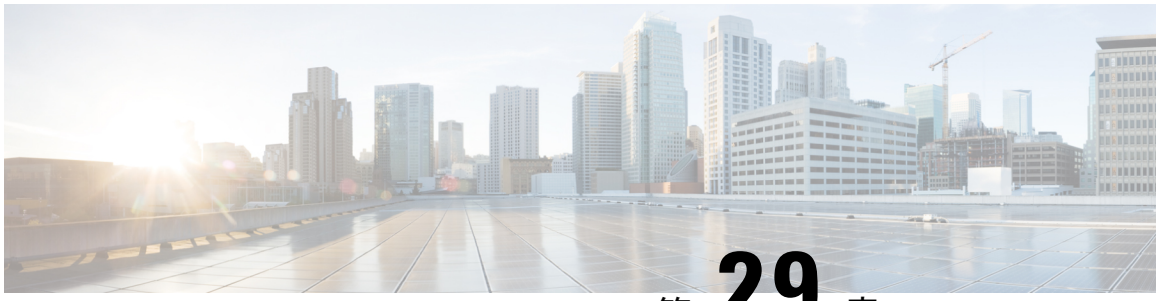
a) 入力インターフェイスを選択して、[編集（Edit）] をクリックします。
b) [ルートマップ（Route Map）] で、適用するポリシーベースのルートマップを選択します。
c) [OK] をクリックし、さらに [Apply] をクリックします。

ポリシーベース ルーティングの履歴

表 *36 :* ルート マップの履歴

機能名	プラットフォームリリース	機能情報
ポリシーベース ルーティング	9.4(1)	ポリシーベースルーティング（PBR）は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ3およびレイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックにQoSを提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネット サービス プロバイダとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザーから送信されるトラフィックをルーティングできます。 次の画面が更新されました。[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Policy Based Routing]、 [Configuration] > [Device Setup] > [Routing] > [Interface Settings] > [Interfaces]

機能名	プラットフォームリリース	機能情報
ポリシーベース ルーティングの IPv6 サポート	9.5(1)	ポリシーベース ルーティングで IPv6 アドレスがサポートされました。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Map] > [Policy Based Routing] [Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Maps] > [Match Clause]**
ポリシーベース ルーティングの VXLAN サポート	9.5(1)	VNI インターフェイスでポリシーベースルーティングを有効にできるようになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General]。
アイデンティティ ファイアウォールと Cisco TrustSec でのポリシーベース ルーティングのサポート	9.5(1)	アイデンティティ ファイアウォールと Cisco TrustSec を設定し、ポリシーベースルーティングのルートマップでアイデンティティ ファイアウォールと Cisco TrustSec ACL を使用できるようになりました。 次の画面が変更されました。**[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Maps] > [Match Clause]**



第 29 章

ルート マップ

この章では、Cisco ASA にルート マップを設定およびカスタマイズする方法について説明します。

ルート マップについて

ルート マップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するときに使用します。また、OSPF ルーティング プロセスにデフォルト ルートを生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個別のステートメントの順序シーケンスです。ACL またはルート マップの評価は、事前に定義された順序でのリストのスキャンと、一致する各ステートメントの基準の評価で構成されています。リストのスキャンは、ステートメントの一致が初めて見つかり、そのステートメントの一致に関連付けられたアクションが実行されると中断します。
- これらは汎用的なメカニズムです。基準照合と一致解釈は、適用方法とこれらを使用する機能によって決定します。同じルートマップであっても異なる機能に適用されると、解釈が異なる場合があります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルート タイプが内部であるかどうかを確認できます。
- 設計規則により、各 ACL は暗黙の deny ステートメントで終了します。照合中にルートマップの終わりに達した場合、そのルート マップの特定の適用によって結果が異なります。再配布に適用されるルート マップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny ステートメントが含まれている場合と同様に、ルート再配布が拒否されます。

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるので、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL の permit + ルート マップの permit：ルートは再配布されます。
- ACL の permit + ルート マップの deny：ルートは再配布されません。
- ACL の deny + ルート マップの permit または deny：ルート マップの句は一致せず、次のルート マップ句が評価されます。

match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。

- ルート マップの permit 句に set エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。

（注） ルート マップの deny 句では set エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

match エントリまたは set エントリがないルート マップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。

ルート マップのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

その他のガイドライン

ルート マップは、ユーザー、ユーザー グループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

ルート マップの定義

ルート マップを定義する必要があるのは、指定したルーティング プロトコルからのどのルートを対象ルーティング プロセスに再配布できるのかを指定するときです。ASDM でルート マップを定義するには、ルートマップ名、シーケンス番号、または再配布を追加、編集、または削除します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Route Maps]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Route Map] または [Edit Route Map] ダイアログボックスが表示されます。

ステップ 3 ルート マップ名とシーケンス番号を入力します。ルート マップ名とは、特定のルートに割り当てる名前です。シーケンス番号とは、ルート マップ エントリを ASA に追加または削除するときの順序です。

（注） 既存のルート マップ名を編集する場合、ルート マップ名とシーケンス番号のフィールドにはすでに値が入力されています。

ステップ 4 一致するルートの再配布を拒否するには、[Deny] をクリックします。ルート マップの Deny 句で ACL を使用すると、その ACL で許可されるルートは再配布されなくなります。一致するルートの再配布を許可するには、[Permit] をクリックします。ルートマップの Permit 句で ACL を使用すると、その ACL で許可されるルートが再配布されます。

さらに、ルートマップの Permit または Deny 句で ACL を使用する場合に、その ACL でルートが拒否されたときは、そのルートマップ句に一致するものは見つからなかったことになり、次のルート マップ句が評価されます。

ステップ 5 [Match Clause] タブをクリックして、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。

- [Match first hop interface of route] チェックボックスをオンにして、ルートのファースト ホップ インターフェイスの照合をイネーブルにするか、オフにしてディセーブルにし、指定されたネクスト ホップ インターフェイスを任意のルートと照合します。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。
  - [Interface] フィールドにインターフェイス名を入力するか、または省略記号をクリックして [Browse Interface] ダイアログボックスを表示します。
  - 1 つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。
- [IPv4] および [IPv6] セクションで、次の 1 つ以上を行います。
  - [Match Address] チェックボックスをオンにして、ルートの一致アドレスをイネーブルにするか、オフにしてディセーブルにし、パケットを照合します。
  - [Match Next Hop] チェックボックスをオンにするとルートのネクスト ホップ アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - [Match Route Source] チェックボックスをオンにするとルートのアドバタイジング ソース アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - ドロップダウン リストで [Access List] から [Prefix List] を選択して、IP アドレスを照合します。
  - 以前の選択内容に従って、省略記号をクリックして [Browse Access List] または [Browse Prefix List] ダイアログボックスを表示します。
  - 必要な ACL またはプレフィックス リストを選択します。
- [Match metric of route] チェックボックスをオンにするとルートのメトリックの照合がイネーブルになり、オフにするとディセーブルになります。
  - [Metric Value] フィールドに、メトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

- [Match Route Type] チェックボックスをオンにするとルート タイプの照合がイネーブルになり、オフにするとディセーブルになります。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルート タイプをリストから選択することができます。

ステップ 6 [Set Clause] タブをクリックして、ターゲット プロトコルに再配布される次の情報を変更します。

- [Set Metric Clause] チェックボックスを使用して、宛先ルーティング プロトコルに対するメトリック値をイネーブルにするかディセーブルにするかを指定し、値を [Value] フィールドに入力します。
- [Set Metric Type] チェックボックスをオンにすると宛先ルーティング プロトコルのメトリック タイプがイネーブルになり、オフにするとディセーブルになります。ドロップダウン リストからメトリック タイプを選択します。

ステップ 7 [BGP Match Clause] タブをクリックして、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。

- [Match AS path access lists] チェックボックスをオンにすると、BGP 自律システム パス アクセス リストと指定されたパス アクセス リストの照合がイネーブルになります。複数のパス アクセス リストを指定した場合、ルートはいずれかのパス アクセス リストと一致します。
- [Match Community] チェックボックスをオンにすると、BGP コミュニティと指定されたコミュニティの照合がイネーブルになります。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンド ルート マップにアドバタイズされません。
  - [Match the specified community exactly] チェックボックスをオンにすると、BGP コミュニティと指定されたコミュニティの厳密な照合がイネーブルになります。
- BGP ポリシーを評価および処理するためのルート マップを設定するには、[Match Policy list]チェックボックスをオンにします。複数のポリシー リストを指定した場合、ルートはいずれかのポリシー リストを処理できます。

ステップ 8 [BGP Set Clause] タブをクリックして、BGP プロトコルに再配布される次の情報を変更します。

- BGP ルートの自律システム パスを変更するには、[Set AS Path] チェックボックスをオンにします。
  - BGP ルートの前に任意の自律システム パス文字列を付加するには、[Prepend AS path] チェックボックスをオンにします。通常、ローカルな AS 番号が複数回追加され、自律システム パス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。
  - 最後の AS 番号の AS パスを先頭に追加するには、[Prepend Last AS to the AS Path] チェックボックスをオンにします。AS 番号の値を 1 ～ 10 の範囲で入力します。

- ルートのタグを自律システム パスに変換するには、[Convert route tag into AS Path] チェックボックスをオンにします。

- BGP コミュニティ属性を設定するには、[Set Community] チェックボックスをオンにします。
  - コミュニティ番号を入力するには、[Specify Community] をクリックします（必要な場合）。有効な値は、1 ～ 4294967200、internet、no-advertise、no-export です。
  - 既存のコミュニティにコミュニティを追加するには、[Add to the existing communities] チェックボックスをオンにします。
  - ルートマップをパスするプレフィックスからコミュニティ属性を除去するには、[None] をクリックします。

- 自律システム パスのプリファレンス値を指定するには、[Set local preference] チェックボックスをオンにします。
- ルーティング テーブルに対して BGP ウェイトを指定するには、[Set weight] チェックボックスをオンにします。0 ～ 65535 の範囲で値を入力します。
- BGP 送信元コードを指定するには、[Set origin] チェックボックスをオンにします。有効な値は [Local IGP] および [Incomplete] です。
- ルート マップの match 句を満たすパケットの出力アドレスを指定するには、[Set next hop] チェックボックスをオンにします。
  - パケットが出力されるネクスト ホップの IP アドレスを入力するには、[Specify IP address] をクリックします。隣接ルータである必要はありません。複数の IP アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。
  - BGP ピア アドレスにするネクスト ホップを設定するには、[Use peer address] をクリックします。

ステップ 9 [OK] をクリックします。

ルート マップのカスタマイズ

ここでは、ルート マップをカスタマイズする方法について説明します。

特定の宛先アドレスに一致するルートの定義

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Route Maps]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Route Map] ダイアログボックスが表示されます。このダイアログボックスでは、ルートマップ名、シーケンス番号、その再配布アクセス（許可または拒否）の割り当てまたは選択を行うことができます。ルートマップのエントリは順番に読み取られます。この順序は、シーケンス番号で指定できます。シーケンス番号が指定されていない場合は、ASA にエントリを追加した順序が使用されます。

ステップ 3 [Match Clause] タブをクリックして、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。

- [Match first hop interface of route] チェックボックスをオンにして、ルートのファースト ホップ インターフェイスの照合をイネーブルにするか、オフにしてディセーブルにし、指定されたネクスト ホップ インターフェイスを任意のルートと照合します。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。
  - [Interface] フィールドにインターフェイス名を入力するか、または省略記号をクリックして [Browse Interface] ダイアログボックスを表示します。
  - インターフェイス タイプ（[inside] または [outside]）を選択し、[Selected Interface] をクリックして、[OK] をクリックします。
  - [Match IP Address] チェックボックスをオンにして、ルートの一致アドレスをイネーブルにするか、オフにしてディセーブルにし、パケットを照合します。
  - [Match Next Hop] チェックボックスをオンにするとルートのネクスト ホップ アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - [Match Route Source] チェックボックスをオンにするとルートのアドバタイジング ソース アドレスの照合がイネーブルになり、オフにするとディセーブルになります。
  - ドロップダウン リストで [Access List] から [Prefix List] を選択して、IP アドレスを照合します。
  - 以前の選択内容に従って、省略記号をクリックして [Browse Access List] または [Browse Prefix List] ダイアログボックスを表示します。
  - 必要な ACL またはプレフィックス リストを選択します。
- [Match metric of route] チェックボックスをオンにするとルートのメトリックの照合がイネーブルになり、オフにするとディセーブルになります。

- [Metric Value] フィールドに、メトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

- [Match Route Type] チェックボックスをオンにするとルート タイプの照合がイネーブルになり、オフにするとディセーブルになります。有効なルート タイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルート タイプをリストから選択することができます。

プレフィックス ルールの設定

（注） プレフィックス ルールを設定する前に、プレフィックス リストを設定する必要があります。

プレフィックス ルールを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[IPv4 Prefix Rules]** または [IPv6 Prefix Rules] を選択します。

ステップ 2 [Add] をクリックし、[Add Prefix Rule] を選択します。

[Add Prefix Rule] ダイアログボックスが表示されます。このダイアログボックスでは、シーケンス番号を追加し、IP のバージョン（IPv4 または IPv6）を選択し、ネットワークのプレフィックス、再配布アドレス（許可または禁止）、プレフィックスの最小長と最大長を指定できます。

ステップ 3 オプションの [Sequence Number} を入力するか、デフォルト値を受け入れます。

ステップ 4 IP アドレス/マスク長の形式で [Prefix] 番号を指定します。

ステップ 5 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6 オプションの [Minimum length] および [Maximum length] を入力します。

ステップ 7 完了したら、[OK] をクリックします。

新規追加または修正したプレフィックス ルールがリストに表示されます。

ステップ 8 [Apply] をクリックして変更内容を保存します。

プレフィックス リストの設定

ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。デフォルトでは、シーケンス番号は自動的に生成され、開始値は 5 で 5 ずつ増えていきます。

プレフィックス リストを追加するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[IPv4 Prefix Rules]** または [IPv6 Prefix Rules] を選択します。

ステップ 2 **[Add]** > **[Add Prefix List]** をクリックします。

[Add Prefix List] ダイアログボックスが表示されます。

ステップ 3 プレフィックス名と説明を入力して [OK] をクリックします。

ルート アクションのメトリック値の設定

ルート アクションのメトリック値を設定するには、次の手順を実行します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Route Maps]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Route Map] または [Edit Route Map] ダイアログボックスが表示されます。このダイアログボックスでは、ルートマップ名、シーケンス番号、およびその再配布アクセス（許可または拒否）の割り当てまたは選択を行うことができます。ルートマップのエントリは順番に読み取られます。この順序は、シーケンス番号で指定できます。シーケンス番号が指定されていない場合は、ASA にルート マップ エントリを追加した順序が使用されます。

ステップ 3 [Set Clause] タブをクリックして、ターゲット プロトコルに再配布される次の情報を変更します。

- [Set Metric Clause] チェックボックスを使用して、宛先ルーティング プロトコルに対するメトリック値をイネーブルにするかディセーブルにするかを指定し、値を [Value] フィールドに入力します。
- [Set Metric Type] チェックボックスをオンにすると宛先ルーティング プロトコルのメトリック タイプがイネーブルになり、オフにするとディセーブルになります。ドロップダウン リストからメトリック タイプを選択します。

ルート マップの例

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。

1. ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Route Maps]** の順に選択します。
2. [Add] をクリックします。
3. [Route Map Name] フィールドに **1-to-2** と入力します。
4. ルーティング シーケンス番号を [Sequence Number] フィールドに入力します。
5. [Permit] オプション ボタンをクリックします。

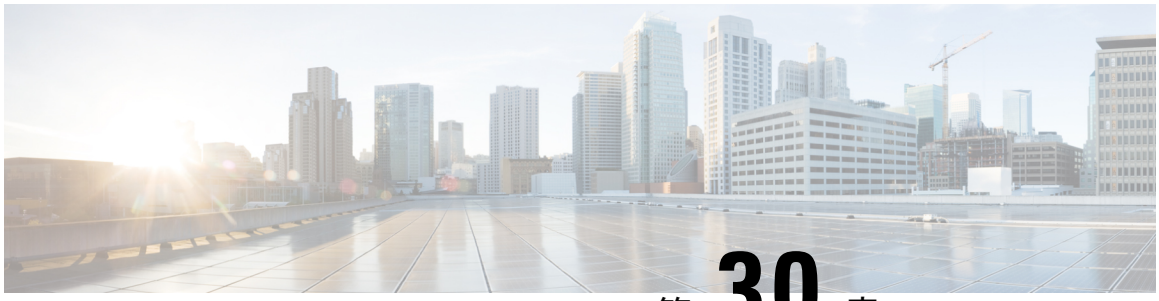
   デフォルトでは、このタブは一番上にあります。
6. [Match Clause] タブをクリックします。
7. [Match Metric of Route] チェックボックスをオンにして、メトリック値 **1** を入力します。
8. [Set Clause] タブをクリックします。
9. [Set Metric Value] チェックボックスをオンにして、メトリック値 **5** を入力します。
10. [Set Metric-Type] チェックボックスをオンにして、[Type-1] を選択します。

ルート マップの履歴

表 *37 :* ルート マップの機能履歴

機能名	プラットフォームリリース	機能情報
ルート マップ	7.0(1)	この機能が導入されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [Route Maps]。

機能名	プラットフォームリリース	機能情報
スタティックおよびダイナミック ルート マップのサポートの強化	8.0(2)	ダイナミックおよびスタティック ルート マップのサポートが強化されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	ルート マップは、マルチ コンテキスト モードでサポートされます。
BGP のサポート	9.2(1)	この機能が導入されました。 [Configuration] > [Device Setup] > [Routing] > [Route Maps] 画面が更新され、2 つのタブ [BGP match clause] および [BGP set clause] が追加されました。
プレフィックス ルールの IPv6 サポート	9.3.2	この機能が導入されました。 次の画面が更新されました。 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[IPv4 Prefix Rules]** および **[IPv6 Prefix Rules]**



第 30 章

双方向フォワーディング検出ルーティング

この章では、双方向フォワーディング検出（BFD）ルーティング プロトコルを使用するように Secure Firewall ASA を設定する方法について説明します。

BFD ルーティングについて

BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。BFD は、2 つのシステム間の転送データ プロトコルすべてに加えて、ユニキャストのポイントツーポイント モードで動作します。パケットは、メディアやネットワークに対して適切なカプセル化プロトコルのペイロードで送信されます。

BFD は高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD 非同期モードおよびエコー機能

BFD は、エコー機能が有効であるかどうかに関わらず非同期モードで動作できます。

非同期モード

非同期モードでは、システムが相互に BFD 制御パケットを定期的に送信します。一方のシステムがこれらのパケットの多くを連続して受信しない場合、セッションはダウンしているものと宣言されます。純粋な非同期モード（エコー機能なし）では、エコー機能に必要な特定の検出時間を達成するのに必要なパケットの数が半分で済むため、便利です。

BFD エコー機能

BFD エコー機能は、フォワーディング エンジンから、直接接続シングル ホップ BFD ネイバーへエコー パケットを送信します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために同じパスに沿って返信されます。もう一方の BFD セッションは、エコー パケットの実際のフォワーディングに参加しません。エコー機能およびフォワーディング エンジンが検出プロセスを処理するため、BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディング エンジンがリモート ネイバー システムでフォワーディング パスをテストする際にリモート システムが関与しないため、パケット間の遅延のばらつきが改善します。この結果、障害検出にかかる時間が短くなります。

エコー機能が有効な場合、BFD はスロー タイマーを使用して、非同期セッションの時間を長くし、BFD ネイバー間で送信される BFD 制御パケットの数を減らすことができます。これにより、処理オーバーヘッドが削減し、同時に障害検出時間が短くなります。

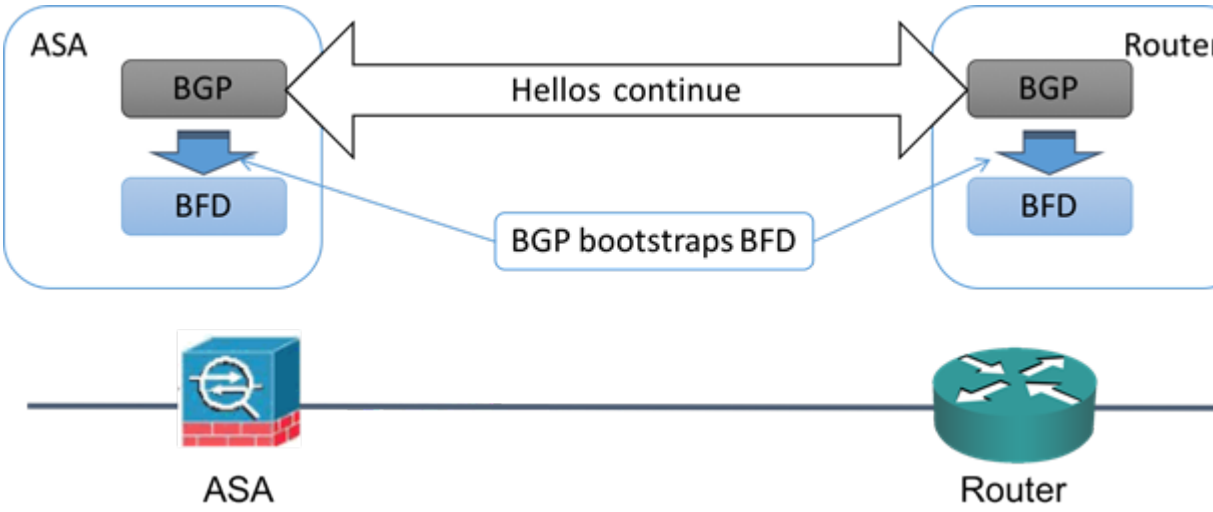
（注） IPv4 マルチホップまたは IPv6 シングルホップ BFD ネイバーでは、エコー機能はサポートされていません。

BFD はインターフェイス レベルとルーティング プロトコル レベルで有効にできます。両方のシステム（BFD ピア）で BFD を設定する必要があります。インターフェイスと、該当するルーティング プロトコルのルータ レベルで BFD を有効にすると、BFD セッションが作成され、BFD タイマーがネゴシエートされ、BFD ピアが BFD コントロール パケットをネゴシエートされたレベルで相互に送信し始めます。

BFD セッション確立

次の例は、ASA と Border Gateway Protocol（BGP）を実行する隣接ルータを示します。両方のデバイスが起動する時点では、デバイス間で BFD セッションは確立されていません。

図 *65 : BFD* セッションの確立



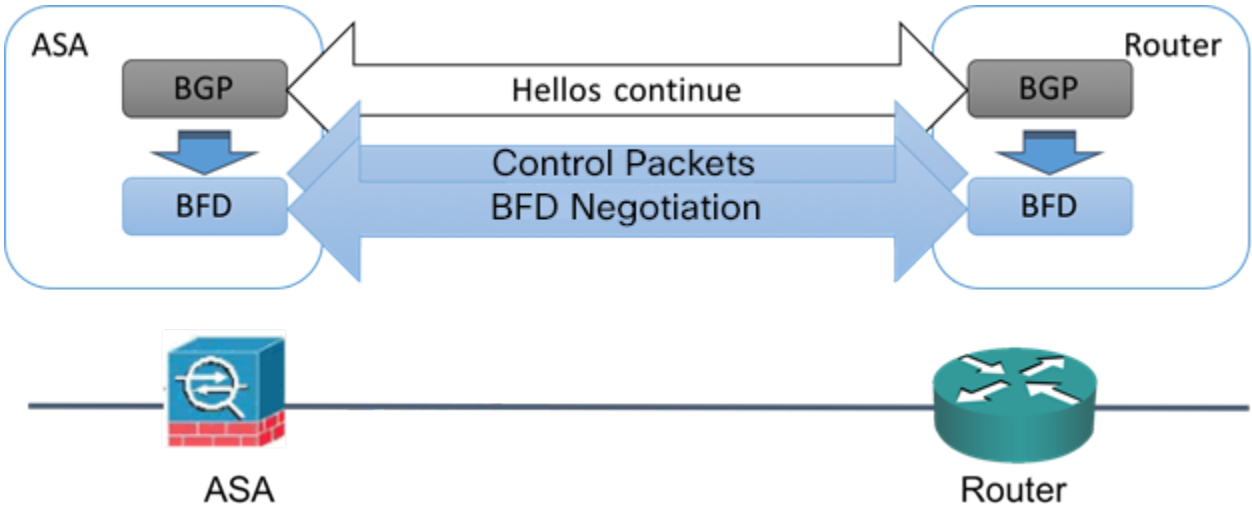
BGP は、BGP ネイバーの特定後に、そのネイバーの IP アドレスを使用して BFD プロセスをブートストラップします。BFD はそのピアを動的に検出しません。BFD は、設定されているルーティング プロトコルから、使用する IP アドレスと形成するピア関係を把握します。

ルータの BFD と ASA の BFD により BFD 制御パケットが形成され、BFD セッションが確立されるまで 1 秒間隔でこのパケットが相互に送信されます。両方のシステムの最初の制御パケットは非常によく似ています。たとえば、Vers、Diag、H、D、P、および F ビットはすべてゼロに設定され、State は Down に設定されます。[My Discriminator] フィールドには、送信デバイスで一意の値が設定されます。[Your Discriminator] フィールドにはゼロが設定されます。これは、BFD セッションがまだ確立されていないためです。TX タイマーと RX タイマーには、デバイスの設定で検出された値が設定されます。

リモート BFD デバイスは、セッション開始フェーズで BFD 制御パケットを受信すると、[My Discriminator] フィールドの値をデバイス自体の [Your Discriminator] フィールドに設定し、[Down] 状態から [Init] 状態、そして最終的には [Up] 状態に移行します。両方のシステムが、相互の制御パケットで各自の Discriminator を検出すると、セッションが正式に確立されます。

次の図は、確立された BFD 接続を示します。

図 *66 : BFD* セッションが確立されていない *BGP*



BFD タイマー ネゴシエーション

BFD デバイスは、BFD 制御パケットの送信速度を制御および同期するため、BFD タイマーをネゴシエートする必要があります。BFD タイマーをネゴシエートする前に、デバイスは以下の点を確認する必要があります。

- そのピア デバイスが、ローカル デイバスの提示されるタイマーを含むパケットを確認している。
- ピアで設定されている BFD 制御パケットの受信速度を上回る速度でデバイスが BFD 制御パケットを送信することがない。
- ローカル システムで設定されている BFD 制御パケットの受信速度を上回る速度でピアが BFD 制御パケットを送信することがない。

[Your Discriminator] フィールドと H ビットの設定は、初期タイマーの期間中にリモート デバイスがそのパケットを確認するローカルデバイスを交換できるようにするのに十分です。各システムは BFD 制御パケットを受信すると、Required Min RX Interval をシステム自体の Desired Min TX Interval と比較し、2 つの値のうち大きい方の値（低速な値）を、BDF パケットの転送速度として使用します。2 つのシステムのうち低速なシステムによって、転送速度が決定します。

これらのタイマーがネゴシエートされていない場合、セッション中の任意の時点で、セッションをリセットすることなく再ネゴシエートできます。タイマーを変更するデバイスは、F ビットがセットされている BFD 制御パケットをリモート システムから受信するまで、後続のすべての BFD 制御パケットの P ビットをセットします。このビット交換により、転送中に失われる可能性があるパケットが保護されます。

（注） リモート システムによって F ビットがセットされている場合、新たに提示されるタイマーをリモート システムが受け入れることを意味しているわけではありません。これは、タイマーが変更されたパケットをリモート システムが確認したことを意味します。

BFD 障害検出

BFD セッションとタイマーがネゴシエートすると、BFD のピアは、ネゴシエートされた間隔で BFD 制御パケットを相互に送信します。これらの制御パケットはハートビートの役割を果たします。これは、IGP Hello プロトコルとよく似ていますが、レートはさらに速くなっています。

設定されている検出間隔（必要な最小 RX 間隔）内の BFD 制御パケットを各 BFD ピアが受信する限り、BFD セッションは有効であり、BFD と関連付けられたルーティング プロトコルは隣接関係を維持します。BFD ピアがこの間隔内に制御パケットを受信しない場合、その BFD セッションに参加しているクライアントに障害発生を通知します。ルーティング プロトコルにより、その情報に対する適切な応答が決定されます。標準的な応答は、ルーティング プロトコル ピア セッションを終了し、再コンバージェンスの後、障害の発生したピアをバイパスすることです。

BFD セッション中に BFD ピアが正常に BFD 制御パケットを受信するたびに、このセッションの検出タイマーがゼロにリセットされます。したがって、障害検出は、受信側が最後にパケットを送信した時点ではなく、パケット受信に依存しています。

BFD 導入シナリオ

具体的なシナリオで BFD がどのように動作するかについて、以下に説明します。

フェールオーバー

フェールオーバー シナリオでは、アクティブ ユニットとネイバー ユニット間で BFD セッションが確立、維持されます。スタンバイ ユニットはネイバーとの BFD セッションを維持しません。フェールオーバーが発生すると、新しいアクティブ ユニットがネイバーとのセッション確立を開始する必要があります。これは、アクティブ ユニットとスタンバイ ユニットの間ではセッション情報が同期されないためです。

グレースフル リスタート/NSF シナリオでは、クライアント（BGP IPv4/IPv6）がそのネイバーに対してイベントを通知します。ネイバーはこの情報を受信すると、フェールオーバーが完了するまで RIB テーブルを維持します。フェールオーバー中に、デバイスで BFD と BGP セッションがダウンします。フェールオーバーが完了し、BGP セッションがアップになると、ネイバー間で新しい BFD セッションが確立されます。

スパンド EtherChannel および L2 クラスタ

スパンド EtherChannel クラスタ シナリオでは、プライマリ ユニットとそのネイバー間で BFD セッションが確立、維持されます。従属ユニットはネイバーとの間の BFD セッションを維持しません。スイッチでのロードバランシングが原因で BFD パケットが従属ユニッ

トにルーティングされる場合、従属ユニットはこのパケットをクラスタ リンク経由でプライマリ ユニットに転送する必要があります。クラスタ スイッチオーバーが発生すると、新しいプライマリユニットがネイバーとのセッション確立を開始します。これは、プライマリ ユニットと従属ユニットの間でセッション情報が同期されていないためです。

個別インターフェイス モードと L3 クラスタ

個別インターフェイスモードクラスタのシナリオでは、個々のユニットが各自のネイバーとの BFD セッションを維持します。

BFD ルーティングのガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでサポートされます。スタンドアロン、フェールオーバー、およびクラスタ モードをサポートします。BFD は、フェールオーバーおよびクラスタ インターフェイスではサポートされません。クラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。BFD は、トランスペアレント モードではサポートされません。

IPv6 のガイドライン

エコー モードは IPv6 ではサポートされません。

その他のガイドライン

BGP IPv4 および BGP IPv6 プロトコルはサポートされません。

OSPFv2、OSPFv3、IS-IS、および EIGRP プロトコルはサポートされません。

スタティック ルートの BFD はサポートされません。

転送およびトンネルでの BFD はサポートされません。

BFD の設定

ここでは、システムで BGP ルーティング プロセスを有効にして設定する方法について説明します。

手順

ステップ 1 BFD テンプレートの作成 （891 ページ）。

ステップ 2 BFD インターフェイスの設定 （893 ページ）。

ステップ 3 BFD マップの設定 （893 ページ）。

BFD テンプレートの作成

このセクションでは、BFD テンプレートを作成して BFD コンフィギュレーション モードを開始するために必要な手順を説明します。

BFD テンプレートは、一連の BFD 間隔値を指定します。BFD テンプレートで指定された BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。また、シングルホップ セッションとマルチホップ セッションの認証も設定できます。エコーをイネーブルにできるのは、シングルホップのみです。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Template]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

新しい BFD テンプレートを作成する場合は、[Add BFD Template] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[Edit BFD Template] ダイアログボックスを使用します。

ステップ 3 [Template] タブで、次の項目を設定します。

- [Template Name]：この BFD テンプレートの名前。テンプレートの残りのパラメータを設定するには、名前を割り当てる必要があります。テンプレート名にスペースを含めることはできません。
- [Configuration Mode]：ドロップダウン リストから、[single-hop] または [multi-hop] を選択します。
- [Enable Echo]：（オプション）シングルホップ テンプレートでエコーをイネーブルにします。

エコー機能がネゴシエートされない場合、検出時間を満たすように高いレートで BFD 制御パケットが送信されます。エコー機能がネゴシエートされている場合、BFD制御パケットはより低速の、ネゴシエートされたレートで送信され、自己転送されるエコーパケットはより高速のレートで送信されます。可能であればエコー モードを使用することを推奨します。

ステップ 4 [Interval] タブで、次の項目を設定します。

a) [Interval Type] ドロップダウン リストから、[None]、[Both]、[Microseconds]、または [Milliseconds] を選択します。

b) [Both] を選択した場合は、次のオプションを設定します。

- [Multiplier Values]：ホールド ダウン時間を計算するために使用する値。BFD ピアから連続して紛失してよいBFD制御パケットの数を指定します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言し、レイヤ3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。デフォルトは 3 です。
- [Both Transmit and Receive Values]：最小送受信間隔機能です。有効値は 50 ～ 999 ミリ秒です。

c) [Microseconds] を選択した場合は、[Both] オプション ボタンをクリックして次の項目を設定できます。

- [Multiplier Values]：ホールド ダウン時間を計算するために使用する値。BFD ピアから連続して紛失してよいBFD制御パケットの数を指定します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言し、レイヤ3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。デフォルトは 3 です。
- [Minimum Transmit Values]：最小伝送間隔機能です。有効値は 50,000 ～ 999,000 マイクロ秒です。
- [Minimum Receive Values]：最小受信間隔機能です。有効値は 50,000 ～ 999,000 マイクロ秒です。

d) [Milliseconds] を選択した場合は、次のオプションを設定します。

- [Multiplier Values]：BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。
- [Minimum Transmit Values]：最小伝送間隔機能です。有効値は 50 ～ 999 ミリ秒です。
- [Minimum Receive Values]：最小受信間隔機能です。有効値は 50 ～ 999 ミリ秒です。

ステップ 5 [Authentication] タブで、次の項目を設定します。

- [Authentication Type]：ドロップダウン リストから、[NONE]、[md5]、[meticulous-sha-1]、[meticulous-md5]、または [sha-1] を選択します。
- [Key Value]：認証されるルーティング プロトコルを使用してパケットで送信および受信される必要のある認証文字列を指定します。有効な値は、1～17文字の大文字と小文字の英数字からなる文字列です。ただし、最初の文字は数字にはできません。
- [Key ID]：キー値と照合する共有キー ID。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックして、BFD テンプレート コンフィギュレーションを保存します。

BFD インターフェイスの設定

BFD テンプレートをインターフェイスにバインドすることで、基準 BFD セッション パラメータの設定およびエコーモードのイネーブル化をインターフェイスごとに行うことができるようになります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Interface]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

新しい BFD インターフェイスを設定する場合は、[Add Interface] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[Edit Interface] ダイアログボックスを使用します。

ステップ 3 [Interface] ドロップダウン リストから、BFD を設定するインターフェイスを選択します。

ステップ 4 [Template Name] チェックボックスをオンにして、ドロップダウン リストから BFD テンプレートを選択します。

ステップ 5 次の BFD 間隔を設定します。

- [Minimum Transmit Values]：最小伝送間隔を指定します。有効値は 50 ～ 999 ミリ秒です。
- [Minimum Receive Values]：最初受信間隔を指定します。有効値は 50 ～ 999 ミリ秒です。
- [Multiplier]：BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。

ステップ 6 （オプション）このインターフェイスでエコーモードを使用する場合は、[Echo] チェックボックスをオンにします。エコーをイネーブルにできるのは、シングル ホップ テンプレートのみです。

ステップ 7 [OK] をクリックします。

BFD マップの設定

マルチホップ テンプレートに関連付けることができる宛先が含まれている BFD マップを作成できます。マルチホップ BFD テンプレートがすでに設定されている必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BFD]** > **[Map]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

新しいBFDマップを設定する場合は、[Add Map] ダイアログボックスを使用します。既存のパラメータを変更する場合は、[Edit Map] ダイアログボックスを使用します。

ステップ 3 [Template Name] ドロップダウンリストから BFD テンプレートを選択します。

ステップ 4 次の BFD 間隔を設定します。

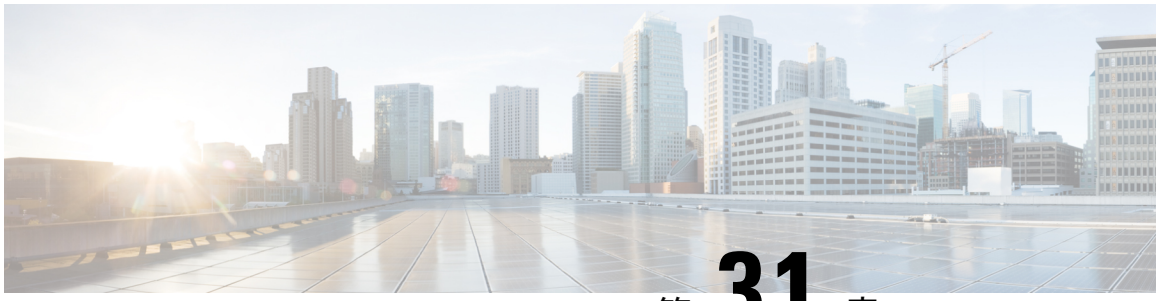
- [Minimum Transmit Values]：最小伝送間隔機能です。有効値は 50 ～ 999 ミリ秒です。
- [Minimum Receive Values]：最初受信間隔を指定します。有効値は 50 ～ 999 ミリ秒です。
- [Multiplier]：BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言し、レイヤ3BFDピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。

ステップ 5 [OK] をクリックします。

BFD ルーティングの履歴

表 *38 : BFD* ルーティングの機能履歴

機能名	プラットフォームリリース	機能情報
BFD ルーティング サポート	9.6(2)	ASAは、BFD ルーティング プロトコルをサポートするようになりました。BFDテンプレート、インターフェイスおよびマッピングの設定が新たにサポートされました。BFDを使用するための BGP ルーティング プロトコルのサポートも追加されました。 次の画面が追加または変更されました。 **[Configuration] > [Device Setup] > [Routing] > [BFD] > [Template]** **[Configuration] > [Device Setup] > [Routing] > [BFD] > [Interface]** **[Configuration] > [Device Setup] > [Routing] > [BFD] > [Map]** **[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] > [Neighbor]**



第 31 章

BGP

この章では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Cisco ASA を設定する方法について説明します。

BGP について

BGP は相互および内部の自律システムのルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダ（ISP）間で使用されるプロトコルです。

BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイ プロトコル（IGP）を通常使用しています。顧客は ISP に接続し、ISP は BGP を使用して顧客のルートと ISP のルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

BGP は、IPv6 ネットワーク上で IPv6 プレフィックスのルーティング情報を伝送するために使用することもできます。

（注） BGPv6 デバイスは、クラスタに参加すると、ロギング レベル 7 が有効の場合ソフト トレースバックを生成します。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGPルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

（注） AS ループの検出は、完全な AS パス（AS_PATH 属性で指定される）をスキャンし、ローカル システムの AS 番号が AS パスに現れないことを確認することによって実行されます。デフォルトでは、EBGP は学習したルートを同じピアにアドバタイズすることで、ループチェックを実行するときに ASA で追加の CPU サイクルが発生することを防ぐとともに、既存の発信更新タスクの遅延を防ぎます。

BGPにより学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- [重要度（Weight）]：これは、シスコ定義の属性で、ルータに対してローカルです。[重要度（Weight）] 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重要度（Weight）] 属性値が最も大きいルートが優先されます。
- [ローカル プリファレンス（Local preference）]：この属性は、ローカル AS からの出力点を選択するために使用されます。[重要度（Weight）]属性とは異なり、[ローカルプリファレンス（Local preference）] 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、[ローカル プリファレンス（Local preference）] 属性値が最も高い出力点が特定のルートの出力点として使用されます。
- [Multi-Exit 識別子（Multi-exit discriminator）]：メトリック属性である Multi-Exit 識別子（MED）は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MED を受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- [発信元（Origin）]：この属性は、BGP が特定のルートについてどのように学習したかを示します。[発信元（Origin）] 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - [IGP]：ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する際に設定されます。
  - [EGP]：ルートは Exterior Border Gateway Protocol（EBGP）を使用して学習されます。
  - [未完了（Incomplete）]：ルートの送信元が不明であるか、他の方法で学習されています。未完了の発信元は、ルートが BGP に再配布されるときに発生します。

- [AS_path]：ルート アドバタイズメントが自律システムを通過すると、ルート アドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティング テーブルにインストールされます。
- [ネクスト ホップ（Next hop）]：EBGP の [ネクスト ホップ（Next hop）] 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。
- [コミュニティ（Community）]：この属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルート マップは、[コミュニティ（Community）] 属性を設定するために使用されます。定義済みの [コミュニティ（Community）] 属性は次のとおりです。
  - [no-export]：EBGP ピアにこのルートをアドバタイズしません。
  - [no-advertise]：このルートをどのピアにもアドバタイズしない。
  - [インターネット（internet）]：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP はベスト パスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、この更新はドロップされます。
- ウェイトが最大のパスが優先されます。
- ウェイトが同じである場合、ローカルの優先順位が最大のパスが優先されます。
- ローカルの優先順位が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_path が最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じである場合、起点タイプが最下位のパス（[IGP] は [EGP] よりも低く、[EGP] は [不完全（Incomplete）] よりも低い）が優先されます。
- 起点コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGP マルチパス （898 ページ） のルーティング テーブルで、複数のパスのインストールが必要かどうかを判断します。

- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同一の宛先プレフィックスへの複数の等コスト BGP パスを IP ルーティング テーブルに組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

これらのパスは、負荷共有のためのベスト パスと共にテーブルに組み込まれます。BGP マルチパスは、ベストパスの選択には影響しません。たとえば、ルータは引き続き、アルゴリズムに従っていずれかのパスをベスト パスとして指定し、このベスト パスをルータの BGP ピアにアドバタイズします。

同一宛先へのパスをマルチパスの候補にするには、これらのパスの次の特性がベストパスと同等である必要があります。

- Weight
- ローカル プリファレンス
- AS-PATH の長さ
- オリジン コード
- Multi Exit Discriminator（MED）
- 次のいずれかです。
  - ネイバー AS またはサブ AS（BGP マルチパスの追加前）
  - AS-PATH（BGP マルチパスの追加後）

一部の BGP マルチパス機能では、マルチパス候補に要件が追加されます。

- パスは外部ネイバーまたは連合外部ネイバー（eBGP）から学習される必要があります。
- BGP ネクスト ホップへの IGP メトリックは、ベストパス IGP メトリックと同等である必要があります。

内部 BGP（iBGP）マルチパス候補の追加要件を次に示します。

- 内部ネイバー（iBGP）からパスが学習される必要があります。
- ルータが不等コスト iBGP マルチパス用に設定されていない限り、BGP ネクストホップへの IGP メトリックは、ベスト パス IGP メトリックと同等です。

BGP はマルチパス候補から最近受信したパスのうち、最大 *n* 本のパスを IP ルーティング テーブルに挿入します。この *n* は、BGP マルチパスの設定時に指定した、ルーティング テーブルに組み込まれるルートの数です。マルチパスが無効な場合のデフォルト値は 1 です。

不等コスト ロード バランシングの場合、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルーテッド モードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

その他のガイドライン

- システムは、PPPoE 経由で受信した IP アドレスのルートエントリを CP ルートテーブルに追加しません。BGP は常に CP ルートテーブルを調べて TCP セッションを開始するため、BGP は TCP セッションを形成しません。

  つまり、PPPoE 経由の BGP はサポートされません。

- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。

- メンバーユニットの BGP テーブルは、制御ユニットテーブルと同期されません。ルーティングテーブルだけが、制御ユニットのルーティングテーブルと同期されます。

BGP の設定

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 BGP の有効化 （900 ページ）。
ステップ 2 BGP ルーティング プロセスの最適なパスの定義 （901 ページ）。
ステップ 3 ポリシー リストの設定 （902 ページ）。
ステップ 4 AS パス フィルタの設定 （904 ページ）。
ステップ 5 コミュニティ ルールの設定 （905 ページ）。
ステップ 6 IPv4 アドレス ファミリの設定 （906 ページ）。
ステップ 7 IPv6 アドレス ファミリの設定 （914 ページ）。

BGP の有効化

ここでは、BGP の有効化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

ステップ 1 シングル モードの場合、ASDM で **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[General]** の順に選択します。

（注） マルチ モードの場合、ASDM で [Configuration] > [Context Management] > [BGP] の順に選択します。BGP をイネーブルにした後に、セキュリティ コンテキストに切り替え、[Configuration] > [Device Setup] > [Routing] > [BGP] > [General] の順に選択して BGP をイネーブルにします。

ステップ 2 [Enable BGP Routing] チェックボックスをオンにします。
ステップ 3 [AS Number] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ XX.YY を指定できます。
ステップ 4 （オプション）[Limit the number of AS numbers in the AS_PATH attribute of received routes] チェックボックスをオンにして、AS_PATH 属性の AS 番号の数を特定数に制限します。有効値は 1 ～ 254 です。
ステップ 5 （オプション）[Log neighbor changes] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
ステップ 6 （オプション）[Use TCP path MTU discovery] チェックボックスをオンにし、パス MTU ディスカバリ手法を使用して 2 つの IP ホスト間のネットワーク パスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。

ステップ 7 （オプション）[Enable fast external failover] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。

ステップ 8 （オプション）[Enforce that first AS is peer's AS for EBGP routes] チェックボックスをオンにすると、AS_PATH 属性の最初のセグメントとしてその AS 番号をリストしていない外部 BGP ピアから受信される着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。

ステップ 9 （オプション）[Use dot notation for AS numbers] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。

ステップ 10 [Neighbor timers] 領域でタイマー情報を指定します。

a) [Keepalive interval] フィールドに、BGP ネイバーがキープアライブ メッセージを送信しなくなった後アクティブな状態を継続する時間を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。

b) [Hold Time] フィールドに、BGP 接続が開始されて設定されている間 BGP ネイバーがアクティブな状態を維持する時間を入力します。デフォルト値は 180 秒です。

c) （オプション）[Min. Hold Time] フィールドに、BGP 接続の開始中/設定中に BGP ネイバーがアクティブな状態を維持する最小時間を入力します。0 ～ 65535 の値を指定します。

（注） ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 11 （オプション）[Non Stop Forwarding] セクションで、次の手順を実行します。

a) [Enable Graceful Restart] チェックボックスをオンにして、ASA ピアがスイッチオーバー後のルート フラップを回避できるようにします。

b) [Restart Time] フィールドに、BGP オープン メッセージを受信するまで ASA が古いルートを削除するのを待機する時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。

c) [Stale Path Time] フィールドに、リスタートする ASA から End Of Record（EOR）メッセージを受信した後、古いルートを削除するまで ASA が待機する時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

ステップ 12 [OK] をクリックします。

ステップ 13 [Apply] をクリックします。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、BGP パスの選択 （897 ページ）を参照してください。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[Best Path]** の順に選択します。

[Best Path configuration] ペインが表示されます。

ステップ 2 [Default Local Preference] フィールドに、0 ～ 4294967295 の値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバーに送信されます。

ステップ 3 [Allow comparing MED from different neighbors] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいて Multi-exit discriminator（MED）の比較ができるようにします。

ステップ 4 [Compare router-id for identical EBGP paths] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部 BGP ピアから受信した類似のパスを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。

ステップ 5 [Pick the best MED path among paths advertised from the neighboring AS] チェックボックスをオンにして、連合ピアから学習したパス間における MED 比較をイネーブルにし、新しいネットワーク エントリを追加します。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。

ステップ 6 [Treat missing MED as the least preferred one] チェックボックスをオンにして、欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[Policy Lists]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Policy List] ダイアログボックスが表示されます。このダイアログボックスでは、ポリシー リスト名、その再配布アクセス（許可または拒否）、一致インターフェイス、一致 IP アドレ

ス、一致 AS パス、一致コミュニティ名リスト、一致メトリック、一致タグ番号を追加することができます。

ステップ 3 [Policy List Name] フィールドに、ポリシー リストの名前を入力します。

ステップ 4 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5 [Match Interfaces] チェックボックスをオンにして、指定のインターフェイスの 1 つのネクスト ホップを持つルートを配布し、次のいずれかを実行します。

- [Interface] フィールドに、インターフェイス名を入力します。
- [Interface] フィールドで、省略記号をクリックすると、手動でインターフェイスを参照し、指定できます。1 つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。

ステップ 6 [Specify IP] 領域で、次のように設定します。

a) [Match Address] チェックボックスをオンにして、標準アクセス リストまたはプレフィックス リストで許可された宛先ネットワーク番号アドレスを持つルートを再配布し、パケットにポリシー ルーティングを実行します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

b) [Match Next Hop] チェックボックスをオンにして、指定したアクセス リストまたはプレフィックス リストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

c) [Match Route Source] チェックボックスをオンにして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバーによってアドバタイズされたルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

ステップ 7 [Match AS Path] チェックボックスをオンにして、BGP 自律システム パスを一致させます。

AS パス フィルタを指定するか、省略記号をクリックして手動で AS パス フィルタを参照し、指定します。1 つ以上の AS パス フィルタを選択し、[AS Path Filter] をクリックして [OK] をクリックします。

ステップ 8 [Match Community Names List] チェックボックスをオンにして、BGP コミュニティを一致させます。

a) コミュニティ ルールを指定するか、省略記号をクリックしてコミュニティ ルールを手動で参照し、指定します。1 つ以上のコミュニティ ルールを選択し、[Community Rules] をクリックして [OK] をクリックします。

b) [Match the specified community exactly] チェックボックスをオンにして、特定の BGP コミュニティを一致させます。

ステップ 9 [Match Metrices] チェックボックスをオンにして、指定したメトリックを持つルートを再配布します。複数のメトリックを指定する場合、ルートはいずれかのメトリックと一致します。

ステップ 10 [Match Tag Numbers] チェックボックスをオンにして、指定したタグと一致するルーティングテーブル内のルートを再配布します。複数のタグ番号を指定した場合、ルートはいずれかのメトリックと一致します。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックします。

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。

（注） AS パス アクセス リストは、通常のファイアウォール ACL とは異なります。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[AS Path Filters]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Filter] ダイアログボックスが表示されます。このダイアログボックスで、フィルタの名前、その再配布アクセス（許可または拒否）、および正規表現を追加できます。

ステップ 3 [Name] フィールドに、AS パス フィルタの名前を入力します。

ステップ 4 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5 正規表現を指定します。正規表現を作成するには、[Build] をクリックします。

ステップ 6 [Test] をクリックして、正規表現が選択した文字列と一致するかどうかテストします。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティリストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。ここでは、コミュニティ ルールを設定するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[Community Rules]** > の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Community Rule] ダイアログボックスが表示されます。このダイアログボックスで、ルール名、ルール タイプ、その再配布アクセス（許可または拒否）、および特定のコミュニティを追加できます。

ステップ 3 [Rule Name] フィールドに、コミュニティ ルールの名前を入力します。

ステップ 4 [Standard] または [Expanded] オプション ボタンをクリックして、コミュニティ ルール タイプを指定します。

ステップ 5 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6 標準コミュニティ ルールを追加するには、次の手順を実行します。

a) [Communities] フィールドで、コミュニティ番号を指定します。有効値は 1 ～ 4294967200 です。

b) （オプション）[Internet]（既知のコミュニティ）チェックボックスをオンにして、インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。

c) （オプション）[Do not advertise to any peers]（既知のコミュニティ）チェックボックスをオンにして、no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。

d) （オプション）[Do not export to next AS]（既知のコミュニティ）チェック ボックスをオンにして、no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 7 拡張コミュニティ ルールを追加するには、次の手順を実行します。

a) [Regular Expression] フィールドに、正規表現を入力します。または、[Build] をクリックして正規表現を作成します。

b) [Test] をクリックして、作成した正規表現が選択した文字列と一致するかどうか調べます。

ステップ 8 [OK] をクリックします。

ステップ 9 [Apply] をクリックします。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー 設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [General] をクリックします。

[General IPv4 family BGP parameters] 設定ペインが表示されます。

ステップ 3 [Administrative Distances] 領域で、[External]、[Internal] および [Local] のディスタンスを指定します。

ステップ 4 [Learned Routes Map] ドロップダウン リストからルート マップ名を選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 5 （オプション）[Generate Default Route] チェックボックスをオンにして、デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。

ステップ 6 （オプション）[Summarize subnet routes into network-level routes] チェックボックスをオンにして、ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。

ステップ 7 （オプション）[Advertise inactive routes] チェックボックスをオンにして、ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。

ステップ 8 （オプション）[Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol（IGP）への iBGP の再配布を設定します。

ステップ 9 （オプション）[Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。

ステップ 10 （オプション）[Enable address tracking] チェックボックスをオンにして、BGP ネクスト ホップ アドレス トラッキングを有効化します。[Delay Interval] フィールドで、ルーティング テーブルにインストールされている更新済みのネクストホップ ルートのチェック間の遅延間隔を指定します。

ステップ 11 （オプション）ルーティング テーブルにインストールできる並列の内部ボーダー ゲートウェイ プロトコル（iBGP）ルートの最大数を [Number of paths] フィールドで指定し、[iBGP multipaths] チェックボックスをオンにします。

ステップ 12 [Apply] をクリックします。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの1つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Aggregate Address] をクリックします。

[Aggregate Address parameters] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Aggregate Address] ペインが表示されます。

ステップ 4 [Network] フィールドでネットワーク オブジェクトを指定します。

ステップ 5 [Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。

ステップ 6 [Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートをすべてフィルタリングします。

ステップ 7 [Attribute Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルート マップを追加または設定します。

ステップ 8 [Advertise Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルートを追加または設定します。

ステップ 9 [Suppress Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルートを追加または設定します。

ステップ 10 [OK] をクリックします。

ステップ 11 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。

ステップ 12 [Apply] をクリックします。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** を選択します。

ステップ 2 [Filtering] をクリックします。

[Define filters for BGP updates] ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Filter] ペインが表示されます。

ステップ 4 [Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。

ステップ 5 [Access List] ドロップダウン リストから標準アクセス リストを選択します。[Manage] をクリックして、新しい ACL を追加します。

ステップ 6 発信フィルタには、オプションで、配信されるルートのタイプを指定できます。

a) [Protocol] ドロップダウン リストからオプションを選択します。

[BGP]、[EIGRP]、[OSPF]、または [RIP] などのルーティング プロトコルを選択できます。

接続ルートから学習されたピアおよびネットワークをフィルタリングするには、[Connected] を選択します。

スタティック ルートから学習されたピアおよびネットワークをフィルタリングするには、[Static] を選択します。

b) [BGP]、[EIGRP]、または [OSPF] を選択した場合は、そのプロトコルのプロセス ID も [Process ID] で選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** >**[Routing]** **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Neighbor] クリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 左側のペインで、[General] をクリックします。

ステップ 5 [IP Address] フィールドに BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。

ステップ 6 [Remote AS] フィールドに、BGP ネイバーが属する自律システムを入力します。

ステップ 7 （オプション）[Description] フィールドに BGP ネイバーの説明を入力します。

ステップ 8 （オプション）[Shutdown neighbor administratively] チェックボックスをオンにして、ネイバーまたはピア グループを無効にします。

ステップ 9 （オプション）[Enable address family] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。

ステップ 10 （オプション）[Global Restart Functionality for this peer] チェックボックスをオンにして、ASA ネイバーまたはピア グループの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

ステップ 11 左側のペインで、[Filtering] をクリックします。

ステップ 12 （オプション）[Filter routes using an access list] 領域で、適切な着信または発信アクセス コントロール リストを選択して BGP ネイバー情報を配布します。必要に応じて、[Manage] をクリックして、ACL と ACE を追加します。

ステップ 13 （オプション）[Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。

ステップ 14 （オプション）[Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。

ステップ 15 （オプション）[Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。

ステップ 16 （オプション）[Limit the number of prefixes allowed from the neighbor] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。

- [Maximum prefixes] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
- [Threshold level] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。
- （オプション）[Control prefixes received from a peer] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
  - プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[Terminate peering when prefix limit is exceeded] をクリックします。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
  - 最大プレフィックス数の制限値を超えたときにログ メッセージを生成するには、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。

ステップ 17 左側のペインで、[Routes] をクリックします。

ステップ 18 [Advertisement Interval] フィールドに、BGP ルーティング アップデートが送信される最小間隔（秒）を入力します。

ステップ 19 （オプション）[Generate Default route] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

- [Route map] ドロップダウン リストから、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 20 （オプション）条件に応じてアドバタイズされるルートを追加するには、次の手順を実行します。

a) [Conditionally Advertised Routes] セクションで [Add] をクリックします。

b) exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。

c) 次のいずれかを実行します。

- [Exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
- [Non-exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

d) [OK] をクリックします。

ステップ 21 （オプション）[Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバイタイズ対象から除外します。

ステップ 22 左側のペインで、[Timers] をクリックします。

ステップ 23 （オプション）[Set timers for the BGP peer] チェックボックスをオンにし、キープアライブ頻度、保持時間、最小保持時間を設定します。

- [Keepalive frequency] フィールドに、ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
- [Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）を入力します。デフォルト値は 180 秒です。
- （オプション）[Min Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）を入力します。

（注） ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 24 左側のペインで、[Advanced] をクリックします。

ステップ 25 （オプション）[Enable Authentication] チェックボックスをオンにして、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。

- [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。
- パスワードを [Password] フィールドに入力します。[パスワードの確認（Confirm Password）] フィールドにパスワードを再入力します。

  パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 26 （オプション）[Send Community Attribute to this neighbor**]** チェックボックスをオンにします。

ステップ 27 （オプション）[Use ASA as next hop for neighbor] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

ステップ 28 次のいずれかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
  - （オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。
  - （オプション）[Disable connection verification] チェックボックスをオンにし、ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認を無効にします。
- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリング セッションを保護できるようにします。
  - [TTL ホップ（TTL hops）] フィールドに、eBGP ピアを区切るホップの最大数を入力します。 有効な値は、1 ～ 254 です。

ステップ 29 （オプション）[Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 30 [BGP version] ドロップダウン リストから、ASA が受け入れる BGP バージョンを選択します。

（注） バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 31 （オプション）[TCP Path MTU Discovery] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションをイネーブルにします。

ステップ 32 [TCP transport mode] ドロップダウン リストから TCP 接続モードを選択します。

ステップ 33 左側のペインで、[Migration] をクリックします。

ステップ 34 （オプション）[Customize the AS number for routes received from the neighbor] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

- [Local AS Number] フィールドにローカル自律システム番号を入力します。有効な値は、1 ～ 65535 です。
- （オプション）[Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。
- （オプション）[Replace real AS number with local AS number in routes received from neighbor] チェックボックスをオンにします。ローカル ルーティング プロセスの AS 番号は前に追加されません。
- （オプション）[Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 35 [OK] をクリックします。

ステップ 36 [Apply] をクリックします。

IPv4 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Networks] をクリックします。

[Define networks to be advertised by the BGP routing process] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Network] ペインが表示されます。

ステップ 4 [Address] フィールドで BGP がアドバタイズするネットワークを指定します。

ステップ 5 （オプション）[Netmask] ドロップダウン リストからネットワーク マスクまたはサブネットワーク マスクを選択します。

ステップ 6 [Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルートマップを設定または追加します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv4 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** > の順に選択します。

ステップ 2 [Redistribution] をクリックします。

[Redistribution] ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Redistribution] ペインが表示されます。

ステップ 4 [Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。

ステップ 5 [Process ID] ドロップダウン リストからソース プロトコルのプロセス ID を選択します。

ステップ 6 （オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。

ステップ 7 [Route Map] ドロップダウン リストから、再配布されるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 8 [Internal]、[External]、および [NSSA External Match] チェックボックスのうち 1 つ以上をオンにして、OSPF ネットワークからルートを再配布します。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 9 [OK] をクリックします。

ステップ 10 [Apply] をクリックします。

IPv4 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** > の順に選択します。

ステップ 2 [Route Injection] をクリックします。

[Route Injection] ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Conditionally injected route] ペインが表示されます。

ステップ 4 [Inject Map] ドロップダウン リストから、ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを選択します。

ステップ 5 [Exist Map] ドロップダウン リストから、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。

ステップ 6 [Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、集約ルートの属性を継承するよう注入されたルートを設定します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv6 アドレス ファミリの設定

BGP の IPv6 設定は、BGP 設定セットアップ内の IPv6 ファミリ オプションから指定できます。IPv6 ファミリ セクションには、一般設定、集約アドレスの設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv6 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv6 ファミリの設定をカスタマイズする方法について説明します。

IPv6 ファミリの一般設定

ここでは、一般的な IPv6 の設定に必要な手順を説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [General] をクリックします。

[General IPv6 family BGP parameters] 設定ペインが表示されます。

ステップ 3 [Administrative Route Distances] 領域で、外部、内部およびローカル ディスタンスを指定します。

ステップ 4 （オプション）[Generate Default Route] チェックボックスをオンにして、デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。

ステップ 5 （オプション）[Advertise inactive routes] チェックボックスをオンにして、ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。

ステップ 6 （オプション）[Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol（IGP）への iBGP の再配布を設定します。

ステップ 7 （オプション）[Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。

ステップ 8 （オプション）[Number of paths**]** フィールドに、Border Gateway Protocol ルートの最大数を指定します。

ステップ 9 （オプション）[IBGP multipaths] チェックボックスをオンにし、[Number of paths] フィールドに、ルーティング テーブルにインストールできる並列の内部ボーダー ゲートウェイ プロトコル（iBGP）ルートの最大数を指定します。

ステップ 10 [Apply] をクリックします。

IPv6 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Aggregate Address] をクリックします。

[Aggregate Address parameters] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Aggregate Address] ペインが表示されます。

ステップ 4 [IPv6/Address Mask] フィールドで IPv6 アドレスを指定します。または、ネットワーク オブジェクトを参照して追加します。

ステップ 5 [Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。このルートにアドバタイズされるパスは、集約中のすべてのパス内に含まれるすべての要素で構成される AS_SET になります。

（注） このルートは集約されたルート変更に関する自律システム パス到着可能性情報として継続的に削除してアップデートする必要があるため、多くのパスを集約する際に aggregate-address コマンドのこの形式を使用しないでください。

ステップ 6 [Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートをすべてフィルタリングします。これにより、集約ルートが作成されるだけでなく、すべてのネイバーへの固有性の強いルートのアドバタイズメントが抑制されます。

ステップ 7 [Attribute Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルート マップを追加または設定します。これにより、集約ルートの属性を変更できます。

ステップ 8 [Advertise Map] ドロップダウン リストからルート マップを選択します。[Manage] をクリックして、ルートを追加または設定します。これにより、集約ルートのさまざまなコンポーネントの作成に使用される特定のルートが選択されます。

ステップ 9 [Suppress Map] ドロップダウン リストからルートマップを選択します。[Manage] をクリックして、ルートを追加または設定します。これにより、集約ルートが作成されますが、指定したルートのアドバタイズメントは抑制されます。

ステップ 10 [OK] をクリックします。

ステップ 11 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。この値で、ルートが集約される間隔を指定します。デフォルト値は 30 秒です。

ステップ 12 [Apply] をクリックします。

IPv6 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Neighbor] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 左側のペインで、[General] をクリックします。

ステップ 5 [IPv6 Address] フィールドに BGP ネイバーの IPv6 アドレスを入力します。この IPv6 アドレスは、BGP ネイバー テーブルに追加されます。

ステップ 6 [Remote AS] フィールドに、BGP ネイバーが属する自律システムを入力します。

ステップ 7 （オプション）[Description] フィールドに BGP ネイバーの説明を入力します。

ステップ 8 （オプション）[Shutdown neighbor administratively] チェックボックスをオンにして、ネイバーまたはピア グループを無効化します。

ステップ 9 （オプション）[Enable address family] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。

ステップ 10 左側のペインで、[Filtering] をクリックします。

ステップ 11 （オプション）[Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。

ステップ 12 （オプション）[Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。

ステップ 13 （オプション）[Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。

ステップ 14 （オプション）[Limit the number of prefixes allowed from the neighbor] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。

ステップ 15 [Maximum prefixes] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。

ステップ 16 [Threshold level] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。

ステップ 17 （オプション）[Control prefixes received from a peer] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。

- プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[Terminate peering when prefix limit is exceeded] をクリックします。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
- 最大プレフィックス数の制限値を超えたときにログ メッセージを生成するには、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。

ステップ 18 左側のペインで、[Routes] をクリックします。

ステップ 19 [Advertisement Interval] フィールドに、BGP ルーティング アップデートが送信される最小間隔（秒）を入力します。

ステップ 20 （オプション）[Generate Default route] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

ステップ 21 [Route map] ドロップダウン リストから、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 22 （オプション）条件に応じてアドバタイズされるルートを追加するには、次の手順を実行します。

a) [Conditionally Advertised Routes] セクションで [Add] をクリックします。
b) exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。
c) 次のいずれかを実行します。

- [Exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
- [Non-exist Map] をクリックしてルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

d) [OK] をクリックします。

ステップ 23 （オプション）[Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバイタイズ対象から除外します。

ステップ 24 左側のペインで、[Timers] をクリックします。

ステップ 25 （オプション）[Set timers for the BGP peer] チェックボックスをオンにし、キープアライブ頻度、保持時間、最小保持時間を設定します。

ステップ 26 [Keepalive frequency] フィールドに ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。

ステップ 27 [Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）を入力します。デフォルト値は 180 秒です。

ステップ 28 （オプション）[Min Hold time] フィールドに、キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）を入力します。

（注） ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 29 左側のペインで、[Advanced] をクリックします。

ステップ 30 （オプション）[Enable Authentication] チェックボックスをオンにして、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。

ステップ 31 [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。

ステップ 32 パスワードを [Password] フィールドに入力します。[Confirm Password] フィールドにパスワードを再入力します。

パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 33 （オプション）[Send Community Attribute to this neighbor] チェックボックスをオンにします。

ステップ 34 （オプション）[Use ASA as next hop for neighbor] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

ステップ 35 次のいずれかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
  - （オプション）[TTL ホップ（TTL hops）] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。
  - （オプション）[Disable connection verification] チェックボックスをオンにし、ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認を無効にします。

- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリング セッションを保護できるようにします。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。

ステップ 36 （オプション）[Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 37 [BGP version] ドロップダウン リストから、ASA が受け入れる BGP バージョンを選択します。

（注） バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 38 （オプション）[TCP Path MTU Discovery] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションをイネーブルにします。

ステップ 39 [TCP transport mode] ドロップダウン リストから TCP 接続モードを選択します。

ステップ 40 左側のペインで、[Migration] をクリックします。

ステップ 41 （オプション）[Customize the AS number for routes received from the neighbor] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

- [Local AS Number] フィールドにローカル自律システム番号を入力します。有効な値は、1 ～ 65535 です。
- （オプション）[Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。
- （オプション）[Replace real AS number with local AS number in routes received from neighbor] チェックボックスをオンにします。ローカル ルーティング プロセスの AS 番号は前に追加されません。
- （オプション）[Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 42 [OK] をクリックします。

ステップ 43 [Apply] をクリックします。

IPv6 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Networks] をクリックします。

[Define the networks to be advertised by the BGP routing process] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Network] ペインが表示されます。

ステップ 4 （任意）[Prefix Name] フィールドに、DHCPv6 プレフィックス委任クライアントのプレフィックスの名前を指定します（IPv6 プレフィックス委任クライアントの有効化（694 ページ）を参照）。

ステップ 5 [IPv6 Address/mask] フィールドで、BGP がアドバタイズするネットワークを指定します。

[Prefix Name] を指定した場合、サブネット プレフィックスおよびサブネット マスクを入力します。アドバタイズされたネットワークは、委任されたプレフィックスとサブネット プレフィクスで構成されます。

ステップ 6 [Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。任意で、[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv6 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Redistribution] をクリックします。

ステップ 3 [Add] をクリックします。

[Add Redistribution] ペインが表示されます。

ステップ 4 [Source Protocol] ドロップダウン リストで、BGP ドメインにルートを再配布する元となるプロトコルを選択します。

ステップ 5 [Process ID] ドロップダウン リストで、ソース プロトコルのプロセス ID を選択します。これは OSPF ソース プロトコルに対してのみ使用できます。

ステップ 6 （オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。

ステップ 7 [Route Map] ドロップダウン リストで、再配布されるネットワークをフィルタリングをするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 8 [Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 9 [OK] をクリックします。

ステップ 10 [Apply] をクリックします。

IPv6 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Route Injection] をクリックします。

ステップ 3 [Add] をクリックします。

[Add Conditionally injected route] ペインが表示されます。

ステップ 4 [Inject Map] ドロップダウン リストで、ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを選択します。

ステップ 5 [Exist Map] ドロップダウン リストで、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。

ステップ 6 [Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、集約ルートの属性を継承するよう注入されたルートを設定します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

BGP のモニターリング

次のコマンドを使用して、BGP ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな BGP ルーティング統計情報をモニターするには、次のコマンドの 1 つを入力します。

（注） BGP ログ メッセージを無効にするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングが無効になります。BGP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。デフォルトでは、ネイバー変更はログに記録されます。

- **[Monitoring] > [Routing] > [BGP Neighbors]**

  各行は 1 つの BGP ネイバーを表します。リストには、ネイバーごとに、IP アドレス、AS 番号、ルータ ID、状態（アクティブ、アイドルなど）、稼働時間、グレースフル リスタート機能、再起動時間、stalepath 時間が含まれます。

- **[Monitoring] > [Routing] > [BGP Routes]**

  各行は 1 つの BGP ルートを表します。リストには、ルートごとに、ステータス コード、IP アドレス、ネクスト ホップ アドレス、ルート メトリック、Local preference 値、重み、パスが含まれます。

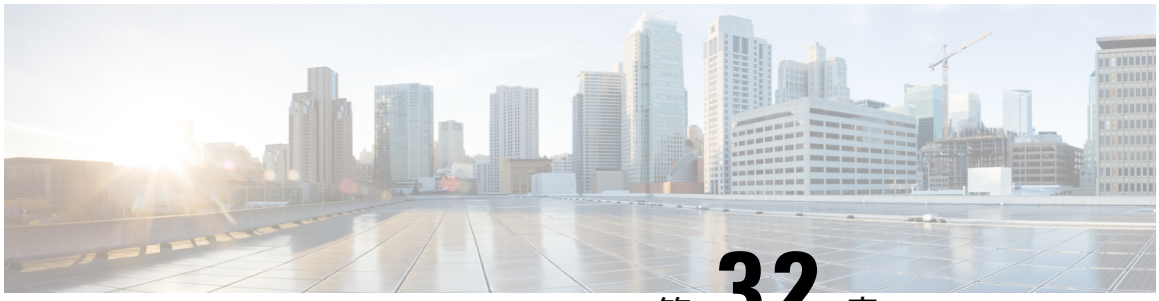
BGP の履歴

表 *39 : BGP* の各機能の履歴

機能名	プラットフォームリリース	機能情報
BGP のサポート	9.2(1)	Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [BGP Monitoring] > [Routing] > [BGP Neighbors, Monitoring] > [Routing] > [BGP Routes] 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [Static Routes> Add] > [Add Static Route Configuration] > [Device Setup] > [Routing] > [Route Maps> Add] > [Add Route Map]

機能名	プラットフォームリリース	機能情報
ASA クラスタリングに対する BGP のサポート	9.3(1)	L2 および L3 クラスタリングのサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]
ノンストップ フォワーディングに対する BGP のサポート	9.3(1)	ノンストップ フォワーディングのサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [General]、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor]、[Monitoring] > [Routing] > [BGP Neighbors]
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor] > [Add BGP Neighbor] > [Routes]
IPv6 に対する BGP のサポート	9.3(2)	IPv6 のサポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family]

機能名	プラットフォームリリース	機能情報
委任プレフィックスのIPv6ネットワーク アドバタイズメント	9.6(2)	ASAはDHCPv6プレフィックスの委任クライアントをサポートするようになりました。ASAはDHCPv6サーバーから委任プレフィックスを取得します。ASAは、これらのプレフィックスを使用して他のASAインターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上でIPv6アドレスを自動設定できるようにします。これらのプレフィックスをアドバタイズするようにBGPルータを設定できます。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** > **[Networks]**



第 32 章

OSPF

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

OSPF について

OSPF は、パスの選択にディスタンス ベクターではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく、リンクステート アドバタイズメントを伝達します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の接続先までの最短パスを構築し、計算します。OSPF エリア内の各ルータには、同一のリンクステート データベース（ルータが使用可能なインターフェイスおよび到達可能なネイバーの各一覧）が置かれています。

RIP と比べ OSPF には次の利点があります。

- OSPF では、リンクステート データベースの更新が RIP ほど頻繁に送信されません。また、ステート情報がタイムアウトすると、リンクステート データベースは徐々にではなく、すぐに更新されます。

- ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。Secure Firewall ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、接続先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。

最短パスを優先するアルゴリズムの欠点は、CPUサイクルとメモリが大量に必要になることです。

Secure Firewall ASA は、OSPF プロトコルのプロセスを 2 つ同時に異なるインターフェイス セット上で実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスが共存可能ですが、OSPF ではアドレスは重複できません）がある場合に、2 つのプロセスを実行できます。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの2つのプロセス間で再配布することもできます。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、またはOSPF対応インターフェイスに設定されているスタティック ルートおよび接続ルートから、ルートを再配布できます。

Secure Firewall ASA では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）。
- Secure Firewall ASA の代表ルータまたはバックアップ代表ルータとしての設定。Secure Firewall ASA は、ABR として設定することもできます。
- スタブ エリアと Not-So-Stubby Area。
- エリア境界ルータのタイプ 3 LSA フィルタリング。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。OSPF と他のプロトコル（RIP など）の間のルート再配布にあたっては、攻撃者によるルーティング情報の悪用の可能性があるため、できる限りすべてのルーティング プロトコルで認証を行う必要があります。

NAT を使用していて、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータ間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA により、プライベー

トエリアとパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、プライベート ネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1 つのエリアから他のエリアにフィルタリングできます。

（注） フィルタリングできるのはタイプ 3 LSA のみです。プライベート ネットワーク内の ASBR として設定されている Secure Firewall ASA は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークへのルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、Secure Firewall ASA により保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一の Secure Firewall ASA インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

Secure Firewall ASA では、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでのコンバージェンスがより迅速になります。

Fast Hello パケットに対する OSPF サポートの前提条件

OSPF がネットワークですでに設定されているか、Fast Hello パケット機能向けの OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

次に、fast hello パケットに関する OSPF のサポートと、OSPF fast hello パケットの利点について説明します。

OSPF Hello インターバルと dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、dead 間隔中に受信したすべてのネイバーのリストが含まれます。dead 間隔も設定可能なインターバル（秒単位）で送信されます。デフォルトは Hello インターバルの値の 4 倍です。Hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。dead 間隔の値も、ネットワーク内ですべて同一にする必要があります。

この2つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータが dead 間隔内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短い間隔で送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルと dead 間隔との関係についてあらかじめ理解しておく必要があります。OSPF Hello インターバルと dead 間隔 （927 ページ）を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。dead 間隔は 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる Hello インターバルは 0 に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF Fast Hello パケットの利点

OSPF Fast Hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、コンバージェンス時間が短くなります。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失がオープン システム相互接続（OSI）物理層またはデータリンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との後方互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。

- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

コンテキスト モードのガイドライン

OSPFv2 は、シングル コンテキスト モードとマルチ コンテキスト モードをサポートしています。

- デフォルトでは、共有インターフェイス間でのマルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、OSPFv2 インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、OSPFv2 プロセスの OSPFv2 プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの OSPFv2 ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 OSPFv2 がサポートされています。

OSPFv3 は、シングル モードのみをサポートしています。

キー チェーン認証のガイドライン

OSPFv2は、単一モードと複数モードの両方で、物理モードでも、仮想モードでも、キーチェーンの認証をサポートしています。ただし、複数モードでキーチェーンが設定できるのはコンテキスト モードのみです。

- 循環キーはOSPFv2プロトコルにのみ適用されます。キー チェーンを使用したOSPF エリア認証はサポートされていません。
- OSPFv2内に時間範囲がない既存のMD5認証も、新しい循環キーとともにサポートされています。
- プラットフォームは SHA1 と MD5 の暗号化アルゴリズムをサポートしていますが、認証には MD5 暗号化アルゴリズムのみが使用されます。

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

フェールオーバー ガイドライン

OSPFv2 および OSPFv3 は、ステートフル フェールオーバー をサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- Secure Firewall ASA は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。
- OSPFv3 パケットは、**capture** コマンドの IPv6 ACL を使用してフィルタリングで除外できます。

OSPFv3 Hello パケットと GRE

通常、OSPF トラフィックは GRE トンネルを通過しません。IPv6 の OSPFv3 が GRE 内でカプセル化されている場合、マルチキャスト宛先などのセキュリティチェックで IPv6 ヘッダー検証が失敗します。このパケットは、宛先が IPv6 マルチキャストであるため、暗黙的なセキュリティチェックの検証でドロップされます。

GRE トラフィックをバイパスするプレフィルタルールを定義できます。ただし、プレフィルタルールでは、内部パケットはインスペクションエンジンによって問い合わせられません。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- 個別インターフェイスモードで、OSPFv2 または OSPFv3 ネイバーとして制御ユニットおよびデータユニットが確立されていることを確認します。
- 個別インターフェイスモードでは、OSPFv2 との隣接関係は、制御ユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立できます。スタティック ネイバーの設定は、ポイントツーポイント リンクでのみサポートされます。したがって、インターフェイスで許可されるのは 1 つのネイバー ステートメントだけです。
- クラスタで制御ロールの変更が発生した場合、次の挙動が発生します。
  - スパンド インターフェイス モードでは、ルータプロセスは制御ユニットでのみアクティブになり、データユニットでは停止状態になります。コンフィギュレーションが制御ユニットと同期されているため、各クラスタユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
  - 個別インターフェイス モードでは、ルータ プロセスはすべての個別のクラスタ ユニットでアクティブになります。各クラスタ ユニットは設定されたクラスタ プールから

独自の個別のルータ ID を選択します。クラスタで制御ロールが変更されても、ルーティングトポロジは変更されません。

マルチプロトコル ラベル スイッチング（MPLS）と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート（LS）アップデート パケットに、Opaque Type-10 リンクステート アドバタイズメント（LSA）が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデート パケットを確認せずにサイレントにドロップします。ピア ルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、ASA の Opaque 機能を無効にします。

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

ルートの再配布のガイドライン

OSPFv2 または OSPFv3 の IPv4 または IPv6 プレフィックスリストを使用したルートマップの再配布はサポートされていません。再配布には OSPF の接続ルートを使用します。

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよびIETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケット サイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。

OSPFv2 の設定

ここでは、ASA で OSPFv2 プロセスを有効化する方法について説明します。

OSPFv2 をイネーブルにした後、ルート マップを定義する必要があります。詳細については、ルート マップの定義（875 ページ）を参照してください。その後、デフォルト ルートを生成します。詳細については、スタティック ルートの設定（860 ページ）を参照してください。

OSPFv2 プロセスのルート マップを定義した後で、ニーズに合わせてカスタマイズできます。ASA 上で OSPFv2 プロセスをカスタマイズする方法については、OSPFv2 のカスタマイズ（936 ページ）を参照してください。

OSPFv2 をイネーブルにするには、OSPFv2 ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

最大 2 つの OSPFv2 プロセス インスタンスをイネーブルにできます。各 OSPFv2 プロセスには、独自のエリアとネットワークが関連付けられます。

OSPFv2 をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

[OSPF Setup] ペインでは、OSPF プロセスのイネーブル化、OSPF エリアおよびネットワークの設定、および OSPF ルート集約の定義を行うことができます。

ステップ 2 ASDM で OSPF をイネーブルにするには、次の 3 つのタブを使用します。

- [Process Instances] タブでは、各コンテキストに対して最大 2 つの OSPF プロセス インスタンスを有効化できます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。[Enable Each OSPF Process] チェックボックスをオンにすると、その OSPF プロセスの固有識別子である数値識別子を入力できるようになります。このプロセス ID は内部的に使用されるものであり、他の OSPF デバイスでの OSPF プロセス ID と一致している必要はありません。有効な値の範囲は 1 ～ 65535 です。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

  [Advanced] をクリックすると、[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。ここで、各 OSPF プロセスに対して、[Router ID]、スパンド EtherChannel または個別インターフェイス クラスタリングのクラスタ IP アドレス プール、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] を設定することができます。

- [Area/Networks] タブでは、ASA 上で各 OSPF プロセスに対して指定されているエリアとネットワークが表示されます。このタブからは、エリア ID、エリア タイプ、およびそのエリアに対して設定された認証のタイプを表示できます。OSPF のエリアまたはネットワークを追加または編集する方法については、OSPFv2 エリア パラメータの設定（945 ページ）を参照してください。

- [Route Summarization] タブでは、ABR を設定できます。OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。1 つのエリア内のネットワーク番号

が連続するように割り当てられている場合は、サマリールートをアドバタイズするように ABR を設定できます。このサマリー ルートには、そのエリア内の個々のネットワークのうち、指定の範囲に当てはまるものがすべて含まれます。詳細については、OSPFv2 エリア間のルート集約の設定 （940 ページ）を参照してください。

認証用のキー チェーンの設定

デバイスのデータ セキュリティと保護を向上させるため、循環キーを有効にして IGP ピアを認証することができます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

この項では、OSPF ピア認証用のキー チェーンを作成する方法について説明します。また、キー チェーンの属性を追加または編集するステップについても説明します。キー チェーン オブジェクトを設定した後、それを使用して、インターフェイスおよび仮想リンクの OSPFv2 認証を定義することができます。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。インターフェイスの認証を定義する方法についてはOSPFv2 インターフェイス パラメータの設定 （941 ページ）を参照してください。仮想リンクについてはOSPF の仮想リンクの設定 （955 ページ）を参照してください。

キー チェーンを設定するには、次のステップを実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Key Chain]** を選択します。

ステップ 2 [Configure Key Chain] セクションで、[Add] をクリックします。

ステップ 3 キー チェーンの名前を [Add Key Chain] ダイアログボックスに入力し、[Ok] をクリックします。

作成されたキー チェーンの名前が [Configure Key Chain] グリッドのリストに表示されます。

ステップ 4 [Configure Key Chain] セクションからキー チェーン名を選択し、[Configure Key] セクションで [Add] をクリックします。既存のキーを編集するには、キー名を選択して [Edit] をクリックします。

選択したアクションに応じて、[Add Key] または [Edit Key] ダイアログボックスが表示されます。

ステップ 5 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

（注） 保存されたキー ID は編集できません。

ステップ 6 [Cryptographic Algorithm] ドロップダウンから、[MD5] を選択します。MD5 は、キー チェーンの認証に対してサポートされている唯一のアルゴリズムです。

ステップ 7 [Plain Text] または [Encrypted] オプション ボタンをクリックして暗号化タイプを選択し、[Authentication Key] フィールドにパスワードを入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 8 [Accept Lifetime] フィールドと [Send Lifetime] フィールドにライフタイムの値を入力します。

別のデバイスとのキー交換時にキーを受け入れるか、または送信するための時間間隔をデバイスに指定できます。終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、終了ライフタイムよりも前である必要があります。

ステップ 9 キー チェーンの属性を保存するには、[Ok] をクリックします。[Key Chain] ページで、[Appy] をクリックします。

次のタスク

これで、設定したキーチェーンを適用してインターフェイスおよび仮想リンクの OSPFv2 認証を定義できるようになりました。

- OSPFv2 インターフェイス パラメータの設定 （941 ページ）
- OSPF の仮想リンクの設定 （955 ページ）

OSPFv2 ルータ ID の設定

OSPF ルータ ID は、OSPF データベース内の特定のデバイスを識別するために使用されます。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできません。

ルータ ID が OSPF ルーティングプロセスで手動で設定されていない場合、ルータはアクティブインターフェイスの最も高い IP アドレスから決定されたルータ ID を自動的に設定します。

ルータ ID を設定すると、ルータに障害が発生するか、または OSPF プロセスがクリアされ、ネイバー関係が再確立されるまで、ネイバーは自動的に更新されません。

OSPF ルータ ID の手動設定

ここでは、ASA の OSPFv2 プロセスで router-id を手動で設定する方法について説明します。

手順

ステップ 1 固定ルータ ID を使用するには、**router-id** コマンドを使用します。

router-id *ip-address*

例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

ステップ 2 以前の OSPF ルータ ID の動作に戻すには、**no router-id** コマンドを使用します。

no router-id *ip-address*

例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

移行中のルータ ID の挙動

ある ASA、たとえば ASA 1 から別の ASA、たとえば ASA 2 に OSPF 設定を移行すると、次のルータ ID 選択動作が見られます。

1. すべてのインターフェイスがシャットダウン モードの場合、ASA 2 は OSPF router-id に IP アドレスを使用しません。すべてのインターフェイスが「admin down」ステートまたはシャットダウン モードの場合に考えられる router-id の設定は次のとおりです。
   - ASA 2 に以前設定された router-id がない場合は、次のメッセージが表示されます。

     ```
     %OSPF: Router process 1 is not running, please configure a router-id
     ```

     最初のインターフェイスが起動すると、ASA 2 はこのインターフェイスの IP アドレスをルータ ID として取得します。
   - ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときにすべてのインターフェイスが「admin down」ステートになっていた場合、ASA 2 は古いルータ ID を使用します。ASA 2 は、「clear ospf process」コマンドが発行されるまで、起動されたインターフェイスの IP アドレスが変更されても、古いルータ ID を使用します。

2. ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときに少なくとも 1 つのインターフェイスが「admin down」ステートまたはシャットダウン モードになっていない場合、ASA 2 は新しいルータ ID を使用します。インターフェイスが「down/down」ステートの場合でも、ASA 2 はインターフェイスの IP アドレスから新しいルータ ID を使用します。

OSPFv2 のカスタマイズ

ここでは、OSPFv2 プロセスをカスタマイズする方法について説明します。

OSPFv2 へのルートの再配布

ASA は、OSPFv2 ルーティング プロセス間のルート再配布を制御できます。

（注） 指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルト ルートを最初に生成する必要があります。スタティック ルートの設定（860 ページ）を参照し、その後にルート マップの定義（875 ページ）に従ってルート マップを定義します。

スタティック ルート、接続されているルート、RIP ルート、または OSPFv2 ルートを OSPFv2 プロセスに再配布するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Redistribution]** の順に選択します。

[Redistribution] ペインには、1 つのルーティング プロセスから OSPF ルーティング プロセスへのルートを再配布する場合のルールが表示されます。RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。スタティックまたは接続されているルートが、[Setup] > [Networks] タブで設定されたネットワークの範囲内にある場合は、そのルートを再配布する必要はありません。

ステップ 2 [Add] または [Edit] をクリックします。

または、[Redistribution] ペインでテーブル エントリ（ある場合）をダブルクリックすると、そのエントリの [Add/Edit OSPF Redistribution Entry] ダイアログボックスが開きます。

（注） 以降のステップはすべて、省略可能です。

[Add/Edit OSPF Redistribution Entry] ダイアログボックスでは、[Redistribution] テーブルに新しい再配布ルールを追加することや、既存の再配布ルールを編集することができます。既存の再配布ルールを編集するとき、一部の再配布ルール情報は変更できません。

ステップ 3 ルート再配布エントリに関連付ける OSPF プロセスを選択します。既存の再配布ルールを編集している場合、この設定は変更できません。

ステップ 4 どのソース プロトコルからルートを再配布するかを選択します。次のいずれかのオプションを選択できます。

- [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
- [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。
- [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。リストから OSPF プロセス ID を選択してください。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ステップ 5 に進みます。
- [RIP]：RIP ルーティング プロセスからルートを再配布します。
- [BGP]：BGP ルーティング プロセスからルートを再配布します。
- [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。

ステップ 5 OSPF をソース プロトコルとして選択した場合は、選択した OSPF ルーティング プロセスに別の OSPF ルーティング プロセスからのルートを再配布するのに使用される条件を選択します。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。

- [Internal]：ルートは特定の AS の内部です。
- [External 1]：自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
- [External 2]：自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
- [NSSA External 1]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
- [NSSA External 2]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

ステップ 6 [Metric Value] フィールドに、再配布されるルートのメトリック値を入力します。有効値の範囲は 1 ～ 16777214 です。

同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは1つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

ステップ 7 [Metric Type] で、次のオプションのいずれかを選択します。

- メトリックがタイプ 1 外部ルートの場合は、[1] を選択します。
- メトリックがタイプ 2 外部ルートの場合は、[2] を選択します。

ステップ 8 タグ値を [Tag Value] フィールドに入力します。

タグ値は 32 ビット 10 進数値です。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。有効値の範囲は、0～4294967295 です。

ステップ 9 [Use Subnets] チェックボックスをオンにすると、サブネット化ルートの再配布がイネーブルになります。サブネットされていないルートだけを再配布するには、このチェックボックスをオフにします。

ステップ 10 再配布エントリに適用するルート マップの名前を [Route Map] ドロップダウン リストで選択します。

ステップ 11 ルート マップを追加または設定するには、[Manage] をクリックします。

[Configure Route Map] ダイアログボックスが表示されます。

ステップ 12 [Add] または [Edit] をクリックしてから、指定したルーティング プロトコルからのルートのうち、どれをターゲットのルーティング プロセスに再配布するかを定義します。詳細については、ルート マップの定義 （875 ページ）を参照してください。

ステップ 13 [OK] をクリックします。

OSPFv2 にルートを再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのルートをアドバタイズするように ASA を設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。

指定した IP アドレス マスク ペアと一致するルートは抑制できます。ルート マップで再配布を制御するために、タグ値を一致値として使用できます。

ルート サマリー アドレスの追加

[Summary Address] ペインには、各 OSPF ルーティング プロセスに設定されたサマリー アドレスに関する情報が表示されます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。集約ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF の集約ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

（注） OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

ネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

手順

ステップ 1 メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Summary Address]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add OSPF Summary Address Entry] ダイアログボックスが表示されます。[Summary Address] テーブルの既存のエントリに新しいエントリを追加できます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3 [OSPF Process] ドロップダウン リストから、サマリー アドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4 [IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 5 サマリー アドレスのネットワーク マスクを [Netmask] ドロップダウン リストから選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 6 [Advertise] チェックボックスをオンにして、サマリー ルートをアドバタイズします。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

[Tag value] に表示される値は、各外部ルートに付加される 32 ビットの 10 進数値です。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。

ステップ 7 [OK] をクリックします。

OSPF サマリー アドレスの追加または編集

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Route Summarization] タブをクリックします。

[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。

[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3 [OSPF Process] ドロップダウン リストから、サマリー アドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4 [IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 5 サマリーアドレスのネットワーク マスクを [Netmask] ドロップダウン リストから入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 6 [Advertise] チェックボックスをオンにして、サマリールートをアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

OSPFv2 エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべて含むサマリールートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Route Summarization] タブをクリックします。

[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。

[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3 [Area ID] フィールドに OSPF エリア ID を入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4 [IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

OSPFv2 インターフェイス パラメータの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello インターバル、デッドインターバル、認証キーの各インターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ASDM では、[Interface] ペインでインターフェイス固有の OSPF ルーティング プロパティ（たとえば OSPF メッセージ認証やプロパティ）を設定できます。OSPF のインターフェイスを設定するためのタブは次の 2 つです。

- [Authentication] タブには、ASA インターフェイスの OSPF 認証情報が表示されます。
- [Properties] タブには、各インターフェイスに定義された OSPF プロパティがテーブル形式で表示されます。

OSPFv2 インターフェイス パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 [Authentication] タブをクリックすると、ASA のインターフェイスの認証情報が表示されます。このテーブルの行をダブルクリックすると、選択したインターフェイスの [Edit OSPF Authentication Interface] ダイアログボックスが開きます。

ステップ 2 [Edit] をクリックします。

[Edit OSPF Authentication Interface] ダイアログボックスが表示されます。[Edit OSPF Interface Authentication] ダイアログボックスでは、選択したインターフェイスの OSPF 認証タイプおよびパラメータを設定できます。

ステップ 3 関連するオプション ボタンをクリックして、認証タイプを選択します。

- [No authentication]：OSPF 認証が無効になります。
- [Area authentication, if defined]（デフォルト）：そのエリアに指定された認証タイプを使用します。エリア認証の設定については、OSPFv2 エリア パラメータの設定 （945 ページ）を参照してください。エリア認証はデフォルトでディセーブルになっています。したがっ

て、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。

- [Password authentication]：クリア テキストによるパスワード認証が使用されます（セキュリティの懸念がある場合は推奨しません）。
- [MD5 authentication]：MD5 認証を使用します。
- [Key chain authentication]：キー チェーン認証を使用します（推奨）。認証用のキー チェーンの設定については認証用のキー チェーンの設定 （933 ページ）を参照してください。

ステップ 4 パスワード認証を選択した場合は、[Authentication Password] 領域で次のようにパスワードを入力します。

a) [Enter Password] フィールドに、最大 8 文字のテキスト文字列を入力します。
b) [Re-enter Password] フィールドに、パスワードを再入力します。

ステップ 5 キー チェーン認証を選択した場合は、[Enter Key chain name] フィールドにキー チェーン名を入力します。

ステップ 6 MD5 の ID とキーの設定を [ID] 領域で選択します。この領域には、MD5 認証がイネーブルのときの MD5 キーとパラメータの入力に関する設定があります。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。

a) [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。選択したインターフェイスのキー ID が表示されます。
b) [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキーが表示されます。
c) [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Properties] タブをクリックします。

ステップ 9 編集するインターフェイスを選択します。テーブルの行をダブルクリックすると、選択したインターフェイスの [Properties] タブ ダイアログボックスが開きます。

ステップ 10 [Edit] をクリックします。

[Edit OSPF Interface Properties] ダイアログボックスが表示されます。[Interface] フィールドに、OSPF プロパティ設定の対象であるインターフェイスの名前が表示されます。このフィールドは編集できません。

ステップ 11 このインターフェイスがブロードキャスト インターフェイスかどうかに応じて、[Broadcast] チェックボックスをオンまたはオフにします。

デフォルトでは、イーサネットインターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャストインターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。

インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- ネイバーは手動で設定する必要があります。詳細については、「スタティック OSPFv2 ネイバーの定義 （950 ページ）」を参照してください。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。詳細については、「スタティック ルートの設定 （860 ページ）」を参照してください。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリーム ルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
- OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後で暗号マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。

ステップ 12 次のオプションを設定します。

- [Cost] フィールドに、このインターフェイスを通してパケット 1 個を送信するコストを決定する値を入力します。デフォルト値は 10 です。
- [Priority] フィールドに、OSPF ルータ優先順位の値を入力します。

  2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

  この設定の有効値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイントの非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。

  マルチコンテキスト モードでは、共有インターフェイスに 0 を指定して、デバイスが指定ルータにならないようにします。OSPFv2 インスタンスは、共有インターフェイス間で相互に隣接関係を形成できません。
- [MTU Ignore] チェックボックスをオンまたはオフにします。

  OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケットに受信した MTU が着信インターフェイスに設定されている IP MTU より高い場合、OSPF の隣接性は確立されません。
- [Database filter] チェックボックスをオンまたはオフにします。

  この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全

メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながることがあります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。

ステップ 13 （任意）[Advanced] をクリックして [Edit OSPF Advanced Interface Properties] ダイアログボックスを開きます。ここでは、OSPF hello 間隔、再送信間隔、送信遅延、およびデッド間隔の値を変更できます。

通常は、ネットワーク上で OSPF の問題が発生した場合にだけ、これらの値をデフォルトから変更する必要があります。

ステップ 14 [Intervals] セクションには、次の値を入力します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 15 [Detecting Lost Neighbors] セクションで、次のいずれかを実行します。

- [Configure interval within which hello packets are not received before the router declares the neighbor to be down] をクリックします。[Dead Interval] フィールドで、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効な値の範囲は、1 ～ 8192 秒です。この設定のデフォルト値は、[Hello Interval] フィールドで設定された時間の長さの 4 倍です。
- [Send fast hello packets within 1 seconds dead interval] をクリックします。[Hello multiplier] フィールドで、1 秒ごとに送信される hello パケットの数を指定します。有効な値は、3 ～ 20 です。

OSPFv2 エリア パラメータの設定

複数の OSPF エリア パラメータを設定できます。これらのエリア パラメータ（後述のタスク リストに表示）には、認証の設定、スタブ エリアの定義、デフォルト サマリー ルートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワード ベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Area/Networks] タブをクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 3 次に示す [Area Type] のオプションのいずれかを選択します。

- [Normal] を選択すると、このエリアは標準の OSPF エリアとなります。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。
- [Stub] を選択すると、このエリアはスタブエリアとなります。スタブエリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブエリアにフラッドされないようにします。スタブエリアを作成するときに、サマリー LSA（タイプ 3 および 4）がそのエリアにフラッディングされないように設定するには、[Summary] チェックボックスをオフにします。
- [Summary] チェックボックスは、エリアをスタブエリアとして定義するときに、LSA がこのエリアに送信されないよう設定する場合にオフにします。デフォルトでは、スタブエリアの場合にこのチェックボックスはオンになります。
- [NSSA] を選択すると、このエリアは Not-So-Stubby Area となります。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 4 [IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルトエリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を使用します。**0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 5 [Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 6 [OSPF Authentication type] で、次のオプションから選択します。

- [None] を選択すると、OSPF エリア認証が無効になります。これがデフォルト設定です。
- [Password] を選択すると、クリアテキスト パスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
- [MD5] を選択すると、MD5 認証ができるようになります。

ステップ 7 [Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。

有効な値の範囲は 0 ～ 65535 です。デフォルト値は 1 です。

ステップ 8 [OK] をクリックします。

OSPFv2 フィルタ ルールの設定

OSPF アップデートで受信または送信されるルートまたはネットワークをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Filter Rules]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [OSPF AS] で OSPF プロセス ID を選択します。

ステップ 4 [Access List] ドロップダウン リストから標準アクセス リストを選択します。[Manage] をクリックして、新しい ACL を追加します。

ステップ 5 [Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。

ステップ 6 着信フィルタには、オプションでインターフェイスを指定して、そのインターフェイスが受信するアップデートにフィルタを制限することができます。

ステップ 7 発信フィルタには、オプションで、配信されるルートのタイプを指定できます。

a) [Protocol] ドロップダウン リストからオプションを選択します。

[BGP]、[EIGRP]、[OSPF]、または [RIP] などのルーティング プロトコルを選択できます。

接続ルートから学習されたピアおよびネットワークをフィルタリングするには、[Connected] を選択します。

スタティック ルートから学習されたピアおよびネットワークをフィルタリングするには、[Static] を選択します。

b) [BGP]、[EIGRP]、または [OSPF] を選択した場合は、そのプロトコルのプロセス ID も [Process ID] で選択します。

ステップ 8 [OK] をクリックします。

ステップ 9 [Apply] をクリックします。

OSPFv2 NSSA の設定

NSSA の OSPFv2 への実装は、OSPFv2 のスタブ エリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッディングすることはありませんが、自律システムの外部ルートをある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティング ドメイン全体にフラッディングされます。変換中は集約とフィルタリングがサポートされます。

OSPFv2 を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPFv2 スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

この機能を使用する前に、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために使用可能なタイプ 7 のデフォルト ルートを設定できます。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ 7 のデフォルトがルータによって生成されます。
- 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。そうでない場合、ルータは互いに通信できません。

手順

ステップ 1 メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Area/Networks] タブをクリックします。

ステップ 3 [Add] をクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 4 [Area Type] 領域の [NSSA] オプション ボタンをクリックします。

エリアを Not-So-Stubby Area にするには、このオプションを選択します。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにするこ

とでサマリーLSAがそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 5 [IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルトエリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を使用します。**0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 6 [Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 7 [Authentication] 領域の [None] オプション ボタンをクリックすると、OSPF エリア認証がディセーブルになります。

ステップ 8 [Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。

有効な値の範囲は 0 ～ 65535 です。デフォルト値は 1 です。

ステップ 9 [OK] をクリックします。

クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）

個別インターフェイス クラスタリングを使用する場合は、ルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てることができます。

OSPFv2 の個別インターフェイスのルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てるには、次の手順を実行します。

手順

ステップ 1 メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Cluster Pool] オプション ボタンをクリックします。クラスタリングを使用している場合は、ルータ ID の IP アドレス プールを指定する必要はありません（つまりフィールドは空）。IP アドレス プールを入力しない場合、ASA は自動的に生成されたルータ ID を使用します。

ステップ 5 IP アドレス プールの名前を入力するか、省略記号をクリックして [Select IP Address Pool] ダイアログボックスを表示します。

ステップ 6 既存の IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加します。[Add] をクリックして、新しい IP アドレス プールを作成することもできます。

[Add IPv4 Pool] ダイアログボックスが表示されます。

ステップ 7 [Name] フィールドに新しい IP アドレス プール名を入力します。

ステップ 8 開始 IP アドレスを入力するか、または省略記号をクリックして、[Browse Starting IP Address] ダイアログボックスを表示します。

ステップ 9 エントリをダブルクリックして、[Starting IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 10 最後の IP アドレスを入力するか、または省略記号をクリックして、[Browse Ending IP Address] ダイアログボックスを表示します。

ステップ 11 エントリをダブルクリックして、[Ending IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 12 ドロップダウン リストからサブネット マスクを選択し、続いて [OK] をクリックします。

[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。

ステップ 13 新しい IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加し、続いて [OK] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスの [Cluster Pool] フィールドに、新しい IP アドレス プール名が表示されます。

ステップ 14 [OK] をクリックします。

ステップ 15 新しく追加された IP アドレス プール設定を変更する場合は、[Edit] をクリックします。

[Edit IPv4 Pool] ダイアログボックスが表示されます。

ステップ 16 ステップ 4 ～ 14 を繰り返します。

（注） すでに割り当てられ、1 つ以上の接続プロファイルによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

ステップ 17 [OK] をクリックします。

ステップ 18 OSPFv3 の個別インターフェイス クラスタリングのルータ ID のクラスタ プールに IPv4 アドレス範囲を割り当てるには、次の手順を実行します。

a) メインの ASDM ホーム ページで、**[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]** の順に選択します。

b) [Process Instances] タブをクリックします。

c) 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

d) [Router ID] ドロップダウン リストから [Cluster Pool] オプションを選択します。ルータ ID の IP アドレス プールを指定する必要がない場合は、[Automatic] オプションを選択します。IP アドレス プールを設定しない場合、ASA は自動的に生成されたルータ ID を使用します。

e) IP アドレス プール名を入力します。省略記号をクリックして、[IP Address Pool] ダイアログボックスを表示することもできます。

f) 既存の IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加します。[Add] をクリックして、新しい IP アドレス プールを作成することもできます。

[Add IPv4 Pool] ダイアログボックスが表示されます。

g) [Name] フィールドに新しい IP アドレス プール名を入力します。
h) 開始 IP アドレスを入力するか、または省略記号をクリックして、[Browse Starting IP Address] ダイアログボックスを表示します。
i) エントリをダブルクリックして、[Starting IP Address] フィールドに追加し、続いて [OK] をクリックします。
j) 最後の IP アドレスを入力するか、または省略記号をクリックして、[Browse Ending IP Address] ダイアログボックスを表示します。
k) エントリをダブルクリックして、[Ending IP Address] フィールドに追加し、続いて [OK] をクリックします。
l) ドロップダウン リストからサブネット マスクを選択し、続いて [OK] をクリックします。

[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。

m) 新しい IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加し、続いて [OK] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスの [Cluster Pool] フィールドに、新しい IP アドレス プール名が表示されます。

n) [OK] をクリックします。
o) 新しく追加されたクラスタ プールの設定を変更する場合は、[Edit] をクリックします。

[Edit IPv4 Pool] ダイアログボックスが表示されます。

p) ステップ 4 ～ 14 を繰り返します。

（注） すでに割り当てられ、別の OSPFv3 プロセスによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

q) [OK] をクリックします。

スタティック OSPFv2 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv2 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定（860 ページ）を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Static Neighbor]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add/Edit OSPF Neighbor Entry] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャストインターフェイスごとに、スタティック ネイバーを1つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPF プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3 [OSPF Process] ドロップダウン リストで、スタティック ネイバーに関連付ける OSPF プロセスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4 [Neighbor] フィールドに、スタティック ネイバーの IP アドレスを入力します。

ステップ 5 [Interface] フィールドで、スタティック ネイバーに関連付けるインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 6 [OK] をクリックします。

ルート計算タイマーの設定

OSPFv2 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Timers] 領域では、LSA ペーシングおよび SPF 計算のタイマーの設定に使用される値を変更できます。[Timers] 領域で、次の値を入力します。

- [Initial SPF Delay] は、OSPF がトポロジ変更を受信してから SPF 計算が開始されるまでの時間（ミリ秒）を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。

- [Minimum SPF Hold Time] は、連続する SPF 計算間の保持時間をミリ秒で指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
- [Maximum SPF Wait Time] は、2 回の連続する SPF 計算間の最大待機時間を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。

ステップ 5 [OK] をクリックします。

ネイバーの起動と停止のロギング

デフォルトでは、OSPFv2 ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Adjacency Changes] 領域には、syslog メッセージ送信を引き起こす隣接関係変更を定義するための設定があります。[Adjacency Changes] 領域で、次の値を入力します。

- [Log Adjacency Changes] チェックボックスをオンにすると、OSPFv2 ネイバーがアップ状態またはダウン状態になるたびに ASA によって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
- [Log Adjacency Changes Detail] チェックボックスをオンにすると、ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも ASA によって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

ステップ 5 [OK] をクリックします。

（注） ネイバーのアップまたはダウンのメッセージが送信されるには、ロギングがイネーブルになっている必要があります。

認証用のキー チェーンの設定

デバイスのデータ セキュリティと保護を向上させるため、循環キーを有効にして IGP ピアを認証することができます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

この項では、OSPF ピア認証用のキー チェーンを作成する方法について説明します。また、キー チェーンの属性を追加または編集するステップについても説明します。キー チェーン オブジェクトを設定した後、それを使用して、インターフェイスおよび仮想リンクの OSPFv2 認証を定義することができます。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。インターフェイスの認証を定義する方法についてはOSPFv2 インターフェイス パラメータの設定 （941 ページ）を参照してください。仮想リンクについてはOSPF の仮想リンクの設定 （955 ページ）を参照してください。

キー チェーンを設定するには、次のステップを実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Key Chain]** を選択します。

ステップ 2 [Configure Key Chain] セクションで、[Add] をクリックします。

ステップ 3 キー チェーンの名前を [Add Key Chain] ダイアログボックスに入力し、[Ok] をクリックします。

作成されたキー チェーンの名前が [Configure Key Chain] グリッドのリストに表示されます。

ステップ 4 [Configure Key Chain] セクションからキー チェーン名を選択し、[Configure Key] セクションで [Add] をクリックします。既存のキーを編集するには、キー名を選択して [Edit] をクリックします。

選択したアクションに応じて、[Add Key] または [Edit Key] ダイアログボックスが表示されます。

ステップ 5 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

（注） 保存されたキー ID は編集できません。

ステップ 6 [Cryptographic Algorithm] ドロップダウンから、[MD5] を選択します。MD5 は、キー チェーンの認証に対してサポートされている唯一のアルゴリズムです。

ステップ 7 [Plain Text] または [Encrypted] オプション ボタンをクリックして暗号化タイプを選択し、[Authentication Key] フィールドにパスワードを入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 8 [Accept Lifetime] フィールドと [Send Lifetime] フィールドにライフタイムの値を入力します。

別のデバイスとのキー交換時にキーを受け入れるか、または送信するための時間間隔をデバイスに指定できます。終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、終了ライフタイムよりも前である必要があります。

ステップ 9 キー チェーンの属性を保存するには、[Ok] をクリックします。[Key Chain] ページで、[Appy] をクリックします。

次のタスク

これで、設定したキーチェーンを適用してインターフェイスおよび仮想リンクの OSPFv2 認証を定義できるようになりました。

- OSPFv2 インターフェイス パラメータの設定 （941 ページ）
- OSPF の仮想リンクの設定 （955 ページ）

OSPF でのフィルタリングの設定

[Filtering] ペインには、各 OSPF プロセスに対して設定済みの ABR タイプ 3 LSA フィルタが表示されます。

ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリアフィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

（注） フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

OSPF でのフィルタリングを設定するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Filtering]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add or OSPF Filtering Entry] ダイアログボックスでは、新しいフィルタを [Filter] テーブルに追加することや、既存のフィルタを修正することができます。既存のフィルタを編集するとき、一部のフィルタリング情報は変更できません。

ステップ 3 フィルタ エントリに関連付ける OSPF プロセスを [OSPF Process] ドロップダウン リストで選択します。

ステップ 4 フィルタ エントリに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 5 プレフィックス リストを [Prefix List] ドロップダウン リストで選択します。

ステップ 6 フィルタリングするトラフィックの方向を [Traffic Direction] ドロップダウン リストで選択します。

OSPF エリアへの LSA をフィルタリングするには [着信（Inbound）] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信（Outbound）] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 7 [Manage] をクリックすると [Configure Prefix Lists] ダイアログボックスが表示され、ここでプレフィックス リストとプレフィックス ルールを追加、編集、または削除できます。詳細については、プレフィックス リストの設定（881 ページ）およびルート アクションのメトリック値の設定（881 ページ）を参照してください。

ステップ 8 [OK] をクリックします。

OSPF の仮想リンクの設定

OSPF ネットワークにエリアを追加し、そのエリアをバックボーン エリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デバイスを接続します。OSPF デバイスのいずれかは、バックボーン エリアに接続されている必要があります。

新しい仮想リンクを定義する、または既存の仮想リンクのプロパティを変更するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Virtual Link]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add OSPF Virtual Link] または [Edit OSPF Virtual Link] ダイアログボックスが表示され、ここで新しい仮想リンクを定義することや、既存の仮想リンクのプロパティを変更することができます。

ステップ 3 仮想リンクに関連付ける OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 4 仮想リンクに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。

ネイバー OSPF デバイスによって共有されるエリアを選択します。[NSSA] エリアまたは [Stub] エリアは選択できません。既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 5 [Peer Router ID] フィールドに、仮想リンク ネイバーのルータ ID を入力します。

既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 6 仮想リンクの詳細プロパティを編集するには、[Advanced] をクリックします。

[Advanced OSPF Virtual Link Properties] ダイアログボックスが表示されます。このエリアにある仮想リンクに対して、OSPF プロパティを設定できます。プロパティには、認証およびパケット間隔設定が含まれます。

ステップ 7 [Authentication] 領域で、[Authentication type] を選択します。次のオプション ボタンのいずれかをクリックします。

- [No authentication]：OSPF 認証が無効になります。
- [Password authentication]：クリア テキストによるパスワード認証が使用されます（セキュリティの懸念がある場合は推奨しません）。
- [MD5 authentication]：MD5 認証を使用します。
- [Key chain authentication]：キー チェーン認証を使用します（推奨）。認証用のキー チェーンの設定については認証用のキー チェーンの設定 （933 ページ）を参照してください。

ステップ 8 [Authentication Password] 領域で、パスワードを入力し、もう一度入力します（パスワード認証がイネーブルのとき）。パスワードは、最大 8 文字のテキスト文字列であることが必要です。

ステップ 9 [MD5 IDs and Key] 領域で、MD5 のキーとパラメータを入力します（MD5 認証がイネーブルのとき）。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。次の設定を指定します。

a) [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。選択したインターフェイスのキー ID が表示されます。

b) [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキー ID が表示されます。
c) [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 10 [Interval] 領域で、パケットの間隔を指定します。次のオプションから選択します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1～65535 秒です。デフォルト値は 1 秒です。
- [Dead Interval] には、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効値の範囲は 1 ～ 65535 です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

ステップ 11 [OK] をクリックします。

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPFv3 の有効化

OSPFv3 をイネーブルにするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスをイネーブルにする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブで、[Enable OSPFv3 Process] チェックボックスをオンにします。最大 2 つの OSPF プロセス インスタンスをイネーブルにできます。シングル コンテキスト モードだけがサポートされます。

ステップ 3 [Process ID] フィールドにプロセス ID を入力します。ID は、任意の正の整数が可能です。

ステップ 4 [Apply] をクリックして変更内容を保存します。

ステップ 5 以降の手順については、OSPFv3 エリア パラメータの設定（960 ページ）を参照してください。

OSPFv3 インターフェイス パラメータの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Interfaces]** の順に選択します。

ステップ 2 [Authentication] タブをクリックします。

ステップ 3 インターフェイスの認証パラメータを指定するには、インターフェイスを選択し、[Edit] をクリックします。

[Edit OSPFv3 Interface Authentication] ダイアログボックスが表示されます。

ステップ 4 [Authentication Type] ドロップダウン リストから認証タイプを選択します。使用可能なオプションは、[エリア（Area）]、[インターフェイス（Interface）]、[なし（None）] です。[なし（None）] オプションを選択すると、認証が行われません。

ステップ 5 [Authentication Algorithm] ドロップダウン リストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。

ステップ 6 [Authentication Key] フィールドに認証キーを入力します。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。

ステップ 7 [Encryption Algorithm] ドロップダウン リストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエントリは暗号化されません。

ステップ 8 [Encryption Key] フィールドに暗号キーを入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Properties] タブをクリックします。

ステップ 11 プロパティを変更するインターフェイスを選択し、[Edit] をクリックします。

[Edit OSPFv3 Interface Properties] ダイアログボックスが表示されます。

ステップ 12 [Enable OSPFv3 on this interface] チェックボックスをオンにします。

ステップ 13 ドロップダウン リストからプロセス ID を選択します。

ステップ 14 ドロップダウン リストから領域 ID を選択します。

ステップ 15 （オプション）インターフェイスに割り当てる領域インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 16 ドロップダウン リストからネットワーク タイプを選択します。サポートされるオプションは、[Default]、[Broadcast]、[Point-to-Point] です。

ステップ 17 [Cost] フィールドにインターフェイスでのパケット送信コストを入力します。

ステップ 18 [Priority] フィールドにルータ プライオリティを入力します。これは、ネットワークにおける指定ルータの特定に役立ちます。有効値の範囲は 0 ～ 255 です。

ステップ 19 [Disable MTU mismatch detection] チェックボックスをオンにして、DBD パケットが受信された場合の OSPF MTU 不一致検出をディセーブルにします。OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。

ステップ 20 [Filter outgoing link state advertisements] チェックボックスをオンにして、OSPFv3 インターフェイスに対する出力 LSA をフィルタします。デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。

ステップ 21 [Timers] 領域の [Dead Interval] フィールドに hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。

ステップ 22 [Hello Interval] フィールドに、hello パケットがインターフェイスに送信される間隔を秒単位で入力します。この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1～65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。

ステップ 23 [Retransmit Interval] フィールドに、インターフェイスに属する隣接ルータの LSA 再送信間隔を秒単位で入力します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

ステップ 24 [Transmit Delay] フィールドに、インターフェイスでリンク ステート アップデート パケットを送信する予想時間を秒単位で入力します。有効な値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

ステップ 25 [OK] をクリックします。

ステップ 26 [Apply] をクリックして変更内容を保存します。

OSPFv3 エリア パラメータの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Areas] タブをクリックします。

ステップ 3 新しいエリアを追加するには、[Add] をクリックします。既存のエリアを変更するには、[Edit] をクリックします。選択したエリアを削除するには、[Delete] をクリックします。

[Add OSPFv3 Area] ダイアログボックスまたは [Edit OSPFv3 Area] ダイアログボックスが表示されます。

ステップ 4 [OSPFv3 Process ID] ドロップダウン リストから、プロセス ID を選択します。

ステップ 5 ルートが集約されるエリアを指定するエリア ID を [Area ID] フィールドに入力します。

ステップ 6 [Area Type] ドロップダウン リストからエリア タイプを選択します。使用可能なオプションは、[Normal]、[NSSA]、[Stub] です。

ステップ 7 エリアにサマリー LSA の送信を許可する場合は、[Allow sending of summary LSAs into the area] チェックボックスをオンにします。

ステップ 8 標準および not so stubby エリアへのインポート ルートの再配布を許可するには、[Redistribution imports routes to normal and NSSA areas] チェックボックスをオンにします。

ステップ 9 OSPFv3 ルーティング ドメインにデフォルト外部ルートを生成するには、[Default information originate] チェックボックスをチェックします。

ステップ 10 デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。

ステップ 11 [Metric Type] ドロップダウン リストからメトリック タイプを選択します。メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

ステップ 12 [Default Cost] フィールドにコストを入力します。

ステップ 13 [OK] をクリックします。

ステップ 14 [Route Summarization] タブをクリックします。

ステップ 15 ルートを統合および集約するための新しい範囲を指定するには、[Add] をクリックします。ルートを統合および集約する既存の範囲を変更するには、[Edit] をクリックします。

[Add Route Summarization] ダイアログボックスまたは [Edit Route Summarization] ダイアログボックスが表示されます。

ステップ 16 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 17 [Area ID] ドロップダウン リストからエリア ID を選択します。

ステップ 18 [IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 19 （オプション）このサマリールートのメトリックまたはコストを入力します。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ～ 16777215 です。

ステップ 20 [Advertised] チェックボックスをオンにして、アドレス範囲の状態をアドバタイズされた設定し、タイプ 3 サマリー LSA を生成します。

ステップ 21 [OK] をクリックします。

ステップ 22 以降の手順については、仮想リンク ネイバーの設定 （961 ページ）を参照してください。

仮想リンク ネイバーの設定

仮想リンク ネイバーを設定するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Virtual Link]** の順に選択します。

ステップ 2 新しい仮想リンク ネイバーを追加するには、[Add] をクリックします。既存の仮想リンク ネイバーを変更するには、[Edit] をクリックします。指定された仮想リンク ネイバーを削除するには、[Delete] をクリックします。

[Add Virtual Link] ダイアログボックスまたは [Edit Virtual Link] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [Area ID] ドロップダウン リストからエリア ID を選択します。

ステップ 5 [Peer Router ID] フィールドにピア ルータ ID（IP アドレス）を入力します。

ステップ 6 （オプション）[TTL Security] フィールドに仮想リンクの存続可能時間 (TTL) のセキュリティのホップ数を入力します。ホップ数の値は 1 ～ 254 の範囲で指定します。

ステップ 7 [Timers] 領域の [Dead Interval] フィールドに、hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。Dead 間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。

ステップ 8 [Hello Interval] フィールドに、インターフェイスで送信される hello パケットの間隔を秒単位で入力します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。デフォルトは 10 です。

ステップ 9 [Retransmit Interval] フィールドに、インターフェイスに属している隣接ルータの LSA 再送信間隔を秒単位で入力します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 8192 の範囲で指定できます。デフォルトは 5 分です。

ステップ 10 [Transmit Delay] フィールドに、インターフェイスのリンク ステート アップデート パケットの送信に必要な予想時間を秒単位で入力します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

ステップ 11 [Authentication] 領域の [Enable Authentication] チェックボックスをオンにして、認証をイネーブルにします。

ステップ 12 [Security Policy Index] フィールドに、セキュリティ ポリシー インデックスを入力します。値の範囲は、256～4294967295 の数字です。

ステップ 13 [Authentication Algorithm] ドロップダウン リストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。

ステップ 14 [Authentication Key] フィールドに認証キーを入力します。キーは 32 文字の 16 進数文字で構成される必要があります。

ステップ 15 [Encryption Algorithm] ドロップダウン リストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエントリは暗号化されません。

ステップ 16 [Encryption Key] フィールドに暗号キーを入力します。

ステップ 17 [OK] をクリックします。

ステップ 18 [Apply] をクリックして変更内容を保存します。

OSPFv3 受動インターフェイスの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Passive Interfaces] 領域では、インターフェイスのパッシブ OSPFv3 ルーティングをイネーブルにすることができます。パッシブ ルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信をディセーブルにします。[Passive Interfaces] 領域で、次の設定を選択します。

- [Global passive] チェックボックスをオンにして、テーブルに表示されているインターフェイスすべてをパッシブにします。個々のインターフェイスをオフにすると、そのインターフェイスは非パッシブになります。

- [Global passive] チェックボックスをオフにすると、すべてのインターフェイスが非パッシブになります。個々のインターフェイスをオンにすると、そのインターフェイスはパッシブになります。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv3 アドミニストレーティブ ディスタンスの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Administrative Route Distances] 領域では、管理ルート間隔の設定に使用された設定を変更することができます。管理ルート間隔は 10～254 の整数です。[Administrative Route Distances] 領域で、次の値を入力します。

- [Inter Area] には、IPv6 ルートの OSPV のエリア間ルートを指定します。
- [Intra Area] には、IPv6 ルートの OSPF のエリア内ルートを指定します。
- [External] には、IPv6 ルートの OSPF の外部タイプ 5 および外部タイプ 7 のルートを指定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックして変更内容を保存します。

OSPFv3 タイマーの設定

OSPFv3 の LSA 到着タイマー、LSA ペーシング タイマー、およびスロットリング タイマーを設定できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Timers] 領域では、LSA 到着、LSA ペーシング、LSA 再送信、LSA スロットル、SPF スロットル時間の設定に使用された設定を変更することができます。[Timers] 領域で、次の値を入力します。

- [LSA Arrival] には、ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ～ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [LSA Flood Pacing] には、フラッディング キュー内の LSA のアップデートのペースをミリ秒単位で指定します。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
- [LSA Group Pacing] には、LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [LSA Retransmission Pacing] には、再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は、66 ミリ秒です。
- [LSA Throttle Initial] には、LSA の最初のオカレンスを生成する遅延をミリ秒単位で指定します。デフォルト値は 0 ミリ秒です。
- [LSA Throttle Min Hold] には、同じ LSA を発信する最短遅延時間をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [LSA Throttle Max Wait] には、同じ LSA を発信する最長遅延時間をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。

  （注） LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

- [SPF Throttle Initial] には、SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [SPF Throttle Min Hold] には、1 番目と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は 10000 ミリ秒です。
- [SPF Throttle Max Wait] には、SPF 計算の最長待機時間をミリ秒単位で指定する。デフォルト値は、10000 ミリ秒です。

  （注） SPF スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

スタティック OSPFv3 ネイバーの定義

ポイントツーポイントの非ブロードキャストネットワークを介してOSPFv3ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv3 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定（860 ページ）を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Static Neighbor]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add Static Neighbor] または [Edit Static Neighbor] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを 1 つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPFv3 プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3 [Interface] ドロップダウン リストから、スタティック ネイバーに関連付けられたインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4 [Link-local address] フィールドに、スタティック ネイバーの IPv6 アドレスを入力します。

ステップ 5 （オプション）[Priority] フィールドに、プライオリティ レベルを入力します。

ステップ 6 （オプション）[Poll Interval] フィールドに、ポーリング間隔を秒単位で入力します。

ステップ 7 [OK] をクリックします。

Syslog メッセージの送信

OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Adjacency Changes] 領域では、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するための設定を変更することができます。[Adjacency Changes] 領域で、次の手順を実行します。

- OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するには、[Log Adjacency Changes] チェックボックスをオンにします。
- OSPFv3 ネイバーが起動または停止したときだけではなく、各状態の syslog メッセージを送信するには、[Include Details] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックして変更内容を保存します。

Syslog メッセージの抑止

ルータがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信した場合の syslog メッセージの送信を抑止するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Ignore LSA MOSPF] チェックボックスをオンにして、[OK] をクリックします。

集約ルート コストの計算

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [RFC1583 Compatible] チェックボックスをオンにして、[OK] をクリックします。

OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Default Information Originate Area] で、次の手順を実行します。

a) [Enable] チェックボックスをオンにして、OSPFv3 ルーティング プロセスをイネーブルにします。

b) [Always advertise] チェックボックスをオンにして、出口が 1 つであるかどうかにかかわらず、常時デフォルト ルートをアドバタイズします。

c) デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。

d) [Metric Type] ドロップダウン リストは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。有効な値は次のとおりです。

- 1：タイプ 1 外部ルート
- 2：タイプ 2 外部ルート

デフォルトはタイプ 2 外部ルートです。

e) [Route Map] ドロップダウン リストから、ルート マップが満たされている場合に、デフォルト ルートを生成するルーティング プロセスを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

IPv6 サマリー プレフィックスの設定

手順

ステップ 1 ASDM のメイン ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Summary Prefix]** の順に選択します。

ステップ 2 新しいサマリープレフィックスを追加するには、[Add] をクリックします。既存のサマリープレフィックスを適用するには、[Edit] をクリックします。サマリー プレフィックスを削除するには、[Delete] をクリックします。

[Add Summary Prefix] ダイアログボックスまたは [Edit Summary Prefix] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 5 [Advertise] チェックボックスをオンにして、指定したプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。

ステップ 6 ルートマップを使用して再配布を制御するように照合値として使用できるタグ値を [Tag] フィールドに入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックして変更内容を保存します。

IPv6 ルートの再配布

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Redistribution]** の順に選択します。

ステップ 2 OSPFv3 プロセスに接続済みルートを再配布するための新しいパラメータを追加するには、[Add] をクリックします。OSPFv3 プロセスに接続済みルートを再配布するための既存のパラメータを変更するには、[Edit] をクリックします。パラメータの選択したセットを削除するには [Delete] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [Source Protocol] ドロップダウン リストから、ルートが再配布されるソース プロトコルを選択します。サポートされるプロトコルは、接続済み、スタティック、OSPF です。

ステップ 5 [Metric] フィールドにメトリック値を入力します。同じルータ上の一方の OSPF プロセスから他方の OSPF プロセスにルートを再配布する場合、メトリック値を指定しないと、メトリックは一方のプロセスから他方のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

ステップ 6 [Metric Type] ドロップダウン リストからメトリック タイプを選択します。使用可能なオプションは、[None]、[1]、[2] です。

ステップ 7 （オプション）[Tag] フィールドにタグ値を入力します。このパラメータは、ASBR 間で情報の転送に使用される可能性のある各外部ルートに付加される 32 ビットの 10 進数値を指定します。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ～ 4294967295 です。

ステップ 8 [Route Map] ドロップダウン リストからルート マップを選択して、ソース ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをオンにします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。

ステップ 9 再配布に接続済みルートを含めるには、[Include Connected] チェックボックスをオンにします。

ステップ 10 [Match] チェックボックスをオンにして他のルーティング ドメインへのルートを再配布し、次のチェックボックスの 1 つをオンにします。

- [Internal] は、特定の自律システムの内部にあるルートです。
- [External 1] は、自律システムの外部ながら、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。
- [External 2] は、自律システムの外部ながら、OSPFv3 にタイプ 2 外部ルートとしてインポートされるルートです。
- [NSSA External 1] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 1 の外部ルートとしてインポートされるルートです。
- [NSSA External 2] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 2 の外部ルートとしてインポートされるルートです。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックして変更内容を保存します。

グレースフル リスタートの設定

ASA では、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding

（NSF）機能では、ルーティングプロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。

ハイアベイラビリティモードでは、アクティブユニットが非アクティブになり、スタンバイユニットが新しいアクティブになると、OSPF プロセスが再起動します。同様に、クラスタモードでは、制御ユニットが非アクティブになり、データユニットが新しい制御ユニットとして選択されると、OSPF プロセスが再起動します。このような OSPF 移行プロセスでは、かなりの遅延が発生します。OSPF プロセスの状態変更時のトラフィック損失を回避するように NSF を設定できます。また NSF 機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。

グレースフル リスタートは、OSPFv2 と OSPFv3 の両方でサポートされています。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。graceful-restart（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

（注） OSPFv2 用に fast hello が設定されている場合、アクティブ ユニットのリロードが発生し、スタンバイ ユニットがアクティブになっても、グレースフル リスタートは発生しません。これは、ロール変更にかかる時間は、設定されているデッド インターバルよりも大きいためです。

OSPFv2 のグレースフル リスタートの設定

OSPFv2、Cisco NSF および IETF NSF には、2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

OSPFv2 の Cisco NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフル リスタートを設定します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2 [Configuring Cisco NSF] の下で、[Enable Cisco nonstop forwarding (NSF)] チェックボックスをオンにします。

ステップ 3 （オプション）必要に応じて、[Cancels NSF restart when non-NSF-aware neighboring networking devices are detected] チェックボックスをオンにします。

ステップ 4 （オプション）[Configuring Cisco NSF helper] の下で、[Enable Cisco nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

（注） このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで Cisco NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv2 の IETF NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2 [Configuring IETF NSF] で、[Enable IETF nonstop forwarding (NSF)] チェックボックスをオンにします。

ステップ 3 （オプション）[Length of graceful restart interval] フィールドに、リスタート間隔を秒単位で入力します。

（注） デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

ステップ 4 （オプション）[Configuring IETF NSF helper] で、[Enable IETF nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで IETF NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv3 のグレースフル リスタートの設定

OSPFv3 の NSF グレースフル リスタート機能を設定するには、2 つのステップを伴います。NSF 対応としてのデバイスの設定と、NSF 認識としてのデバイスの設定です。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2 [Configuring Graceful Restart] の下で、[Enable Graceful Restart] チェックボックスをオンにします。

ステップ 3 （オプション）[Restart Interval] フィールドにリスタート間隔の値を入力します。

（注） デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

ステップ 4 [Configuring Graceful Restart Helper] の下で、[Enable Graceful Restart Helper] チェックボックスをオンにします。

このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 （オプション）[Enable LSA checking] チェックボックスをオンにして、厳密なリンク ステート アドバタイズメント チェックをイネーブルにします。

イネーブルにすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックして変更内容を保存します。

OSPF のグレースフル リスタート待機タイマーの設定

OSPF ルータでは、すべてのネイバーがパケットに含まれているかが不明な場合は、Hello パケットにアタッチされている EO-TLV に RS ビットを設定することが予期されます。ただし、隣接関係（アジャセンシー）を維持するにはルータの再起動が必要です。ただし、RS ビット値は RouterDeadInterval 秒より長くすることはできません。そのため、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するための **timers nsf wait** コマンドが導入されました。NSF 待機タイマーのデフォルト値は 20 秒です。

始める前に

- OSPF の Cisco NSF 待機時間を設定するには、デバイスが NSF 認識または NSF 対応である必要があります。

手順

ステップ 1 OSPF ルータ コンフィギュレーション モードを開始します。

例：

```
ciscoasa(config)# router ospf
```

ステップ 2 タイマーを入力し、NSF を指定します。

例：

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

ステップ 3 グレースフルリスタート待機間隔を入力します。この値は、1 ～ 65535 の範囲で指定できます。

例：

```
ciscoasa(config-router)# timers nsf wait 200
```

グレースフルリスタート待機間隔を使用することで、待機間隔がルータの dead 間隔よりも長くならないようにできます。

OSPFv2 設定の削除

OSPFv2 設定を削除します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Enable this OSPF Process] チェックボックスをオフにします。

ステップ 3 [Apply] をクリックします。

OSPFv3 設定の削除

OSPFv3 設定を削除します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Enable OSPFv3 Process] チェックボックスをオフにします。

ステップ 3 [Apply] をクリックします。

OSPFv2 の例

次の例に、さまざまなオプションのプロセスを使用して OSPFv2 をイネーブルにし、設定する方法を示します。

1. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。
2. [Process Instances] タブをクリックし、[OSPF Process 1] フィールドに **2** と入力します。
3. [Area/Networks] タブをクリックし、[Add] をクリックします。
4. [Area ID] フィールドに **0** と入力します。
5. [Area Networks] 領域の [IP Address] フィールドに **10.0.0.0** と入力します。
6. [Netmask] ドロップダウン リストで [255.0.0.0] を選択します。
7. [OK] をクリックします。
8. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Redistribution]** の順に選択します。
9. [Add] をクリックします。

[Add/Edit OSPF Redistribution Entry] ダイアログボックスが表示されます。

10. [Protocol] 領域の [OSPF] オプション ボタンをクリックして、ルートが再配布されるソース プロトコルを指定します。[OSPF] を選択すると、別の OSPF ルーティング プロセスからのルートが再配布されるようになります。
11. OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。
12. [Match] 領域の [Internal] チェックボックスをオンにします。
13. [Metric Value] フィールドに、再配布されるルーティングのメトリック値として **5** を入力します。
14. [Metric Type] ドロップダウン リストで、メトリック タイプの値として 1 を選択します。
15. [Route Map] ドロップダウン リストで、1 を選択します。
16. [OK] をクリックします。
17. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Interface]** の順に選択します。
18. [Properties] タブで、[inside] インターフェイスを選択して [Edit] をクリックします。

    [Edit OSPF Properties] ダイアログボックスが表示されます。
19. [Cost] フィールドに **20** と入力します。
20. [Advanced] をクリックします。
21. [Retransmit Interval] フィールドに **15** と入力します。
22. [Transmit Delay] フィールドに **20** と入力します。
23. [Hello Interval] フィールドに **10** と入力します。
24. [Dead Interval] フィールドに **40** と入力します。
25. [OK] をクリックします。
26. [Edit OSPF Properties] ダイアログボックスで、[Priorities] フィールドに **20** と入力して [OK] をクリックします。
27. [Authentication] タブをクリックします。

    [Edit OSPF Authentication] ダイアログボックスが表示されます。
28. [Authentication] 領域の [MD5] オプション ボタンをクリックします。
29. [MD5 and Key ID] 領域の [MD5 Key] フィールドに **cisco** と入力し、[MD5 Key ID] フィールドに **1** と入力します。
30. [OK] をクリックします。
31. **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** を選択し、[Area/Networks] タブをクリックします。

32. [OSPF 2] プロセスを選択し、[Edit] を選択します。

    [Edit OSPF Area] ダイアログボックスが表示されます。

33. [Area Type] 領域で、[Stub] を選択します。

34. [Authentication] 領域で、[None] を選択し、[Default Cost] フィールドに **20** と入力します。

35. [OK] をクリックします。

36. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

37. [Process Instances] タブをクリックし、[OSPF process 2] チェックボックスをオンにします。

38. [Advanced] をクリックします。

    [Edit OSPF Area] ダイアログボックスが表示されます。

39. [Timers] 領域で、[SPF Delay Time] フィールドに **10** と入力し、[SPF Hold Time] フィールドに **20** と入力します。

40. [Adjacency Changes] 領域の [Log Adjacency Change Details] チェックボックスをオンにします。

41. [OK] をクリックします。

42. [リセット（Reset）] をクリックします。

OSPFv3 の例

次に、ASDM で OSPFv3 ルーティングを設定する例を示します。

1. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

2. [Process Instances] タブで、次の手順を実行します。

    1. [Enable OSPFv3 Process] チェックボックスをオンにします。

    2. [Process ID] フィールドに **1** を入力します。

3. [Areas] タブをクリックし、続いて [Add] をクリックして、[Add OSPFv3 Area] ダイアログボックスを表示します。

4. [OSPFv3 Process ID] ドロップダウン リストから、**1** を選択します。

5. [Area ID] フィールドに **22** と入力します。

6. [Area Type] ドロップダウン リストから [Normal] を選択します。

7. [Default Cost] フィールドに **10** を入力します。

8. [Redistribution imports routes to normal and NSSA areas] をオンにします。
9. [Metric] フィールドに **20** を入力します。
10. [Metric Type] ドロップダウン リストから **1** を選択します。
11. 使用されているインターフェイスの指定に合わせて、**内部**チェックボックスをオンにします。
12. [Enable Authentication] チェックボックスをオンにします。
13. [Security Policy Index] フィールドに **300** を入力します。
14. [Authentication Algorithm] ドロップダウン リストから [SHA-1] を選択します。
15. [Authentication Key] フィールドに **12345ABCDE** を入力します。
16. [Encryption Algorithm] ドロップダウン リストから [DES] を選択します。
17. [Encryption Key] フィールドに **1122334455aabbccddee** を入力します。
18. [OK] をクリックします。
19. [Route Summarization] タブをクリックし、続いて [Add] をクリックして、[Add Route Summarization] ダイアログボックスを表示します。
20. [Process ID] ドロップダウン リストから **1** を選択します。
21. [Area ID] ドロップダウン リストから **22** を選択します。
22. [IPv6 Prefix/Prefix Length] フィールドに **2000:122::/64** を入力します。
23. （オプション）[Cost] フィールドに **100** を入力します。
24. [Advertised] チェックボックスをオンにします。
25. [OK] をクリックします。
26. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Interface]** の順に選択します。
27. [Properties] タブをクリックします。
28. **内部**チェックボックスをオンにし、[Edit] をクリックして、[Edit OSPF Properties] ダイアログボックスを表示します。
29. [Cost] フィールドに **20** と入力します。
30. [Priority] フィールドに **1** を入力します。
31. [Point-to-Point] チェックボックスをオンにします。
32. [Dead Interval] フィールドに **40** と入力します。
33. [Hello Interval] フィールドに **10** と入力します。
34. [Retransmit Interval] フィールドに **15** と入力します。

35. [Transmit Delay] フィールドに **20** と入力します。
36. [OK] をクリックします。
37. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Redistribution]** の順に選択します。
38. [Process ID] ドロップダウン リストから **1** を選択します。
39. [Source Protocol] ドロップダウン リストから [OSPF] を選択します。
40. [Metric] フィールドに **50** を入力します。
41. [Metric Type] ドロップダウン リストから **1** を選択します。
42. [OK] をクリックします。
43. [Apply] をクリックして変更内容を保存します。

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することもできます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

OSPFv2 ルーティングのさまざまな統計情報を ASDM でモニターまたは表示するには、次の手順を実行します。

1. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPF LSAs]** の順に選択します。
2. 選択してモニターできる OSPF LSA は、タイプ 1 ～ 5 と 7 です。各ペインには、次のように 1 つの LSA タイプが表示されます。
   - [Type 1 LSAs] は、特定のエリア内の特定プロセス下にあるすべてのルートを表します。
   - [Type 2 LSAs] には、ルータをアドバタイズする指定ルータの IP アドレスが表示されます。
   - [Type 3 LSAs] には、宛先ネットワークの IP アドレスが表示されます。
   - [Type 4 LSAs] には、AS 境界ルータの IP アドレスが表示されます。
   - [Type 5 LSAs] と [Type 7 LSAs] には、AS 外部ネットワークの IP アドレスが表示されます。
3. [Refresh] をクリックすると、各 LSA タイプのペインが更新されます。

4. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPF Neighbors]** の順に選択します。

   [OSPF Neighbors] ペインの各行は 1 つの OSPF ネイバーを表します。さらに、[OSPF Neighbors] ペインにはそのネイバーが実行されているネットワーク、優先度、状態、デッド時間（秒単位）、ネイバーの IP アドレス、および実行されているインターフェイスも表示されます。OSPF ネイバーが取る可能性のある状態の一覧については、RFC 2328 を参照してください。

5. [Refresh] をクリックすると、[OSPF Neighbors] ペインが更新されます。

OSPFv3 ルーティングのさまざまな統計情報を ASDM でモニターまたは表示するには、次の手順を実行します。

1. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPFv3 LSAs]** の順に選択します。

2. OSPFv3 LSA を選択し、モニターすることができます。[Link State type] ドロップダウン リストでリンク ステート タイプを選択し、指定されたパラメータに従って状態を表示します。サポートされるリンク ステート タイプは、ルータ、ネットワーク、エリア間プレフィックス、エリア間ルータ、AS エクスターナル、NSSA、リンク、エリア内プレフィックスです。

3. [Refresh] をクリックして、各リンク ステート タイプを更新します。

4. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPFv3 Neighbors]** の順に選択します。

   [OSPFv3 Neighbors] ペインの各行は 1 つの OSPFv3 ネイバーを表します。さらに、[OSPFv3 Neighbors] ペインには、ネイバーの IP アドレス、優先度、状態、秒単位のデッド タイム量、動作中のインターフェイスが表示されます。OSPFv3 ネイバーが取る可能性のある状態の一覧については、RFC 5340 を参照してください。

5. [Refresh] をクリックすると、[OSPFv3 Neighbors] ペインが更新されます。

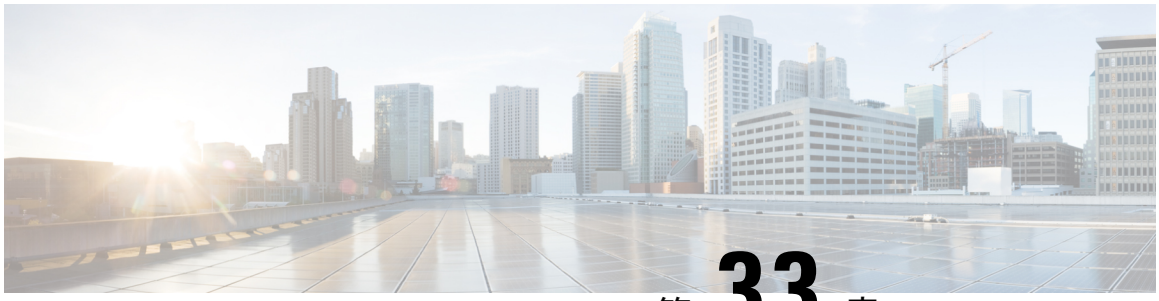
OSPF の履歴

表 *40 : OSPF* の機能履歴

機能名	プラットフォームリリース	機能情報
OSPF サポート	7.0(1)	Open Shortest Path First（OSPF）ルーティングプロトコルを使用した、データのルーティング、認証、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [OSPF]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	OSPFv2 ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing]> [OSPF] > [Setup]
クラスタ	9.0(1)	OSPFv2 および OSPFv3 の場合、バルク同期、ルートの同期およびスパンド EtherChannel ロード バランシングは、クラスタリング環境でサポートされます。
IPv6 の OSPFv3 サポート	9.0(1)	OSPFv3 ルーティングが IPv6 に対してサポートされます。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interface]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Redistribution]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Summary Prefix]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Virtual Link]、[Monitoring] > [Routing] > [OSPFv3 LSAs]、[Monitoring] > [Routing] > [OSPFv3 Neighbors]。

機能名	プラットフォームリリース	機能情報
Fast Hello に対する OSPF サポート	9.2(1)	OSPF は、Fast Hello パケット機能をサポートしているため、OSPF ネットワークでのコンバージェンスが高速なコンフィギュレーションになります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] > [Edit OSPF Interface Advanced Properties]
タイマー	9.2(1)	新しい OSPF タイマーを追加し、古いタイマーを廃止しました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Edit OSPF Process Advanced Properties]
アクセスリストを使用したルートフィルタリング	9.2(1)	ACL を使用したルート フィルタリングがサポートされるようになりました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Filtering Rules] > [Add Filter Rules]
OSPF モニターリングの強化	9.2(1)	OSPF モニターリングの詳細情報が追加されました。
OSPF 再配布 BGP	9.2(1)	OSPF 再配布機能が追加されました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution]
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.3(1)	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [NSF Properties]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [NSF Properties]

機能名	プラットフォームリリース	機能情報
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.13(1)	NSF 待機タイマーが追加されました。 NSF 再起動間隔のタイマーを設定するための新しいコマンドが追加されました。このコマンドが導入され、待機間隔がルータの dead 間隔よりも長くならないようになりました。 次のコマンドが導入されました。 **timers nsf wait <seconds>**



第 33 章

IS-IS

この章では、Intermediate System to Intermediate System（IS-IS）ルーティング プロトコルについて説明します。

IS-IS について

IS-IS ルーティング プロトコルはリンクステート内部ゲートウェイ プロトコル（IGP）です。リンクステートプロトコルは、各参加デバイスで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。IS-IS の実装は、IPv4 と IPv6 をサポートします。

ルーティング ドメインを 1 つ以上のサブドメインに分割することができます。各サブドメインはエリアと呼ばれ、エリアアドレスが割り当てられます。エリア内のルーティングは、レベル 1 ルーティングと呼ばれます。レベル 1 エリア間のルーティングは、レベル 2 ルーティングと呼ばれます。ルータは、中継システム（IS）と呼ばれます。IS はレベル 1 とレベル 2、またはその両方で稼働できます。レベル 1 で稼働している IS は、同じエリア内にある他のレベル 1 の IS とルーティング情報を交換します。レベル 2 で稼働している IS は、他のレベル 2 のルータとルーティング情報を交換します。この場合はルータが同じレベル 1 エリアにあるかどうかは関係しません。レベル 2 にあるルータと、これらとインターコネクトしているリンクは、レベル 2 サブドメインを形成します。ルーティングが正しく機能するためには、これらをパーティション化してはなりません。

NET について

IS は ネットワーク エンティティ タイトル（NET）と呼ばれるアドレスで識別されます。NET はネットワーク サービス アクセスポイント（NSAP）のアドレスで、これにより IS で動作す

る IS-IS ルーティング プロトコルのインスタンスを識別できます。NET は、長さが 8 ～ 20 オクテットで、次の 3 つの部分にわかれています。

- エリア アドレス：このフィールドは 1 ～ 13 オクテット長で、アドレスの上位のオクテットで構成されます。

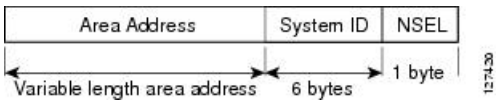
> **注** IS-IS インスタンスに複数のエリア アドレスを割り当てることができます。その場合、すべてのエリア アドレスが同義と見なされます。複数の同義エリア アドレスは、ドメインでエリアをマージまたは分割するときに役立ちます。マージまたは分割が完了した後は、複数のエリア アドレスを IS-IS インスタンスに割り当てる必要はありません。

- システム ID：このフィールドは 6 オクテット長で、エリア アドレスの直後に続きます。IS がレベル 1 で動作する場合、システム ID は、同じエリア内のすべてのレベル 1 デバイス間で一意である必要があります。IS がレベル 2 で動作する場合、システム ID は、ドメイン内のすべてのデバイス間で一意である必要があります。

> **注** 1 つの IS インスタンスに 1 つのシステム ID を割り当てます。

- NSEL：この N セレクタ フィールドは 1 オクテット長で、システム ID の直後に続きます。このフィールドは 00 に設定する必要があります。

図 *67 : NET* の形式



IS-IS ダイナミック ホスト名

IS-IS ルーティング ドメインでは、各 ASA はシステム ID により表されます。システム ID は、IS-IS ASA ごと構成されている NET の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されている ASA のシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ASA でのメンテナンスやトラブルシューティングの間、ASA 名とシステム ID の対応を覚えているのは難しいことです。

ダイナミック ホスト名メカニズムはリンクステート プロトコル（LSP）フラッディングを使用して、ネットワーク全体に ASA 名に対するシステム ID のマッピング情報を配布します。ネットワーク上の ASA はすべて、このシステム ID に対する ASA 名のマッピング情報をルーティング テーブルにインストールしようと試みます。

ネットワーク上で、ダイナミック名のタイプ、長さ、値（TLV）をアドバタイズしているASAが突然、アドバタイズメントを停止した場合、最後に受信されたマッピング情報が最大 1 時間、ダイナミック ホスト マッピング テーブルに残るため、ネットワークに問題が発生している間、ネットワーク管理者はマッピング テーブル内のエントリを表示できます。

IS-IS での PDU のタイプ

IS では、プロトコル データ ユニット（PDU）を使用してルーティング情報をピアと交換します。PDU の中間システム相互間 Hello PDU（IIH）、リンク状態 PDU（LSP）、およびシーケンス番号 PDU（SNP）タイプが使用されます。

IIH

IIH は、IS-IS プロトコルが有効になっている回線の IS ネイバー間で交換されます。IIH には、送信者のシステム ID、割り当てられたエリア アドレス、送信 IS に認識されているその回線上のネイバーのアイデンティティが含まれます。追加のオプションの情報が含まれる場合もあります。

IIH には、次の 2 種類があります。

- レベル 1 LAN IIH：これらは、マルチアクセス回線において、送信 IS がその回線でレベル 1 デバイスとして動作する場合に送信されます。
- レベル 2 LAN IIH：これらは、マルチアクセス回線において、送信 IS がその回線でレベル 2 デバイスとして動作する場合に送信されます。

LSP

IS では LSP を生成して、そのネイバーや IS に直接接続されている接続先をアドバタイズします。LSP は、以下のものによって一意に識別できます。

- LSP を生成した IS のシステム ID。
- Pseudonode ID：この値は LSP が pseudonode LSP の場合を除き、常に 0 です
- LSP 番号（0 ～ 255）
- 32 ビットのシーケンス番号

LSP の新しいバージョンが生成されるたびに、シーケンス番号が増加します。

レベル 1 の LSP は、レベル 1 をサポートしている ISで生成されます。レベル 1 の LSP はレベル 1 のエリア全体にフラッディングされます。エリア内のすべてのレベル 1 の IS で生成されたレベル 1 の LSP のセットは、レベル 1 LSP データベース（LSPDB）となります。エリア内のすべてのレベル 1 の IS は同一のレベル 1 の LSPDB を持ちます。したがって、そのエリアの同一のネットワーク接続マップを持つことになります。

レベル 2 の LSP は、レベル 2 をサポートしている ISで生成されます。レベル 2 の LSP は、レベル 2 のサブドメイン全体にフラッディングされます。ドメイン内のすべてのレベル 2 の IS で生成されたレベル 2 の LSP のセットは、レベル 2 LSP データベース（LSPDB）と

なります。すべてのレベル 2 の IS は同一のレベル 2 の LSPDB を持ちます。したがって、そのレベル 2 のサブドメインの同一の接続マップを持つことになります。

SNP

SNP には、1 つ以上の LSP のサマリー説明が含まれます。レベル 1 とレベル 2 の両方について、次の 2 つのタイプの SNP があります。

- Complete Sequence Number PDU（CSNP）は、特定のレベルに関して IS が持つ LSPDB のサマリを送信するために使用されます。
- Partial Sequence Number PDU（PSNP）は、IS がそのデータベースに持つか取得する必要がある特定のレベルに関する LSP のサブセットのサマリを送信するために使用されます。

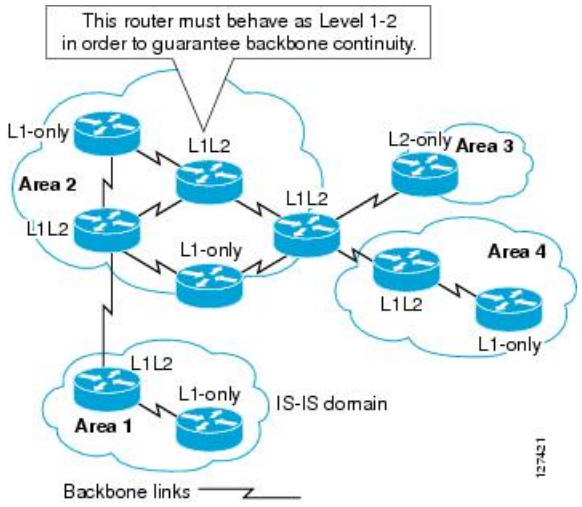
マルチアクセス回線での IS-IS の動作

マルチアクセス回線では複数の IS がサポートされます。つまり、回線で 2 つ以上の IS が動作します。マルチアクセス回線で必要な前提条件は、マルチキャスト アドレスまたはブロードキャストアドレスを使用して複数のシステムのアドレスを指定できることです。マルチアクセス回線でレベル 1 をサポートする IS は、レベル 1 の LAN IIH を回線上に送信します。マルチアクセス回線でレベル 2 をサポートする IS は、レベル 2 の LAN IIH を回線上に送信します。IS は、回線上でネイバー IS とレベルごとに別々の隣接関係（アジャセンシー）を形成します。

IS は回線上でレベル 1 をサポートする他の IS とレベル 1 の隣接関係（アジャセンシー）を形成し、同じエリア アドレスを持ちます。同一マルチアクセス回線上で、レベル 1 をサポートするエリア アドレスの整合性のないセットを持つ 2 つの IS は、サポートされていません。IS は回線上でレベル 2 をサポートする他の IS とレベル 2 の隣接関係（アジャセンシー）を形成します。

以下の図の IS-IS のネットワーク トポロジ内のデバイスは、ネットワークのバックボーンに従って、レベル 1、レベル 2、またはレベル 1 と 2 のルーティングを実行します。

図 *68 : IS-IS* ネットワーク トポロジにおけるレベル *1*、レベル *2*、レベル *1-2* デバイス



IS-IS での代表 IS の選択

各 IS が LSP 内のマルチアクセス回線上のすべての隣接関係をアドバタイズする場合、必要なアドバタイズメントの総数は N 2 になります。ここで、N は回線の特定のレベルで動作している IS の数です。この拡張性の問題を解消するため、IS-IS ではマルチアクセス回線を表す擬似ノードを定義します。特定のレベルで動作するすべての IS が、その回線の代表中継システム（DIS）として機能するように IS のいずれかを選定します。DIS は、回線でアクティブな各レベルごとに選定されます。

DIS は擬似ノード LSP を発行する責任を担います。擬似ノード LSP には、その回線で動作するすべての IS のネイバー アドバタイズメントが含まれます。その回線で動作するすべての IS（DIS を含む）が非擬似ノード LSP 内の擬似ノードにネイバーアドバタイズメントを提供し、マルチアクセス回線上のネイバーはアドバタイズしません。このように、必要なアドバタイズメントの総数は、N（回線で動作する IS の数）に応じて変わります。

擬似ノード LSP は次の ID によって一意に分類されます。

- LSP を生成した DIS のシステム ID
- Pseudonode ID（常にゼロ以外）
- LSP 番号（0 ～ 255）
- 32 ビットのシーケンス番号

ゼロ以外の擬似ノード ID は、擬似ノード LSP と擬似ノード以外の LSP を区別するもので、このレベルでも DIS である場合に、他の LAN 回線の間で一意になるように、DIS によって選択されます。

また、DIS は回線上に定期的な CSNP を送信する責任も担っています。これは、DIS 上の LSPDB の現在のコンテンツに関する完全な要約説明を提供します。回線上の他の IS が次のアクティビティを実行できます。これにより、マルチアクセス回線上のすべての IS の LSPDB が効率的かつ確実に同期されます。

- DIS によって送信された CSNP に存在しない LSP、またはその CSNP に記述された LSP より新しい LSP をフラッディングします。
- ローカル データベースに存在しない DIS によって送信された CSNP セットに記述されている LSP、または CSNP セットに記述されている LSP より古い LSP の PSNP を送信することで、LSP を要求します。

IS-IS LSPDB の同期

IS-IS を適切に動作させるには、各 IS 上の LSPDB を同期するため信頼性の高い効率的なプロセスが必要です。IS-IS では、このプロセスは更新プロセスと呼ばれます。更新プロセスは、各サポート レベルで独立して動作します。ローカルに生成される LSP は常に新しい LSP です。回線上のネイバーから受信した LSP は、他の IS によって生成されているか、またはローカル IS によって生成された LSP のコピーであることがあります。受信した LSP はローカル LSPDB の現在のコンテンツに比べ、古い、同じ、または新しい場合があります。

新しい LSP の処理

ローカル LSPDB に追加された新しい LSP は、LSPDB の同じ LSP の古いコピーを置き換えます。新しい LSP は、新しい LSP を受信した回線を除き、IS が現在、新しい LSP に関連付けられているレベルでアップ状態の隣接関係（アジャセンシー）を持つすべての回線に送信されるようにマークされます。

マルチアクセス回線では、IS は新しい LSP を 1 回フラッディングします。IS は、マルチアクセス回線用に DIS によって定期的に送信される一連の CNSP を調べます。ローカル LSPDB に CSNP セットに記述されている LSP より新しい LSP が 1 つ以上含まれている場合は（これには CSNP セットに存在しない LSP も含まれる）、それらの LSP がマルチアクセス回線経由で再度フラッディングされます。ローカル LSPDB に CSNP セットに記述された LSP より古い LSP が 1 つ以上含まれる場合は（これには、ローカル LSPDB に存在しない CSNP セットに記述された LSP も含まれる）、更新が必要な LSP の記述とともに PSNP がマルチアクセス回線上に送信されます。マルチアクセス回線の DIS は、要求された LSP を送信することで応答します。

古い LSP の処理

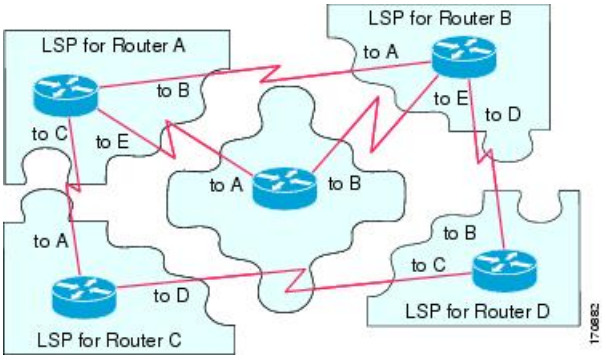
IS でローカルの LSPDB のコピーよりも古い LSP を受信する場合があります。また IS でローカルの LSPDB のコピーよりも古い LSP について説明する SNP（全体または一部）を LSPDB 受信する場合もあります。いずれの場合も、IS によってローカル データベースでその LSP がマークされ、古い LSP が含まれている古い LSP または SNP が受信された回線にフラッディングされます。実行されるアクションは、前述の新しい LSP がローカルデータベースに追加された後のアクションと同じです。

経過期間が同じ LSP の処理

更新プロセスの分散型の特性のため、IS がローカル LSPDB の現在のコンテンツと同じ LSP のコピーを受信する可能性があります。マルチアクセス回線では、経過期間が同じ LSP の受信は無視されます。回線の DIS によって設定された CSNP が定期的に送信され、LSP を受信した送信者への明示的な確認応答の役割を果たします。

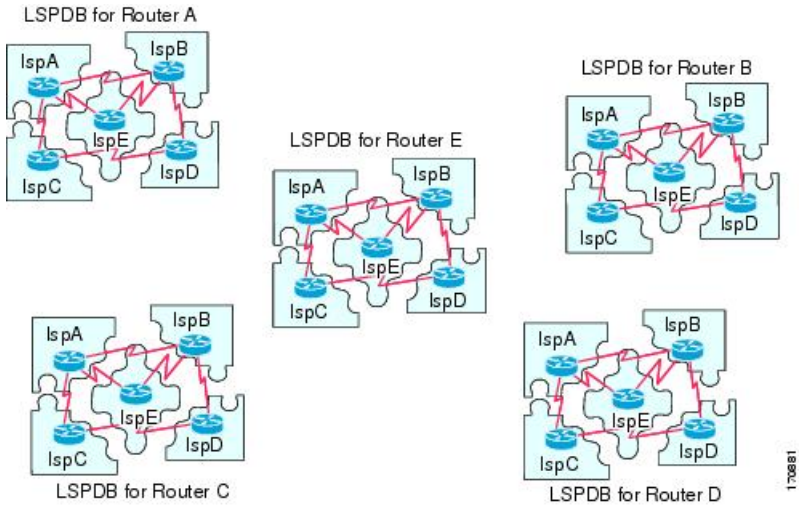
次の図は、LSP を使用してネットワーク マップを作成する方法を示しています。ネットワークトポロジをジグソー パズルとして想像してください。各 LSP（IS を表す）はジグソー パズルの 1 つのピースに相当します。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

図 *69 : IS-IS* ネットワーク マップ



次の図は、ネイバー デバイス間で隣接関係（アジャセンシー）が形成された後に、IS-IS ネットワーク内の各デバイスが完全に更新されたリンクステートデバイスを備えていることを示しています。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

図 *70 : LSPDB* が同期された *IS-IS* デバイス



IS-IS 最短パスの計算

LSPDB のコンテンツが変更されると、各 IS は独立して最短パスの計算を再実行します。アルゴリズムは、有向グラフに沿って最短パスを見つけるためのよく知られたダイクストラアルゴリズムに基づいています。有向グラフでは、各 IS がグラフの頂点で、IS 間のリンクが非負の重みを持つエッジとなります。2 つの IS 間のリンクをグラフの一部として見なす前に、双方向接続チェックが実行されます。これによって、たとえば、1 つの IS がすでにネットワーク内で動作していないが、動作を停止する前に、生成した LSP セットを消去しなかった場合などに、LSPDB 内で古い情報が使用されるのを防ぎます。

SPF の出力は、一連のタプル（宛先、ネクストホップ）です。宛先は、プロトコルによって異なります。複数のネクスト ホップが同じ宛先に関連付けられている場合は、複数の等コストパスがサポートされます。

IS によってサポートされているレベルごとに、独立した SPF が実行されます。同じ宛先がレベル 1 パスとレベル 2 パスの両方によって到達可能な場合は、レベル 1 パスが優先されます。

他のエリアに 1 つ以上のレベル 2 ネイバーを持つことを示しているレベル 2 IS は、デフォルトルートとも呼ばれる、ラストリゾートのパスとして同じエリア内のレベル 1 デバイスによって使用される場合があります。レベル 2 IS は、レベル 1 LSP 0 に ATT（Attached）bit を設定することで、他のエリアへのアタッチメントを示します。

（注） IS は、各レベルで最大 256 の LSP を生成できます。LSP は、0 ～ 255 の番号によって識別されます。LSP 0 は、他のエリアへのアタッチメントを示すための ATT ビットの設定の意味を含め、特別なプロパティを備えています。番号 1 ~ 255 の LSP に ATT ビットが設定されている場合は、それに意味はありません。

IS-IS シャットダウン プロトコル

IS-IS をシャットダウンする（管理上のダウン状態にする）ことで、設定パラメータを失うことなく IS-IS プロトコル設定に変更を加えることができます。グローバル IS-IS プロセス レベルまたはインターフェイス レベルで IS-IS をシャットダウンできます。プロトコルがオフになっているときにデバイスが再起動すると、プロトコルは、通常、ディセーブル状態でアップします。プロトコルが管理上のダウン状態に設定されている場合、ネットワーク管理者は、プロトコル設定を失うことなく IS-IS プロトコルを管理上オフにし、中間状態（多くの場合、望ましくない状態）を経てプロトコルの動作を遷移させることなくプロトコル設定に一連の変更を加え、適切なタイミングでプロトコルを再度イネーブルにすることができます。

IS-IS の前提条件

IS-IS を設定する前に、次の前提条件を満たしている必要があります。

- IPv4 および IPv6 を理解していること。
- IS-IS を設定する前にネットワーク設計およびそれを経由するトラフィックのフロー方法を理解していること。
- エリアを定義し、デバイスのアドレッシング計画を準備し（NET の定義を含む）、IS-IS を実行するインターフェイスを決定していること。
- デバイスを設定する前に、隣接関係テーブルに表示されるネイバーを示す隣接関係のマトリックスを準備しておくこと。これにより検証が容易になります。

IS-IS のガイドライン

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

クラスタのガイドライン

個々のインターフェイス モードでのみサポート：スパンド EtherChannel モードはサポートされません。

その他のガイドライン

双方向転送で、IS-IS はサポートされていません。

IS-IS の設定

ここでは、システムで IS-IS プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 IS-IS ルーティングのグローバルな有効化 （991 ページ）。
ステップ 2 IS-IS 認証の有効化 （993 ページ）。
ステップ 3 IS-IS LSP の設定 （993 ページ）
ステップ 4 IS-IS サマリー アドレスの設定 （995 ページ）。
ステップ 5 IS-IS NET の設定 （997 ページ）。
ステップ 6 IS-IS パッシブ インターフェイスの設定 （998 ページ）。
ステップ 7 IS-IS インターフェイスの設定 （999 ページ）。
ステップ 8 IS-IS IPv4 アドレス ファミリの設定 （1003 ページ）。
ステップ 9 IS-IS IPv6 アドレス ファミリの設定 （1007 ページ）。

IS-IS ルーティングのグローバルな有効化

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[General]** を選択します。
ステップ 2 [Configure ISIS] チェックボックスをオンにして、IS-IS を有効にします。
ステップ 3 [Shutdown protocol] チェックボックスをオンにして、シャットダウン プロトコルを有効にします。

シャットダウン プロトコルの詳細については、IS-IS シャットダウン プロトコル （990 ページ）を参照してください。

ステップ 4 IS-IS でダイナミック ホスト名が使用されるようにするには、[Use dynamic hostname] チェックボックスをオンにします。

デフォルトでは、ダイナミック ホスト名は有効です。IS-IS のダイナミック ホスト名の詳細については、IS-IS ダイナミック ホスト名 （984 ページ）を参照してください。

ステップ 5 IS-IS で LAN hello PDU のパディングが行われないようにするには、[Do not pad LAN hello PDUs] チェックボックスをオンにします。

最大伝送ユニット（MTU）サイズになるまで IS-IS hello がパディングされます。これにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。hello パディングを無効にして、両方のインターフェイスの MTU が同じである場合や、トランスレーショナル ブリッジングの場合に、ネットワーク帯域幅が浪費されないようにすることができます。

ステップ 6 パッシブ インターフェイスのみをアドバタイズするには、[Advertise passive only] チェックボックスをオンにします。

これにより、接続されているネットワークの IP プレフィックスが LSP アドバタイズメントから除外され、IS-IS コンバージェンス時間が短縮されます。

ステップ 7 該当するオプション ボタンをクリックして、ASA がステーション ルータ（レベル 1）、エリア ルータ（レベル 2）、またはその両方（レベル 1-2）のいずれとして動作するかを選択します。

IS-IS レベルの詳細については、IS-IS について （983 ページ）を参照してください。

ステップ 8 [Topology priority] フィールドに、トポロジ内での ASA のプライオリティを示す数値を入力します。指定できる範囲は 0 ～ 127 です。

ステップ 9 [Route priority tag] フィールドに、ASA のルート プライオリティを示すタグを入力します。範囲は 1 ～ 4294967295 です。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、IS-IS システム内のすべてのルータに送信されます。

ステップ 10 条件に応じて IS が L2 としてアドバタイズするように設定するには、ドロップダウン メニューからデバイスを選択し、[Manage] をクリックします。

ルート マップの追加手順は、ルート マップの定義を参照してください。

ステップ 11 [Log changes in adjacency] チェックボックスをオンにすると、IS-IS ネイバーがアップ状態またはダウン状態になるたびに ASA によってログ メッセージが送信されるようになります。

このコマンドは、デフォルトでディセーブルになっています。隣接関係（アジャセンシー）の変更をロギングすると、大規模なネットワークをモニターリングする際に役立ちます。

ステップ 12 非 IIH イベントからの変更を含めるには、[Include changes generated by non-IIH events] チェックボックスをオンにします。

ステップ 13 懐疑的な時間間隔を設定するには、[Skeptical interval] フィールドに時間（分単位）を入力します。指定できる範囲は 0 ～ 1440 分です。デフォルトは 5 分です。

ステップ 14 [Apply] をクリックします。

IS-IS 認証の有効化

IS-IS ルート認証により、未承認の送信元から不正なルーティング メッセージまたは誤ったルーティング メッセージを受信することが防止されます。各 IS-IS エリアまたはドメインにパスワードを設定することで、不正なルータが誤ったルーティング情報をリンクステート データベースに挿入することを阻止できます。あるいは IS-IS 認証タイプ（IS-IS MD5 認証または拡張クリアテキスト認証）を設定できます。インターフェイスごとに認証を設定することもできます。IS-IS メッセージ認証対象として設定されたインターフェイス上にあるすべての IS-IS ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

エリアとドメインの詳細については、IS-IS について （983 ページ）を参照してください。

始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化 （991 ページ）を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[Authentication]** の順に選択します。

ステップ 2 レベル 1 とレベル 2 の認証パラメータを設定します。

- [Key] フィールドに、IS-IS 更新を認証するキーを入力します。このキーの最大長は 16 文字です。
- [Send Only] を有効にするかどうかに応じて、[Enable] または [Disable] オプションボタンをクリックします。

  （注） 送信されるパケットだけに認証が挿入され、受信されるパケットではチェックされない場合、各 ASA で、キーの設定に費やせる時間が長くなります。

- 認証モードを選択するため、[Disabled]、[MD5]、[Plaintext] オプションボタンのいずれかをオンにします。

ステップ 3 [Disabled] をオンにした場合は、レベル 1 エリア（サブドメイン）のエリア パスワードと、レベル 2 ドメインのドメイン パスワードのいずれかまたは両方を入力します。

ステップ 4 [適用（Apply）] をクリックします。

IS-IS LSP の設定

IS では LSP を生成して、そのネイバーや IS に直接接続されている接続先をアドバタイズします。LSP の詳細については、IS-IS での PDU のタイプ （985 ページ）を参照してください。

高速コンバージェンス設定となるように LSP を設定するには、次のコマンドを使用します。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration] > [Device Setup] > [Routing] > [ISIS] > [Link State Packet]** の順に選択します。

（注） IS-IS を設定する前に LSP パラメータを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化 （991 ページ）を参照してください。

ステップ 2 内部チェックサム エラーのある受信 LSP パケットを、ASA がパージするのではなく無視できるようにするには、[Ignore LSP errors] チェック ボックスをオンにしてください。

ステップ 3 SPF 実行の前に LSP の高速フラッディングを実行して埋めるには、[Flood LSPs before running SPF] をオンにし、[Number of LSPs to be flooded] フィールドに数値を入力します。指定できる範囲は 1 ～ 15 です。デフォルトは 5 分です。

このパラメータでは、指定した数の LSP が ASA から送信されます。LSP 数が指定されない場合、デフォルト設定は 5 となります。LSP は、SPF の実行前に SPF を呼び出します。高速フラッディングを有効にすることをお勧めします。それにより、LSP のフラッディング プロセスの速度が上げり、ネットワーク コンバージェンス時間全体が改善されるからです。

ステップ 4 IP プレフィックスを抑制するには、[Suppress IP prefixes] チェック ボックスをオンにし、以下の 1 つをオンにします:

- [Don't advertise IP prefixes learned form another ISIS level when ran out of LSP fragments]：別のレベルから来るルートを抑制します。たとえば、レベル 2 の LSP がフルになると、レベル 1 からのルートが抑制されます。
- [Don't advertise IP prefixes learned form other protocols when ran out of LSP fragments]：ASA 上の再配布ルールを抑制します。

IS-IS への再配布ルート数に制限がないネットワークでは、LSP がフルになってルートが破棄される可能性があります。これらのオプションを使用することにより、PDU がフルになった場合にどのルートが抑制されるかを制御してください。

ステップ 5 レベル 1 とレベル 2 の LSP 生成間隔を設定します。

- [LSP calculation interval]：各 LSP の伝送間の間隔を秒数で入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 分です。

  接続ネットワーク上の任意の 2 台の ASA 間で想定されるラウンドトリップ遅延より大きな数値にする必要があります。この数は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。再送信が発生するのは、LSP が廃棄される場合だけです。したがって、数を大きい値に設定すると、再コンバージェンスへの影響

は小さくなります。ASA のネイバーが多くなるほど、LSP フラッディングの可能性のあるパスが多くなり、この値をより高く設定できます。

- [Initial wait for LSP calculation]：最初の LSP が生成されるまでの初期待機時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルトは 50 です。
- [Minimum wait between first and second LSP calculation]：最初と 2 番目の LSP 生成の間の時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルト値は 5000 です。

ステップ 6 レベル 1 に設定した値をレベル 2 にも適用する場合は、[Use level 1 parameters also for level 2] チェック ボックスをオンにします。

ステップ 7 [Maximum LSP size] フィールドには、連続した 2 つの LSP 生成の間の最大秒数を入力します。指定できる範囲は 128 ～ 4352 です。デフォルトは 1492 です。

ステップ 8 [LSP refresh interval] フィールドには、LSP 更新間隔の秒数を入力します。指定できる範囲は 1 ～ 65,5535 です。デフォルトは 900 です。

リフレッシュ間隔によって、ソフトウェアが定期的に LSP で発信元のルート トポロジ情報を送信するレートが決定されます。これは、データベース情報が古くなるのを避けるために実行されます。

リフレッシュ間隔を短くすると、増加したリンク利用率のコストで未検出のリンク ステート データベース破損が持続する可能性のある期間が短くなります（破損に対する他の予防措置があるため、これは発生する可能性は極めて低いイベントです）。間隔を長くすると、更新されたパケットのフラッディングによるリンク使用率が低下します（ただしこの使用率は非常に低いです）。

ステップ 9 [Maximum LSP lifetime] フィールドには、ルータのデータベース内に更新なしで LSP が保持される最大秒数を入力します。指定できる範囲は 1 ～ 65,535 です。デフォルトは 1200（20 分）です。

LSP の更新間隔を変更した場合、このパラメータを調整する必要があるかもしれません。LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。LSP 更新間隔に設定する値は LSP 最大ライフタイムに設定する値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 更新間隔と比べて LSP ライフタイムを大幅に少なく設定すると、LSP 更新間隔が自動的に短くされて、LSP がタイムアウトしないようになります。

ステップ 10 [Apply] をクリックします。

IS-IS サマリー アドレスの設定

複数のアドレス グループを特定のレベルに集約できます。他のルーティング プロトコルから学習したルートも集約できます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。これにより、ルーティング テーブルのサイズを削減することができます。

ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[Summary Address]** の順に選択します。

[Configure ISIS Summary Address] ペインには、スタティックに定義された IS-IS サマリー アドレスのテーブルが表示されます。デフォルトでは、IS-IS はサブネット ルートをネットワーク レベルに集約します。[Configure ISIS Summary Address] ペインでは、サブネット レベルに集約されるスタティックに定義された IS-IS サマリー アドレスを作成できます。

ステップ 2 新しい IS-IS サマリー アドレスを追加するには [Add] をクリックし、テーブル内の既存の IS-IS サマリー アドレスを編集するには [Edit] をクリックします。

[Add Summary Address] または [Edit Summary Address] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

ステップ 3 [IP Address] フィールドに、サマリー ルートの IP アドレスを入力します。

ステップ 4 [Netmask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択または入力します。

ステップ 5 サマリー アドレスを受信するレベルに応じて、[Level 1]、[Level 2]、または [Level 1 and 2] オプション ボタンをオンにします。

- （オプション）[Level 1]：ルートをレベル 1 およびレベル 2 に再配布するとき、およびレベル 2 IS-IS がレベル 1 ルートをエリアで到達可能なものとしてアドバタイズしたときに集約ルートが適用されます。
- （オプション）[Level 2]：設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートはレベル 2 バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートも集約されます。
- （オプション）[Level 1 and 2]：ルートをレベル 1 およびレベル 2 に再配布するとき、およびレベル 2 IS-IS がレベル 1 ルートをエリアで到達可能なものとしてアドバタイズしたときに集約ルートが適用されます。

ステップ 6 [Tag] フィールドに、タグの番号を入力します。指定できる範囲は 1 ～ 4294967295 です。

[Tag] フィールドには、集約するルートにタグ付けする番号を指定できます。**[Configuration]** > **[Device Setup]** > **[Routing]** > **[SIS]** > **[General]** ペインの [Route priority tag] フィールドですでにタグ付けされているルートは集約されます。集約されない場合、タグは失われます。

ステップ 7 [Metric] フィールドに、集約ルートに適用するメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 10 です。

[Metric] の値はリンクに割り当てられ、宛先へのリンクを介したパス コストを計算するために使用されます。このメトリックは、レベル 1 またはレベル 2 ルーティングに対してだけ設定できます。

ステップ 8 [OK] をクリックします。

ステップ 9 [Apply] をクリックします。

IS-IS NET の設定

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

IS-IS は、Network Entity Title（NET）と呼ばれるアドレスを使用します。このアドレスの長さの範囲は 8 ～ 20 バイトですが、通常は 10 バイトです。ASA でクラスタリングが設定されていない場合に、[NET] ページで NET エントリを追加できます。ASA でクラスタリングが設定されている場合は、[Configuration] > [Device Management] > [Advanced] > [Address Pools] > [NET Address Pools] ペインで、net プール エントリを作成する必要があります。その後、[NET] ペインで NET アドレス プールを参照できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[ISIS]** > **[Network Entity Title (NET)]** を選択します。

[Configure Network Entity (NET)] ペインに、NET アドレスのテーブルが表示されます。ASA でクラスタリングが設定されていない場合にはここで NET エントリを追加できます。クラスタリングが設定されている ASA の場合は、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[Address Pools]** > **[Net Address Pools]** で net プール エントリを作成する必要があります。

その後、[Network Entity Title (NET)] ペインで NET アドレス プールを参照できます。

ステップ 2 新しい IS-IS NET アドレスを追加するには [Add] をクリックし、テーブル内の既存の IS-IS NET アドレスを編集するには [Edit] をクリックします。

[Add Network Entity Title (NET)] または [Edit Network Entity Title (NET)] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

ステップ 3 [Network Entity Title (NET)] ドロップダウンリストから NET を選択します。

ステップ 4 [Maximum allowed Net] フィールドに、有効な NET の最大数を入力します。範囲は 3 ～ 254 です。デフォルトは 3 です。

ほとんどの場合、必要な NET は 1 つだけですが、複数のエリアをマージする場合や 1 つのエリアを複数のエリアに分割する場合には、複数のエリア アドレスを使用する必要がある可能性があります。

ステップ 5 [Apply] をクリックします。

IS-IS パッシブ インターフェイスの設定

トポロジ データベースにインターフェイス アドレスが含まれている間は、インターフェイス上で IS-IS hello パケットおよびルーティング アップデートを無効にできます。これらのインターフェイスは、IS-IS ネイバー隣接関係を形成しません。

IS-IS ルーティングに参加させたくないが、アドバタイズしたいネットワークに接続しているインターフェイスがある場合、インターフェイスが IS-IS を使用しないようにするため、パッシブ インターフェイスを設定します。さらに、ASA がアップデートのために使用する IS-IS のバージョンを指定することもできます。パッシブ ルーティングは、IS-IS ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの IS-IS ルーティング アップデートの送受信を無効にします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[IS-IS]** > **[Passive Interfaces]** の順に選択します。

ステップ 2 すべてのインターフェイスでルーティング アップデートを抑止するには、[Suppress routing updates on all Interfaces] チェックボックスをオンにします。

これにより、すべてのインターフェイスがパッシブ モードで動作します。

ステップ 3 ルーティング アップデートを抑止するように個々のインターフェイスを設定するには、左側のカラムに示されているルーティング インターフェイスを選択し、[Add] をクリックしてそのインターフェイスを [Suppress routing updates] カラムに追加します。

1 つのインターフェイス名を指定すると、そのインターフェイスだけがパッシブ モードに設定されます。パッシブ モードでは、IS-IS ルーティング アップデートは、指定されたインターフェイスにより受信されますが、そこから送信されることはありません。

（注） ダイナミック ホスト名を指定したインターフェイスだけを、ルーティング アップデートを送信しないように設定できます。詳細については、「IS-IS ダイナミック ホスト名 （984 ページ）」を参照してください。

ステップ 4 [Apply] をクリックします。

IS-IS インターフェイスの設定

この手順では、IS-IS ルーティングのための個々の ASA インターフェイスを変更する方法について説明します。

手順

ステップ 1 **[Configuration] > [Device Setup] > [Routing] > [ISIS] > [Interface]** の順に選択します。

[ISIS Interface Configuration] ペインが表示され、IS-IS インターフェイスの設定が表示されます。インターフェイスごとの hello パディングは、[Hello Padding] チェック ボックスをオン/オフにすることによって設定できます。

最大伝送ユニット（MTU）サイズになるまで IS-IS hello がパディングされます。IS-IS hello をフル MTU に埋め込むことにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。

ステップ 2 インターフェイス エントリを選択するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

[Edit ISIS Interface] ダイアログボックスが表示されます。

ステップ 3 [General] タブで、次の項目を設定します。

- [Shutdown ISIS on this interface]：設定パラメータを削除することなく、このインターフェイスの IS-IS プロトコルを無効化できます。IS-IS プロトコルはこのインターフェイスの隣接関係（アジャセンシー）を形成しません。ASA が生成した LSP にインターフェイスの IP アドレスが設定されます。
- [Enable ISIS on this interface]：このインターフェイス上で IS-IS プロトコルを有効にします。
- [Enable IPv6 ISIS routing on this interface]：このインターフェイス上で IPv6 IS-IS ルーティングを有効にします。
- [Priority for level-1]：レベル 1 のプライオリティを設定します。プライオリティ値は、LAN 上の指定ルータまたは Designated Intermediate System（DIS）を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つルータが DIS になります。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。

  （注） IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高いルータがオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

- [Priority for level-2]：レベル 2 のプライオリティを設定します。プライオリティ値は、LAN 上の指定ルータまたは Designated Intermediate System（DIS）を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つルータが DIS になります。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。

（注） IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高いルータがオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

- [Tag]：この IP プレフィックスが IS-IS LSP に設定されている場合に、インターフェイスに設定された IP アドレスにタグを設定します。
- [CSNP Interval for level-1]：レベル 1 のマルチアクセス ネットワークにおける、CSNP の送信間隔の完全なシーケンス番号 PDU (CSNP) を秒数で設定します。この間隔は指定 ASA だけに適用されます。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。デフォルトを変更する必要はまずありません。

  このオプションは、指定したインターフェイスの指定ルータ（DR）に対してのみ適用されます。DR だけがデータベースの同期を維持するために CSNP パケットを送信します。

- [CSNP Interval for level-2]：レベル 2 のマルチアクセス ネットワークにおける、CSNP の送信間隔の完全なシーケンス番号 PDU (CSNP) を秒数で設定します。この間隔は指定 ASA だけに適用されます。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。デフォルトを変更する必要はまずありません。

  このオプションは、指定したインターフェイスの指定ルータ（DR）に対してのみ適用されます。DR だけがデータベースの同期を維持するために CSNP パケットを送信します。

- **[Adjacency filter]**：**IS-IS 隣接関係（アジャセンシー）の確立をフィルタリングします。**

  着信 IS-IS hello パケットから、hello に含まれる各エリア アドレスと システム ID を組み合わせて NSAP アドレスを作成することにより、フィルタリングが実行されます。その後、これらの各 NSAP アドレスがフィルタを通過します。すべてのアドレスが適合することを要求する **Match all area addresses** が指定されていない場合は、いずれかの NSAP が一致するとフィルタに適合したと見なされます。**Match all area addresses** の機能は、特定のアドレスがない場合にのみ隣接関係を受け入れるといったネガティブテストを実行するときに便利です。

- [Match all area addresses]：（オプション）隣接関係（アジャセンシー）を受け入れるには、すべての NSAP アドレスがフィルタと一致する必要があります。指定しない場合（デフォルト）、受け入れる隣接関係（アジャセンシー）に関するフィルタに一致する必要があるのは 1 つのアドレスだけです。

ステップ 4 [OK] をクリックします。

ステップ 5 [Authentication] タブで、レベル 1 やレベル 2 について以下の項目を設定します。

- [Key] フィールドに、IS-IS 更新を認証するキーを入力します。範囲は 0 ～ 8 文字です。

  [Key] オプションで設定されたパスワードが存在しない場合、キー認証は行われません。

- [Send only] については、[Enable] または [Disable] のオプション ボタンをクリックします。

  [Send only] を選択すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフ

トウェアのアップグレード中、移行をスムーズに行うために使用します。デフォルトではディセーブルになっています。

- [Mode] チェック ボックスをオンにし、ドロップダウン リストから [MD5] または [Text] を選択することによって認証モードを選択し、[Password] フィールドにパスワードを入力します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Hello Padding] タブで、次の項目を設定します。

- [Hello Padding]：Hello 埋め込みを有効にします。

  最大伝送ユニット（MTU）サイズになるまで IS-IS hello がパディングされます。IS-IS hello をフル MTU に埋め込むことにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。

- [Minimal holdtime 1 second for Level-1]：レベル 1 で LSP が有効である保留時間（秒数）を有効にします。

- [Hello Interval for level-1]：レベル 1 の hello パケット間の時間の長さを秒数で指定します。

  デフォルトでは、送信される hello パケットで、hello インターバル（seconds）の 3 倍の値が保持時間としてアドバタイズされます（[Hello Multiplier] チェック ボックスをオンにすることにより、この乗数（3）を変更できます）。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。

- [Minimal holdtime 1 second for Level-2]：レベル 2 で LSP が有効である保持時間（秒数）を有効にします。

- [Hello Interval for level-2]：レベル 2 の hello パケット間の時間の長さを秒数で指定します。

  デフォルトでは、送信される hello パケットで、hello インターバル（seconds）の 3 倍の値が保持時間としてアドバタイズされます（[Hello Multiplier] チェック ボックスをオンにすることにより、この乗数（3）を変更できます）。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。

- [Hello Multiplier for level-1]：レベル 1 で、ここに指定する数の IS-IS hello パケットがネイバーにおいて欠落すると、ASA が隣接関係（アジャセンシー）がダウンしたと宣言することになります。

  IS-IS hello パケットのアドバタイズされる hold time は、hello 間隔の hello 乗数倍に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、この ASA への隣接関係（アジャセンシー）がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内の ASA ごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。

- [Hello Multiplier for level-2]：レベル 2 で、ここに指定する数の IS-IS hello パケットがネイバーにおいて欠落すると、ASA が隣接関係（アジャセンシー）がダウンしたと宣言することになります。

  IS-IS hello パケットのアドバタイズされる hold time は、hello 間隔の hello 乗数倍に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、この ASA への隣接関係（アジャセンシー）がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内の ASA ごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。

- [Configure Circuit Type]：ローカル ルーティング（レベル 1）、エリア ルーティング（レベル 2）、またはローカルとエリアの両方のルーティング（レベル 1 ～ 2）のどれについてインターフェイスが設定されているかを指定します。

ステップ 8 [OK] をクリックします。

ステップ 9 [LSP Settings] タブで、次の項目を設定します。

- [Advertise ISIS Prefix]：IS-IS インターフェイスごとの LSP アドバタイズメントで、接続されたネットワークの IP プレフィックスのアドバタイズを許可します。

  このオプションを無効にすることは、LSP アドバタイズメントから、接続されたネットワークの IP プレフィックスを除外し、IS-IS コンバージェンス時間を削減するための IS-IS メカニズムです。

- [Retransmit Interval]：各 IS-IS LSP の再伝送間の時間を秒数で指定します。

  接続ネットワーク上の任意の 2 台の ASA 間で想定されるラウンドトリップ遅延より大きな数値にする必要があります。指定できる範囲は 0 ～ 65535 です。デフォルトは 5 分です。

- [Retransmit Throttle Interval]：各 IS-IS LSP で再送信間のミリ秒数を指定します。

  このオプションは、LSP 再送信トラフィックの制御方法として、多くの LSP およびインターフェイスを持つ大規模なネットワークで役立つ場合があります。このオプションは、インターフェイスで LSP を再送信できるレートを制御します。指定できる範囲は 0 ～ 65535 です。デフォルトは 33 です。

- [LSP Interval]：連続した IS-IS LSP 伝送の間の遅延時間をミリ秒で指定します。

  多数の IS-IS ネイバーやインターフェイスが存在するトポロジでは、LSP 送信および受信を原因とする CPU 負荷が、ASA の障害となる可能性があります。このオプションにより、LSP の送信率（および、暗黙のうちにその他のシステムの受信率）を下げることができます。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 33 です。

ステップ 10 [OK] をクリックします。

ステップ 11 [Metrics] タブで、レベル 1 とレベル 2 について以下の項目を設定します。

両方のレベルのメトリックを同じにするには、[Use the level 1 values also for level 2] チェックボックスをオンにすることができます。

- [Use maximum metric value]：リンクに割り当てるメトリックを指定します。このメトリックは、このリンクを通じてネットワーク内の他の各ルータからその他の宛先へのコストの計算に使用されます。
- [Default metric]：メトリックの番号を入力します。

  指定できる範囲は 1 ～ 16777214 です。デフォルト値は 10 です。

ステップ 12 [OK] をクリックします。

ステップ 13 [適用（Apply）] をクリックします。

IS-IS IPv4 アドレス ファミリの設定

ルータからは、他の任意のルーティング プロトコル、スタティック設定、または接続されたインターフェイスから学習した外部プレフィックスまたはルートを再配布できます。再配布されたルートはレベル 1 ルータまたはレベル 2 ルータで許可されます。

隣接関係（アジャセンシー）、最短パス優先（SPF）を設定し、IPv4 アドレスに対し、別のルーティング ドメインから ISIS（再配布）にルートを再配布するための条件を定義できます。

始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化（991 ページ）を参照してください。

ネイバーを追加しようとする前に、少なくとも 1 つのインターフェイスで IPv4 が有効になっていることを確認します。IPv4 が有効になっていない場合、ASDM によって、設定が失敗したというエラー メッセージが返されます。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv4 Address Family] > [General] を選択します。

a) 近接する IS ルータをルータによりチェックするには、[Perform adjacency check] チェックボックスをオンにします。

b) [Administrative Distance] フィールドに、IS-IS プロトコルによって検出されたルートに割り当てるディスタンスを入力します。

   アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。

distance オプションは、IS-IS ルートがルーティング情報ベース（RIB）に挿入されるときに適用されるアドミニストレーティブディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性を調整します。

c) [Maximum number of forward paths] フィールドに、ルーティング テーブルにインストールできる IS ルートの最大数を入力します。指定できる範囲は 1 ～ 8 です。

d) [Distribute default route] チェックボックスをオンにしてデフォルト ルートを配布するように IS ルーティング プロセスを設定し、ドロップダウン リストからデフォルト ルートを選択するか、[Manage] をクリックして新しいルートを作成します。新しいルートの作成手順については、ルート マップの定義 （875 ページ）を参照してください。

ステップ 2 IS-IS メトリックを設定します。

a) [Global ISIS metric for level 1] に、メトリックを指定する数値を入力します。

指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。

すべての IS-IS インターフェイスのデフォルト メトリック値を変更する必要がある場合、すべてのインターフェイスをグローバルで設定するために、[Global ISIS metric for level 1] オプションを使用することを推奨します。メトリック値がグローバルに設定されている場合、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

b) [Global ISIS metric for level 2] に、メトリックを指定する数値を入力します。

指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。

すべての IS-IS インターフェイスのデフォルト メトリック値を変更する必要がある場合、すべてのインターフェイスをグローバルで設定するために、[Global ISIS metric for level 1] オプションを使用することを推奨します。メトリック値がグローバルに設定されている場合、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

c) 次のいずれかを選択して、タイプ、長さ、および値（TLV）を設定します。

- [Send and accept both styles of TLVs during transition] チェックボックスをオンにします。
- [Use old style of TLVs with narrow metric] オプション ボタンをオンにします。
- [Use new style TLVs to carry wider metric] オプション ボタンをオンにします。

いずれかのオプション ボタンをオンにする場合は、[Accept both styles of TLVs during transition] チェックボックスもオンにできます。

新スタイルの TLV を使用することを強く推奨します。これは、LSP で IPv4 情報をアドバタイズするために使用される TLV は、拡張メトリックのみを使用するように定義されているためです。ソフトウェアは、24 ビット メトリック フィールド（ワイド メ

トリック）のサポートを提供します。新しいメトリック形式を使用すると、リンク メトリックの最大値は 16777214、総パスメトリックは 4261412864 になります。

d) [Apply metric style to] チェックボックスをオンにし、[Level-1]、[Level-2]、またはその両方のチェックボックスをオンにします。

ステップ 3 [Apply] をクリックします。

ステップ 4 **[Configuration] > [Device Setup] > [Routing] > [ISIS]> [IPv4 Address Family] > [SPF]** の順に選択します。

a) SPF 計算に外部メトリックを含めるには、[Honour external metrics during SPF calculations] チェックボックスをオンにします。

b) このデバイスを除外する場合は、[Signal other routers not to use this router as an intermediate hop in their SPF calculations] チェックボックスをオンにし、次のように設定します。

- [Specify on-startup behavior] チェックボックスをオンにして、次のいずれかを選択します。
  - **[Advertise ourself as overloaded until BGP has converged]**
  - **[Specify time to advertise ourself as overloaded after reboot]**

    [Time to advertise ourself as overloaded] フィールドに、ルータが過負荷になっていることをアドバタイズするまでに待機する秒数を入力します。値の範囲は 5 ～ 86400 秒です。

- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from other protocols when overload bit it set] チェックボックスをオンにします。
- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from another ISIS level when overload bit is set] チェックボックスをオンにします。

c) 部分ルート計算（PRC）間隔を設定します。

- [PRC Interval] フィールドに、ルータが部分ルート計算（PRC）間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- [Initial wait for PRC] フィールドに、トポロジ変更後の最初の PRC 計算遅延（ミリ秒）を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。
- [Minimum wait between first and second PRC] フィールドに、ルータが PRC 間で待機するミリ秒数を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒です。

d) レベル 1 およびレベル 2 の SPF 計算間隔を設定します。

（注） 両方のレベルに同じ値を設定する場合は、[Use level 1 values also for level 2] チェックボックスをオンにします。

- [SPF Calculation Interval] フィールドに、ルータが SPF 計算間で待機する時間数を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。

- [Initial wait for SPF calculation] フィールドに、ルータが SPF 計算を待機する時間数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
- [Minimum wait between first and second SPF calculation] フィールドに、ルータが SPF 計算間で待機するミリ秒数を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv6 Address Family] > [Redistribution] を選択します。

[Redistribution] ペインに、再配布ルートのテーブルが表示されます。

ステップ 7 新しい再配布ルートを追加するには [Add] をクリックします。テーブル内の再配布ルートを編集するには [Edit] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

a) [Source Protocol] ドロップダウン リストから、ISIS ドメインにルートを再配布するプロトコル（[BGP]、[Connected]、[EIGRP]、[OSPF]、[RIP]、または [Static]）を選択します。
b) [Process ID] ドロップダウン リストから、ソース プロトコルのプロセス ID を選択します。
c) [Route Level] ドロップダウン リストから、[Level-1]、[Level- 2]、または [Level 1-2] を選択します。
d) （オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。
e) [Metric Type] で、[internal] または [external] オプション ボタンをクリックします。
f) [Route Map] ドロップダウン リストから、再配布するネットワークをフィルタ処理するために調べる必要があるルートマップを選択するか、[Manage] をクリックして、新しいルートマップを追加するか、既存のルートマップを編集します。ルートマップの設定手順は、ルート マップの定義を参照してください。
g) [Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 8 [OK] をクリックします。

ステップ 9 [Apply] をクリックします。

接続ビットの設定

次の例では、ルータが L2 CLNS ルーティング テーブル内の 49.00aa と一致する際に接続ビットが設定されたままになります。

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
```

```
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

IS-IS IPv6 アドレス ファミリの設定

隣接関係（アジャセンシー）、SPF を設定し、IPv6 アドレスに対し、別のルーティング ドメインから IS-IS（再配布）にルートを再配布するための条件を定義できます。

始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化（991 ページ）を参照してください。

ネイバーを追加しようとする前に、少なくとも 1 つのインターフェイスで IPv6 がイネーブルになっていることを確認します。そうしないと、ASDM によって、設定が失敗したというエラー メッセージが返されます。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv6 Address Family] > [General] を選択します。

a) 近接する IS ルータをルータによりチェックするには、[Perform adjacency check] チェックボックスをオンにします。

b) [Administrative Distance] フィールドに、ルートのディスタンスを入力します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。

アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。指定できる範囲は 1 ～ 255 です。デフォルトは 1 です。

distance オプションは、IS-IS ルートがルーティング情報ベース（RIB）に挿入されるときに適用されるアドミニストレーティブディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性を調整します。

c) [Maximum number of forward paths] フィールドに、ルーティング テーブルにインストールできる IS ルートの最大数を入力します。指定できる範囲は 1 ～ 8 です。

d) [Distribute default route] チェックボックスをオンにしてデフォルト ルートを配布するように IS ルーティング プロセスを設定し、ドロップダウン リストからデフォルト ルートを選択するか、[Manage] をクリックして新しいルートを作成します。新しいルートの作成手順については、ルート マップの定義 （875 ページ）を参照してください。

ステップ 2 [Apply] をクリックします。

ステップ 3 **[Configuration] > [Device Setup] > [Routing] > [ISIS]> [IPv6 Address Family] > [SPF]** の順に選択します。

a) このデバイスを除外する場合は、[Signal other routers not to use this router as an intermediate hop in their SPF calculations] チェックボックスをオンにし、次のように設定します。

- [Specify on-startup behavior] チェックボックスをオンにして、次のいずれかを選択します。
  - **[Advertise ourself as overloaded until BGP has converged]**
  - **[Specify time to advertise ourself as overloaded after reboot]**

    [Time to advertise ourself as overloaded] フィールドに、ルータが過負荷になっていることをアドバタイズするまでに待機する秒数を入力します。値の範囲は 5 ～ 86,400 秒です。

- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from other protocols when overload bit it set] チェックボックスをオンにします。
- IP プレフィックスを除外するには、[Don't advertise IP prefixes learned from another ISIS level when overload bit is set] チェックボックスをオンにします。

b) 部分ルート計算（PRC）間隔を設定します。

- [PRC Interval] フィールドに、ルータが部分ルート計算（PRC）間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- [Initial wait for PRC] フィールドに、ルータが PRC を待機する時間数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。
- [Minimum wait between first and second PRC] フィールドに、ルータが PRC 間で待機するミリ秒数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5000 ミリ秒です。

c) レベル 1 およびレベル 2 の SPF 計算間隔を設定します。

（注） 両方のレベルに同じ値を設定する場合は、[Use level 1 values also for level 2] チェックボックスをオンにします。

- [SPF Calculation Interval] フィールドに、ルータが SPF 計算間で待機する時間数を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- [Initial wait for SPF calculation] フィールドに、ルータが SPF 計算を待機する時間数を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。

- [Minimum wait between first and second SPF calculation] フィールドに、ルータが SPF 計算間で待機するミリ秒数を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Configuration] > [Device Setup] > [Routing] > [ISIS] > [IPv6 Address Family] > [Redistribution] を選択します。

[Redistribution] ペインに、再配布ルートのテーブルが表示されます。

ステップ 6 新しい再配布ルートを追加するには [Add] をクリックします。テーブル内の再配布ルートを編集するには [Edit] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

a) [Source Protocol] ドロップダウン リストから、ISIS ドメインにルートを再配布するプロトコル（[BGP]、[Connected]、[EIGRP]、[OSPF]、[RIP]、または [Static]）を選択します。

b) [Process ID] ドロップダウン リストから、ソース プロトコルのプロセス ID を選択します。

c) [Route Level] ドロップダウン リストから、[Level-1]、[Level- 2]、または [Level 1-2] を選択します。

d) （オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。

e) [Metric Type] で、[internal] または [external] オプション ボタンをクリックして、宛先ルーティング プロトコルのメトリック タイプを指定します。

f) [Route Map] ドロップダウン リストから、再配布するネットワークをフィルタ処理するために調べる必要があるルートマップを選択するか、[Manage] をクリックして、新しいルートマップを追加するか、既存のルートマップを編集します。ルートマップの設定手順は、ルート マップの定義を参照してください。

g) [Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IS-IS の監視

次の画面を使用して、IS-IS ルーティング プロセスをモニターできます。

- [Monitoring] > [Routing] > [ISIS Neighbors] このペインには、各 IS-IS ネイバーに関する情報が表示されます。

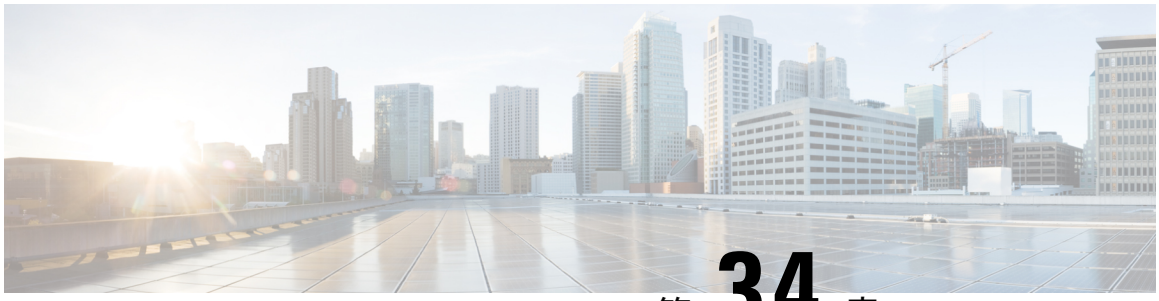
各行は 1 つの IS-IS ネイバーを表します。リストには、ネイバーごとに、システム ID、タイプ、インターフェイス、IP アドレス、状態（アクティブ、アイドルなど）、保留時間、および回路 ID が含まれます。

- [Monitoring] > [Routing] > [ISIS Rib] このペインには、ローカル IS-IS ルーティング情報ベース（RIB）テーブルが表示されます。
- [Monitoring] > [Routing] > [ISIS IPv6 Rib] このペインには、ローカル IPv6 IS-IS RIB テーブルが表示されます。

IS-IS の履歴

表 *41 : IS-IS* の機能の履歴

機能名	プラットフォームリリース	機能情報
IS-IS ルーティング	9.6(1)	ASA で Intermediate System to Intermediate System（IS-IS）のルーティング プロトコルがサポートされました。IS-IS ルーティング プロトコルを使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Routing] > [ISIS]** **[Monitoring] > [Routing] > [ISIS]**



第 34 章

EIGRP

この章では、Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

EIGRP について

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネット マスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネット マスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイバーから hello パケットを受信すると、トポロジ テーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジ テーブルを ASA に返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。**neighbor** コマンドを使用して（または ASDM で [Hello Interval] を設定して）ネイバーを設定すると、そのネイバーへ送信される hello メッセージはユニキャスト メッセージとして送信されます。ルーティング アップデートと確認応答が、ユニキャスト メッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルは、ネイバーの検出、ネイバーの回復、Reliable Transport Protocol（RTP）、およびルート計算に重要な DUAL を含む、4 の主要なアルゴリズム テクノロジーと 4 つの主要なテクノロジーを使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジ テーブルに保存します。最小コストのルートはルーティング テーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブルサクセサから別のルートが選択されます。サクセサとは、宛先への最小コスト パスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティング ループを形成しないことが保証されます。

フィジブル サクセサがトポロジ テーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブル サクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

（注） EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

EIGRP のガイドライン

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

クラスタのガイドライン

EIGRPは、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

IPv6 のガイドライン

IPv6 はサポートされません。

コンテキストのガイドライン

- デフォルトでは、共有インターフェイス間でのマルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、EIGRPインスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、EIGRP プロセスの EIGRP プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの EIGRP ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 EIGRP がサポートされています。

その他のガイドライン

- 最大 1 つの EIGRP プロセスがサポートされます。
- 設定の変更が適用されるたびに、EIGRP隣接関係のフラップが発生し、特に配布リスト、オフセットリスト、および集約への変更のネイバーからの（送信または受信された）ルーティング情報が変更されます。ルータが同期されると、EIGRPはネイバー間の隣接関係を再確立します。隣接関係が壊れて再確立されると、ネイバー間で学習されたすべてのルートが消去され、新しい配布リストを使用して、ネイバー間の同期がすべて新しく実行されます。
- また、EIGRP ネイバーの最大数にも制限はありません。ただし、不要な EIGRP フラップを防ぐために、ユニットあたりの数を 500 に制限することを推奨します。

EIGRP プロセスの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** の順に選択します。

ステップ 2 EIGRP ルーティング プロセスをイネーブルにするには、[Process Instances] タブの [Enable this EIGRP process] チェックボックスをオンにします。EIGRP のイネーブル化（1015 ページ）または EIGRP スタブ ルーティングのイネーブル化（1016 ページ）を参照してください。

ステップ 3 [Setup] > [Networks] タブで、EIGRP ルーティングに参加するネットワークとインターフェイスを定義します。詳細については、「EIGRP ルーティング プロセスのネットワークの定義（1018 ページ）」を参照してください。

ステップ 4 （任意）[Filter Rules] ペインでルート フィルタを定義します。ルート フィルタにより、EIGRP 更新で送受信することを許可されているルートをより細かく制御できます。詳細については、「EIGRP でのネットワークのフィルタリング（1026 ページ）」を参照してください。

ステップ 5 （任意）[Redistribution] ペインでルート再配布を定義します。

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。詳細については、「EIGRP へのルート再配布（1024 ページ）」を参照してください。

ステップ 6 （任意）[Static Neighbor] ペインでスタティック EIGRP ネイバーを定義します。

詳細については、「EIGRP ネイバーの定義（1023 ページ）」を参照してください。

ステップ 7 （任意）[Summary Address] ペインで、サマリー アドレスを定義します。

サマリー アドレスの定義の詳細については、インターフェイスでのサマリー集約アドレスの設定（1020 ページ）を参照してください。

ステップ 8 （任意）[Interfaces] ペインで、インターフェイス固有の EIGRP パラメータを定義します。これらのパラメータには、EIGRP メッセージ認証、保持時間、hello 間隔、遅延メトリック、スプリットホライズンの使用などがあります。詳細については、「EIGRP のインターフェイスの設定（1018 ページ）」を参照してください。

ステップ 9 （任意）[Default Information] ペインで、EIGRP 更新でのデフォルト ルート情報の送受信を制御します。デフォルトでは、デフォルト ルートが送信され、受け入れられます。詳細については、EIGRP でのデフォルト情報の設定（1030 ページ）を参照してください。

EIGRP の設定

この項では、システムでEIGRPプロセスをイネーブルにする方法について説明します。EIGRPをイネーブルにした後に、システムで EIGRP プロセスをカスタマイズする方法については、次の項を参照してください。

EIGRP のイネーブル化

ASA でイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

メインの [EIGRP Setup] ペインには、EIGRP をイネーブルにするための次の 3 つのタブがあります。

- [Process Instances] タブでは、各コンテキストの EIGRP ルーティング プロセスをイネーブルにすることができます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。詳細については、EIGRP のイネーブル化 （1015 ページ）と EIGRP スタブ ルーティングのイネーブル化 （1016 ページ）を参照してください。
- [Networks] タブでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。詳細については、「EIGRP ルーティング プロセスのネットワークの定義 （1018 ページ）」を参照してください。
- [Passive Interfaces] タブでは、1 つ以上のインターフェイスをパッシブ インターフェイスとして設定できます。EIGRP では、パッシブ インターフェイスはルーティング アップデートの送受信を行いません。[Passive Interface] テーブルには、パッシブ インターフェイスとして定義されているインターフェイスが一覧表示されます。

ステップ 2 [Enable this EIGRP process] チェックボックスをオンにします。

デバイスでイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。変更を保存できるようにするには、ルーティング プロセスの自律システム（AS）番号を [EIGRP Process] フィールドに入力する必要があります。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 （任意）EIGRP プロセスの設定を指定するには、[Advanced] をクリックします。指定できる設定には、ルータ ID、デフォルトのメトリック、スタブ ルーティング、ネイバー変更、EIGRP ルートのアドミニストレーティブ ディスタンスなどがあります。

ステップ 5 [Networks] タブをクリックします。

ステップ 6 新しいネットワーク エントリを追加するには、[Add] をクリックします。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択して [Delete] をクリックします。

ステップ 7 ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 8 [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注） ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 9 [Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 10 [OK] をクリックします。

EIGRP スタブ ルーティングのイネーブル化

ASA を EIGRP スタブ ルータとしてイネーブル化し、設定することができます。スタブ ルーティングを使用すると、ASA で必要となるメモリおよび処理要件を減らすことができます。ASA をスタブ ルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティング テーブルを維持する必要がなくなります。一般に、配布ルータからスタブ ルートに送信する必要があるのは、デフォルト ルートだけです。

スタブ ルータから配布ルータには、指定されたルートだけが伝搬されます。スタブ ルータである ASA は、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブ ルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブ ルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブ ルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 EIGRP スタブ ルーティング プロセスを設定するには、[Advanced] をクリックします。

[Edit EIGRP Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 5 [Edit EIGRP Process Advanced Properties] ダイアログボックスの [Stub] 領域で、次の EIGRP スタブ ルーティング プロセスのうち 1 つ以上を選択します。

- [Stub Receive only]：隣接ルータからルート情報を受信しても、それらの隣接ルータにルート情報を送信しない EIGRP スタブ ルーティング プロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。
- [Stub Connected]：接続済みルートをアドバタイズします。
- [Stub Static]：スタティック ルートをアドバタイズします。
- [Stub Redistributed]：再配布ルートをアドバタイズします。
- [Stub Summary]：サマリー ルートをアドバタイズします。

ステップ 6 [OK] をクリックします。

ステップ 7 [Networks] タブをクリックします。

ステップ 8 [Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 9 ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 10 [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注） ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 11 [Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 12 [OK] をクリックします。

EIGRP のカスタマイズ

ここでは、EIGRP ルーティングをカスタマイズする方法について説明します。

EIGRP ルーティング プロセスのネットワークの定義

[Network] テーブルでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。

[Network] テーブルには、EIGRP ルーティング プロセス用に設定されているネットワークが表示されます。このテーブルの各行には、指定した EIGRP ルーティング プロセス用に設定されているネットワーク アドレスおよび関連するマスクが表示されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 [Networks] タブをクリックします。

ステップ 5 [Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 6 ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 7 [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注） ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 8 [Network Mask] フィールドに、IP アドレスに適用するネットワーク マスクを入力します。

ステップ 9 [OK] をクリックします。

EIGRP のインターフェイスの設定

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、インターフェイスが接続されているネットワークが対象に含まれるようにASAを設定し、そのインターフェイスがEIGRPアップデートを送受信しないようにします。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Interfaces]** の順に選択します。

[Interface] ペインが表示され、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、インターフェイスごとに次の設定を修正できます。

- 認証キーとモード。
- EIGRP hello 間隔と保持時間。
- EIGRP メトリックの計算で使用されるインターフェイス遅延メトリック。
- インターフェイスでのスプリットホライズンの使用。

ステップ 5 インターフェイス エントリを選択するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 6 [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 7 [Hello Interval] フィールドに、インターフェイス上で送信される EIGRP hello パケット間の間隔を入力します。

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。

ステップ 8 [Hold Time] フィールドに、保持時間を秒単位で入力します。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。

ステップ 9 [Split Horizon] の [Enable] チェックボックスをオンにします。

ステップ 10 [Delay] フィールドに、遅延の値を入力します。遅延時間は 10 マイクロ秒単位です。有効値の範囲は 1 ～ 16777215 です。

ステップ 11 [Enable MD5 Authentication] チェックボックスをオンにして、EIGRP プロセス メッセージの MD5 認証をイネーブルにします。

ステップ 12 [Key] または [Key ID] の値を入力します。

- [Key] フィールドに、EIGRP 更新を認証するキーを入力します。このキーには、最大 16 文字を含めることができます。
- [Key ID] フィールドに、キー ID 値を入力します。有効値の範囲は、1 ～ 255 です。

ステップ 13 [OK] をクリックします。

パッシブ インターフェイスの設定

1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。ASDM の [Passive Interface] テーブルには、パッシブ インターフェイスとして設定されているインターフェイスが一覧表示されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 [Passive Interfaces] タブをクリックします。

ステップ 5 設定するインターフェイスをドロップダウン リストから選択します。

ステップ 6 [Suppress routing updates on all interfaces] チェックボックスをオンにすると、すべてのインターフェイスがパッシブとして指定されます。[Passive Interface] テーブルに表示されていないインターフェイスも、このチェックボックスがオンのときはパッシブとして設定されます。

ステップ 7 パッシブ インターフェイス エントリを追加するには [Add] をクリックします。

[Add EIGRP Passive Interface] ダイアログボックスが表示されます。パッシブにするインターフェイスを選択して [Add] をクリックします。パッシブ インターフェイスを削除するには、テーブルでそのインターフェイスを選択して [Delete] をクリックします。

ステップ 8 [OK] をクリックします。

インターフェイスでのサマリー集約アドレスの設定

サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Interfaces]** の順に選択します。

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに修正できます。これらの設定の詳細については、EIGRP のインターフェイスの設定（1018 ページ）を参照してください。

ステップ 2 インターフェイスの EIGRP パラメータを設定するには、インターフェイス エントリをダブルクリックするか、そのエントリを選択して [Edit] をクリックします。

ステップ 3 [OK] をクリックします。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Summary Address]** の順に選択します。

[Summary Address] ペインには、スタティックに定義された EIGRP サマリー アドレスのテーブルが表示されます。デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。[Summary Address] ペインでは、サブネット レベルに集約されるスタティックに定義された EIGRP サマリー アドレスを作成できます。

ステップ 5 新しい EIGRP サマリー アドレスを追加するには [Add] をクリックし、テーブル内の既存の EIGRP サマリー アドレスを編集するには [Edit] をクリックします。

[Add Summary Address] または [Edit Summary Address] ダイアログボックスが表示されます。テーブルのエントリをダブルクリックして編集することもできます。

ステップ 6 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 7 [Interface] ドロップダウン リストで、どのインターフェイスからこのサマリー アドレスをアドバタイズするかを選択します。

ステップ 8 [IP Address] フィールドに、サマリー ルートの IP アドレスを入力します。

ステップ 9 [Netmask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択または入力します。

ステップ 10 ルートのアドミニストレーティブ ディスタンスを [Administrative Distance] フィールドに入力します。空白のままにすると、ルートのアドミニストレーティブ ディスタンスはデフォルト値の 5 になります。

ステップ 11 [OK] をクリックします。

インターフェイス遅延値の変更

インターフェイス遅延値は、EIGRP ディスタンス計算で使用されます。この値は、インターフェイスごとに変更できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Interfaces]** の順に選択します。

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、設定をインターフェイスごとに変更できます。これらの設定の詳細については、EIGRP のインターフェイスの設定（1018 ページ）を参照してください。

ステップ 2 インターフェイスの EIGRP パラメータの遅延値を設定するには、インターフェイス エントリをダブルクリックするか、インターフェイス エントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 3 [Delay] フィールドに、遅延時間を 10 マイクロ秒単位で入力します。有効な値は、1 ～ 16777215 です。

ステップ 4 [OK] をクリックします。

インターフェイスでの EIGRP 認証のイネーブル化

EIGRP ルート認証では、EIGRP ルーティング プロトコルからのルーティング アップデートに対する MD5 認証を提供します。MD5 キーを使用したダイジェストが各 EIGRP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。

EIGRP ルート認証は、インターフェイスごとに設定します。EIGRP メッセージ認証対象として設定されたインターフェイス上にあるすべての EIGRP ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

（注） EIGRP ルート認証をイネーブルにするには、事前に EIGRP をイネーブルにする必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** を選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 [Networks] タブをクリックします。

ステップ 5 [Add] をクリックして、新しいネットワーク エントリを追加します。

[Add EIGRP Network] ダイアログボックスが表示されます。ネットワーク エントリを削除するには、テーブルでそのエントリを選択し、[Delete] をクリックします。

ステップ 6 ドロップダウン リストから、EIGRP ルーティング プロセスの AS 番号を選択します。

ステップ 7 [IP Address] フィールドに、EIGRP ルーティング プロセスに参加するネットワークの IP アドレスを入力します。

（注） ネットワーク エントリを変更するには、まずそのエントリを削除してから新しいエントリを追加する必要があります。既存のエントリは編集できません。

ステップ 8 [Network Mask] フィールドで、IP アドレスに適用されるネットワーク マスクを選択するか入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Interfaces]** の順に選択します。

[Interface] ペインには、EIGRP インターフェイスの設定が表示されます。[Interface Parameters] テーブルには、ASA のすべてのインターフェイスが表示され、インターフェイスごとに設定を修正できます。これらの設定の詳細については、EIGRP のインターフェイスの設定（1018 ページ）を参照してください。

ステップ 11 [Enable MD5 Authentication] チェックボックスをオンにして、EIGRP プロセス メッセージの MD5 認証をイネーブルにします。このチェックボックスをオンにした後で、次のいずれかを指定します。

- [Key] フィールドに、EIGRP 更新を認証するキーを入力します。このキーの最大長は 16 文字です。
- [Key ID] フィールドに、キー ID 値を入力します。有効値の範囲は、1 ～ 255 です。

ステップ 12 [OK] をクリックします。

EIGRP ネイバーの定義

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Static Neighbor]** の順に選択します。

[Static Neighbor] ペインが開き、スタティックに定義された EIGRP ネイバーが表示されます。EIGRP ネイバーは、ASA との間で EIGRP ルーティング情報を送受信します。通常は、ネイバー探索プロセスによってネイバーがダイナミックに検出されます。ただし、ポイントツーポイントの非ブロードキャストネットワークでは、ネイバーをスタティックに定義する必要があります。

[Static Neighbor] テーブルの各行には、ネイバーの EIGRP 自律システム番号、ネイバー IP アドレス、およびネイバーに接続するためのインターフェイスが表示されます。

[Static Neighbor] ペインでは、スタティック ネイバーを追加または編集できます。

ステップ 5 EIGRP スタティック ネイバーを追加または編集するには、[Add] または [Edit] をクリックします。

[Add EIGRP Neighbor Entry] または [Edit EIGRP Neighbor Entry] ダイアログボックスが表示されます。

ステップ 6 ネイバーを設定する EIGRP プロセスのドロップダウン リストで EIGRP AS 番号を選択します。

ステップ 7 [Interface Name] ドロップダウン リストからインターフェイス名を選択します。このインターフェイスを通してネイバーが使用可能になります。

ステップ 8 ネイバーの IP アドレスを [Neighbor IP Address] フィールドに入力します。

ステップ 9 [OK] をクリックします。

EIGRP へのルート再配布

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。接続されているルートが、EIGRP コンフィギュレーション内の **network** 文で指定された範囲に含まれている場合、再配布する必要はありません。

（注） RIP 限定：この手順を開始する前に、ルート マップを作成し、指定されたルーティング プロトコルのうち RIP ルーティング プロセスに再配布されるルートを詳細に定義する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Redistribution]** の順に選択します。

[Redistribution] ペインには、他のルーティング プロトコルから EIGRP ルーティング プロセスにルートを再配布するためのルールが表示されます。スタティック ルートや接続済みルートを EIGRP ルーティング プロセスに再配布する場合は、メトリックの設定は必須ではありませんが、設定することを推奨します。[Redistribution] ペインのテーブルの各行に、1 つのルート再配布エントリが表示されます。

ステップ 5 新しい再配布ルールを追加するには、[Add] をクリックします。既存の再配布ルールを編集する場合は、ステップ 6 に進んでください。

[Add EIGRP Redistribution Entry] ダイアログボックスが表示されます。

ステップ 6 既存の EIGRP スタティック ネイバーを編集するには、テーブル内のアドレスを選択して [Edit] をクリックします。テーブル内のエントリをダブルクリックするという方法でも、そのエントリを編集できます。

[Edit EIGRP Redistribution Entry] ダイアログボックスが表示されます。

ステップ 7 このエントリが適用される EIGRP ルーティング プロセスの AS 番号をドロップダウン リストで選択します。

ステップ 8 [Protocol] 領域で、ルーティング プロセスのプロトコルとして次のいずれかを選択してそのオプション ボタンをクリックします。

- [Static] を選択すると、スタティック ルートが EIGRP ルーティング プロセスに再配布されます。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [Connected] を選択すると、接続されているルートが EIGRP ルーティング プロセスに再配布されます。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。
- [RIP] を選択すると、RIP ルーティング プロセスで検出されたルートが EIGRP に再配布されます。
- [OSPF] を選択すると、OSPF ルーティング プロセスで検出されたルートが EIGRP に再配布されます。

ステップ 9 [Optional Metrics] 領域で、再配布されるルートに使用するメトリックとして次のいずれかを選択します。

- [Bandwidth] は EIGRP 帯域幅メトリックで、単位はキロビット/秒です。有効値の範囲は 1 ～ 4294967295 です。
- [Delay] は EIGRP 遅延メトリックで、単位は 10 マイクロ秒です。有効値の範囲は、0 ～ 4294967295 です。
- [Reliability] は EIGRP 信頼性メトリックです。有効値の範囲は 0 ～ 255 で、255 は信頼性が 100 % であることを示します。
- [Loading] は EIGRP 有効帯域幅（負荷）メトリックです。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。
- [MTU] はパスの MTU です。有効値の範囲は 1 ～ 65535 です。

ステップ 10 ルート マップを [Route Map] ドロップダウン リストで選択し、EIGRP ルーティング プロセスに再配布するルートを定義します。ルート マップの設定方法の詳細については、ルート マップ （873 ページ）を参照してください。

ステップ 11 [Optional OSPF Redistribution] 領域で、どの OSPF ルートを EIGRP ルーティング プロセスに再配布するかをさらに詳しく指定するために、次の OSPF オプション ボタンのいずれかをクリックします。

- [Match Internal] を選択すると、指定されている OSPF プロセスの内部であるルートが対象となります。
- [Match External 1] を選択すると、指定されている OSPF プロセスの外部であるタイプ 1 ルートが対象となります。
- [Match External 2] を選択すると、指定されている OSPF プロセスの外部であるタイプ 2 ルートが対象となります。
- [Match NSSA-External 1] を選択すると、指定されている OSPF NSSA の外部であるタイプ 1 ルートが対象となります。
- [Match NSSA-External 2] を選択すると、指定されている OSPF NSSA の外部であるタイプ 2 ルートが対象となります。

ステップ 12 [OK] をクリックします。

EIGRP でのネットワークのフィルタリング

（注） この手順を開始する前に、標準の ACL を作成し、その中にアドバタイズするルートを定義する必要があります。つまり、標準の ACL を作成し、その中に送信または受信したアップデートからフィルタリングするルートを定義します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [EIGRP Process] フィールドに、EIGRP プロセスの AS 番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Filter Rules]** の順に選択します。

EIGRP ルーティング プロセスに対して設定されているルート フィルタリング ルールが [Filter Rules] ペインに表示されます。フィルタ ルールによって、EIGRP ルーティング プロセスで受け入れまたはアドバタイズされるルートを制御できます。

[Filter Rule] テーブルの各行には、特定のインターフェイスまたはルーティング プロトコルに適用されるフィルタ ルールについての情報が記載されます。たとえば、フィルタ ルールで外部インターフェイスでの「in」方向が指定されている場合は、外部インターフェイスで受信された EIGRP アップデートすべてにフィルタリングが適用されます。フィルタ ルールで方向が「out」、ルーティング プロトコルとして OSPF 10 が指定されている場合は、発信 EIGRP アップデートで EIGRP ルーティング プロセスに再配布されるルートにフィルタ ルールが適用されます。

ステップ 5 フィルタ ルールを追加するには [Add] をクリックします。既存のフィルタ ルールを編集する場合は、ステップ 6 に進んでください。

[Add Filter Rules] ダイアログボックスが表示されます。

ステップ 6 フィルタ ルールを編集するには、テーブルでそのフィルタ ルールを選択して [Edit] をクリックします。

[Edit Filter Rules] ダイアログボックスが表示されます。フィルタ ルールをダブルクリックして編集することもできます。フィルタ ルールを削除するには、テーブルでそのフィルタ ルールを選択して [Delete] をクリックします。

ステップ 7 このエントリが適用される EIGRP ルーティング プロセスの AS 番号をドロップダウン リストで選択します。

ステップ 8 フィルタ ルートの方向をドロップダウン リストで選択します。

着信 EIGRP ルーティング アップデートからのルートをフィルタリングするルールの場合は、[in] を選択します。ASA から送信される EIGRP ルーティング アップデートからのルートをフィルタリングするには、[out] を選択します。

[out] を選択した場合、[Routing process] フィールドがアクティブになります。フィルタリングするルートのタイプを選択します。スタティック、接続済み、RIP、および OSPF のルーティング プロセスから再配布されるルートをフィルタリングできます。ルーティング プロセスを指定するフィルタは、すべてのインターフェイスで送信される更新からのルートをフィルタリングします。

ステップ 9 OSPF プロセス ID を [ID] フィールドに入力します。

ステップ 10 [Interface] オプション ボタンをクリックしてから、フィルタを適用するインターフェイスを選択します。

ステップ 11 [Add] または [Edit] をクリックして、フィルタ ルールの ACL を定義します。[Edit] をクリックすると、選択されているネットワーク ルールの [Network Rule] ダイアログボックスが開きます。

ステップ 12 [Action] ドロップダウン リストで、[Permit] を選択すると指定のネットワークのアドバタイズが許可され、[Deny] を選択すると指定のネットワークのアドバタイズが禁止されます。

ステップ 13 [IP Address] フィールドに、許可または禁止するネットワークの IP アドレスを入力します。すべてのアドレスを許可または禁止するには、IP アドレス **0.0.0.0** とネットワーク マスク **0.0.0.0** を使用します。

ステップ 14 [Netmask] ドロップダウン リストで、ネットワークの IP アドレスに適用するネットワーク マスクを選択します。このフィールドにネットワークマスクを入力するか、リストから共通マスクの 1 つを選択します。

ステップ 15 [OK] をクリックします。

EIGRP Hello 間隔と保持時間のカスタマイズ

ASA は、ネイバーを検出する目的、およびネイバーが到達不能または動作不能になったことを把握する目的で、定期的に hello パケットを送信します。デフォルトでは、hello パケットは 5 秒間隔で送信されます。

hello パケットは、ASA の保持時間をアドバタイズします。保持時間によって、EIGRP ネイバーに、ASA を到達可能と見なす時間の長さを知らせます。アドバタイズされた保持時間内にネイバーが hello パケットを受信しなかった場合、ASA は到達不能と見なされます。デフォルトでは、アドバタイズされる保持時間は 15 秒です（hello 間隔の 3 倍）。

hello 間隔とアドバタイズされる保持時間のいずれも、インターフェイスごとに設定します。保持時間は hello 間隔の 3 倍以上に設定することをお勧めします。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Interfaces]** の順に選択します。

[Interface] ペインに、EIGRP インターフェイスのすべての設定が表示されます。

ステップ 5 インターフェイス エントリをダブル クリックするか、またはエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 6 EIGRP AS 番号をドロップダウン リストで選択します。このリストに表示されるのは、EIGRP ルーティング プロセスをイネーブルにしたときに設定されていたシステム番号です。

ステップ 7 [Hello Interval] フィールドに、インターフェイス上で送信される EIGRP hello パケット間の間隔を入力します。

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。

ステップ 8 [Hold Time] フィールドで、保持時間を秒単位で指定します。

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。

ステップ 9 [OK] をクリックします。

自動ルート集約の無効化

自動ルート集約は、デフォルトでイネーブルになっています。EIGRP ルーティング プロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加しているとすると、EIGRP ルーティング プロセスはそれらのルートに対しサマリー アドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリーアドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [Process Instance] タブをクリックします。

ステップ 4 [Advanced] をクリックします。

ステップ 5 [Summary] 領域の [Auto-Summary] チェックボックスをオフにします。

（注） この設定はデフォルトでイネーブルになっています。

ステップ 6 [OK] をクリックします。

EIGRP でのデフォルト情報の設定

EIGRP アップデート内のデフォルト ルート情報の送受信を制御できます。デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルト ルート ビット設定が無効になります。

ASDM では、[Default Information] ペインに、EIGRP アップデートでのデフォルト ルート情報の送受信を制御するルールのテーブルが表示されます。EIGRP ルーティング プロセスごとに、「in」ルールと「out」ルールを 1 つずつ設定できます（現在は 1 つのプロセスだけがサポートされています）。

デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルトのルート情報の送受信を制限またはディセーブルにするには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

メインの [EIGRP Setup] ペインが表示されます。

ステップ 2 [Enable EIGRP routing] チェックボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 次のいずれかを実行します。

- [Add] をクリックして、新しいエントリを作成します。
- エントリを編集するには、テーブル内のエントリをダブルクリックするか、テーブル内のエントリを選択して [Edit] をクリックします。

  そのエントリの [Add Default Information] または [Edit Default Information] ダイアログボックスが表示されます。EIGRP AS 番号が [EIGRP] フィールドで自動的に選択されています。

ステップ 5 [Direction] フィールドで、ルールの方向として次のオプションのいずれかを選択します。

- [in]：このルールは、着信 EIGRP アップデートからのデフォルト ルート情報をフィルタリングします。
- [out]：このルールは、発信 EIGRP アップデートからのデフォルト ルート情報をフィルタリングします。

EIGRP プロセスごとに、「in」ルールと「out」ルールを 1 つずつ設定できます。

ステップ 6 ネットワーク ルール テーブルにネットワーク ルールを追加します。ネットワーク ルールでは、デフォルト ルート情報を送受信するときに許可されるネットワークと拒否されるネットワークを定義します。デフォルト情報フィルタ ルールに追加するネットワーク ルールごとに、次の手順を繰り返します。

a) ネットワーク ルールを追加するには [Add] をクリックします。既存のネットワーク ルールをダブルクリックしてルールを編集します。

b) [Action] フィールドで、そのネットワークを許可する場合は [Permit] をクリックし、ブロックする場合は [Deny] をクリックします。

c) [IP Address] フィールドと [Network Mask] フィールドに、ルールによって許可または拒否されるネットワークの IP アドレスとネットワーク マスクを入力します。

すべてのデフォルト ルート情報の受け入れや送信を拒否するには、ネットワーク アドレスとして **0.0.0.0** を入力し、ネットワーク マスクとして **0.0.0.0** を選択します。

d) 指定したネットワーク ルールをデフォルト情報フィルタ ルールに追加するには、[OK] をクリックします。

ステップ 7 デフォルト情報フィルタ ルールを受け入れるには、[OK] をクリックします。

EIGRP スプリット ホライズンのディセーブル化

スプリット ホライズンは、EIGRP アップデート パケットとクエリー パケットの送信を制御します。スプリット ホライズンがインターフェイスでイネーブルになると、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップとなる宛先には送信されません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループが発生する可能性が低くなります。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンは、ルート情報が、その情報の発信元となるインターフェイスからルータによってアドバタイズされないようにします。通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワークでは、この動作が望ましくない場合があります。このような場合は、EIGRP を設定したネットワークを含め、スプリット ホライズンをディセーブルにする必要が生じることもあります。

インターフェイスでのスプリット ホライズンをディセーブルにする場合、そのインターフェイス上のすべてのルータとアクセス サーバーに対してディセーブルにする必要があります。

EIGRP スプリット ホライズンをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interfaces]** の順に選択します。

[Interface] ペインが表示され、EIGRP インターフェイスの設定が表示されます。

ステップ 2 インターフェイス エントリをダブル クリックするか、またはエントリを選択して [Edit] をクリックします。

[Edit EIGRP Interface Entry] ダイアログボックスが表示されます。

ステップ 3 EIGRP 自律システム（AS）番号をドロップダウン リストで選択します。このリストに表示されるのは、EIGRP ルーティング プロセスをイネーブルにしたときに設定されていたシステム番号です。

ステップ 4 [Split Horizon] チェックボックスをオフにします。

ステップ 5 [OK] をクリックします。

EIGRP プロセスの再始動

EIGRPプロセスを再始動したり、再配布またはカウンタをクリアしたりすることができます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[EIGRP]** > **[Setup]** の順に選択します。

[EIGRP Setup] ペインが表示されます。

ステップ 2 [リセット（Reset）] をクリックします。

EIGRP のモニターリング

次のコマンドを使用して、EIGRP ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンドリファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな EIGRP ルーティング統計情報をモニターまたはディセーブル化するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[EIGRP Neighbor]** の順に選択します。

各行は 1 つの EIGRP ネイバーを表します。ネイバーごとに、リストにはその IP アドレス、接続先のネットワーク、保持時間、アップタイム、キュー長、シーケンス番号、スムーズラウン

ドトリップ時間、再送信タイムアウトが表示されます。考えられる状態変更のリストは次のとおりです。

- [NEW ADJACENCY]：新しいネイバーが確立されました。
- [PEER RESTARTED]：他のネイバーがネイバー関係のリセットを開始しました。メッセージを受け取ったルータは、ネイバーをリセットしているルータではありません。
- [HOLD TIME EXPIRED]：保持時間が経過しても、ルータは EIGRP パケットをネイバーから受け取っていません。
- [RETRY LIMIT EXCEEDED]：EIGRP は EIGRP 高信頼性パケットに対する確認応答をネイバーから受け取らなかったため、高信頼性パケットの再送信をすでに 16 回試行しましたが、一度も成功しませんでした。
- [ROUTE FILTER CHANGED]：ルート フィルタに変更があったため、EIGRP ネイバーがリセットしています。
- [INTERFACE DELAY CHANGED]：インターフェイスでの遅延パラメータの手動設定変更があったため、EIGRP ネイバーがリセットしています。
- [INTERFACE BANDWIDTH CHANGED]：インターフェイスでのインターフェイス帯域幅の手動設定変更があったため、EIGRP ネイバーがリセットしています。
- [STUCK IN ACTIVE]：EIGRP がアクティブ状態のままスタックしているため、EIGRP ネイバーがリセットしています。ネイバーがリセットされるのは、stuck-in-active 状態となったためです。

ステップ 2 モニターする EIGRP ネイバーをクリックします。

ステップ 3 現在のネイバー リストを削除するには、[Clear Neighbors] をクリックします。

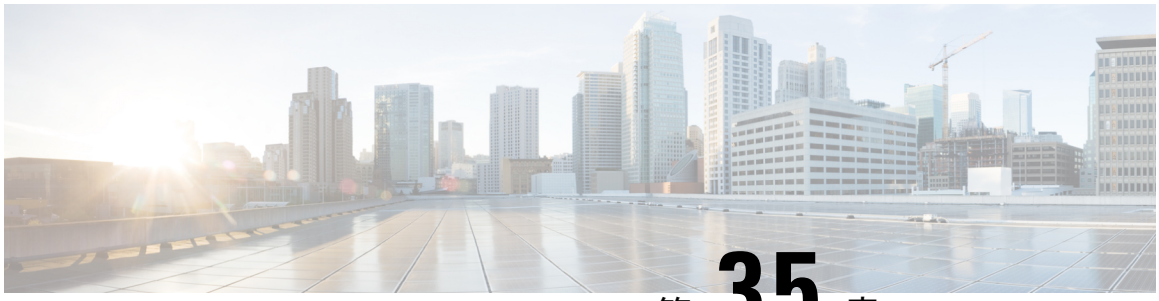
ステップ 4 現在のネイバー リストの表示を更新するには、[Refresh] をクリックします。

（注） デフォルトでは、ネイバー変更メッセージとネイバー警告メッセージはロギングされます。

EIGRP の履歴

表 *42 : EIGRP* の機能の履歴

機能名	プラットフォームリリース	機能情報
EIGRP サポート	7.0(1)	Enhanced Interior Gateway Routing Protocol（EIGRP）を使用するデータのルーティング、認証の実行、およびルーティング情報の再配布とモニターリングのサポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [EIGRP]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	EIGRP ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup]。
クラスタ	9.0(1)	EIGRP の場合、バルク同期、ルートの同期およびレイヤ 2 ロードバランシングは、クラスタリング環境でサポートされます。
EIGRP Auto-Summary	9.2(1)	EIGRP の [Auto-Summary] フィールドはデフォルトでディセーブルになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Setup] > [Edit EIGRP Process Advanced Properties]



第 35 章

マルチキャスト ルーティング

この章では、マルチキャスト ルーティング プロトコルを使用するように Cisco Secure Firewall ASA を設定する方法について説明します。

マルチキャスト ルーティングについて

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、送信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャスト プロトコルを使用した Secure Firewall ASA によりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

Secure Firewall ASA は、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つの Secure Firewall ASA に両方を同時に設定することはできません。

（注） マルチキャスト ルーティングでは、UDP トランスポートおよび非 UDP トランスポートの両方がサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、Secure Firewall ASA は IGMP のプロキシ エージェントとして動作します。Secure Firewall ASA は、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、Secure Firewall ASA を PIM スパース モードまたは双方向モード用に設定できません。IGMP スタブ マルチキャスト ルーティングに参加するインターフェイス上で PIM を有効にする必要があります。

Secure Firewall ASA は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイント（RP）に転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルト ルートが RP に提供されます。

（注） Secure Firewall ASAが PIM RP の場合は、Secure Firewall ASAの変換されていない外部アドレスを RP アドレスとして使用してください。

PIM Source Specific Multicast のサポート

Secure Firewall ASAは PIM Source Specific Multicast（SSM）の機能や関連設定をサポートしていません。ただし、Secure Firewall ASAは最終ホップ ルータとして配置されていない限り、SSM 関連のパケットの通過を許可します。

SSMは、IPTVなどの1対多のアプリケーションのデータ送信メカニズムとして分類されます。SSM モデルは、（S、G）ペアで示される「チャネル」の概念を使用します。S は発信元アドレス、GはSSM宛先アドレスです。チャネルに登録するには、IGMPv3などのグループ管理プロトコルを使用して行います。SSMは、特定のマルチキャスト送信元について学習した後、受信側のクライアントを有効にします。これにより、共有ランデブー ポイント（RP）からではなく、直接送信元からマルチキャスト ストリームを受信できるようになります。アクセス制御メカニズムは SSM 内に導入され、現在のスパースまたはスパース - デンス モードの実装では提供されないセキュリティ拡張機能を提供します。

PIM-SSM は、RP または共有ツリーを使用しない点で PIM-SM とは異なります。代わりに、マルチキャスト グループの発信元アドレスの情報は、ローカル受信プロトコル（IGMPv3）経由で受信者から提供され、送信元固有のツリーを直接作成するために使用されます。

PIM ブートストラップ ルータ（BSR）

PIM ブートストラップ ルータ（BSR）は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント（RP）セレクションモデルです。RP機能には RP の検出が含まれており、RP にデフォルト ルートを提供します。これは、一連のデバイスをBSR の選択プロセスに参加する候補の BSR（C-BSR）として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブー ポイント（C-RP）として設定されたデバイスは、選定された BSR にグループ マッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経由で、マルチキャスト ツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

この機能は、RP を動的に学習する方法を提供するため、RP が停止と起動を繰り返す複雑で大規模なネットワークには不可欠です。

PIM ブートストラップ ルータ（BSR）の用語

PIM BSR の設定では、次の用語がよく使用されます。

- ブートストラップ ルータ（BSR）：BSR はホップバイホップ ベースの PIM が設定された他のルータに、ランデブー ポイント（RP）情報をアドバタイズします。選択プロセスの後に、複数の候補 BSR の中から 1 つの BSR が選択されます。このブートストラップ ルータの主な目的は、すべての候補 RP（C-RP）通知を RP-set というデータベースに収集し、これをネットワーク内の他のすべてのルータに定期的に BSR メッセージとして送信することです（60 秒ごと）。
- ブートストラップ ルータ（BSR）メッセージ：BSR メッセージは、TTL が 1 に設定された All-PIM-Routers グループへのマルチキャストです。これらのメッセージを受信するすべての PIM ネイバーは、メッセージを受信したインターフェイスを除くすべてのインターフェイスからそのメッセージを再送信します（TTL は 1 に設定）。BSR メッセージには、現在アクティブな BSR の RP-set と IP アドレスが含まれています。この方法で、C-RP は C-RP メッセージのユニキャスト先を認識します。
- 候補ブートストラップ ルータ（C-BSR）：候補 BSR として設定されるデバイスは、BSR 選択メカニズムに参加します。最も優先順位の高い C-BSR が BSR として選択されます。C-BSR の最上位の IP アドレスはタイブレイカーとして使用されます。BSR の選択プロセスはプリエンプティブです。たとえば、より優先順位の高い C-BSR が新たに見つかると、新しい選択プロセスがトリガーされます。
- 候補ランデブーポイント（C-RP）：RP はマルチキャストデータの送信元と受信者が対面する場所として機能します。C-RP として設定されているデバイスは、マルチキャスト グループ マッピング情報を、ユニキャスト経由で直接、選択された BSR に定期的にアドバタイズします。これらのメッセージには、グループ範囲、C-RP アドレス、および保留時間が含まれています。現在の BSR の IP アドレスは、ネットワーク内のすべてのルータが

受信した定期的な BSR メッセージから学習されます。このようにして、BSR は現在動作中で到達可能な RP 候補について学習します。

(注) C-RP は BSR トラフィックの必須要件ですが、Secure Firewall ASA は C-RP としては機能しません。ルータのみが C-RP として機能できます。したがって、BSR のテスト機能では、トポロジにルータを追加する必要があります。

- BSR 選択メカニズム：各 C-BSR は、BSR 優先順位フィールドを含むブートストラップ メッセージ（BSM）を生成します。ドメイン内のルータは、ドメイン全体に BSM をフラッディングします。自身より優先順位の高い C-BSR に関する情報を受け取った BSR は、一定期間、BSM の送信を抑止します。残った単一の C-BSR が選択された BSR となり、その BSM により、選択された BSR に関する通知がドメイン内の他のすべてのルータに対して送信されます。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMP を使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。マルチキャスト グループの設定方法の詳細については、マルチキャスト グループの設定 （1052 ページ）を参照してください。

マルチキャスト アドレス

マルチキャスト アドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタリング

マルチキャスト ルーティングは、クラスタリングをサポートします。スパンド EtherChannel クラスタリングでは、ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを送信します。ファーストパス転送が確立されると、データユニットがマルチキャスト データ パケットを転送できます。すべてのデータ フローは、フル フローです。スタブ転送フローもサポートされます。スパンド EtherChannel クラスタリングでは 1 つのユニットだけがマルチキャストパケットを受信するため、制御ユニットへのリダイレクションは共通です。 個別インターフェイス クラスタリングでは、ユニットは個別に機能しません。すべてのデータとルーティングパケットは制御ユニットで処理され、転送されます。データユニットは、送信されたすべてのパケットをドロップします。

マルチキャスト ルーティングのガイドライン

コンテキスト モード

シングル コンテキスト モードでサポートされています。

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6

IPv6 はサポートされません。

マルチキャスト グループ

224.0.0.0 ー 224.0.0.255 のアドレス範囲は、ルーティングプロトコル、およびゲートウェイディスカバリやグループ メンバーシップ レポートなどのその他のトポロジディスカバリまたはメンテナンスプロトコルを使用するために予約されています。したがって、アドレス範囲224.0.0/24からのインターネット マルチキャスト ルーティングはサポートされません。予約されたアドレスのマルチキャストルーティングを有効にすると、IGMP グループは作成されません。

クラスタリング

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

- 224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンド インターフェイス上のアクセス制御ルールを設定する必要があります。ただし、ルールの宛先インターフェイスを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。
- PIM/IGMP マルチキャストルーティングは、トラフィックゾーン内のインターフェイスではサポートされません。
- ASA を同時にランデブーポイント（RP）とファーストホップルータになるように設定しないでください。

マルチキャスト ルーティングの有効化

ASA でマルチキャストルーティングを有効にすると、デフォルトではすべてのデータインターフェイスで IGMP と PIM が有効になりますが、ほとんどのモデルの管理インターフェイスで

は有効になりません（通過トラフィックを許可しないインターフェイスについては、管理スロット/ポートインターフェイス（610ページ）を参照してください）。IGMPは、直接接続されているサブネット上にグループのメンバーが存在するかどうか学習するために使用されます。ホストは、IGMP レポート メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

管理インターフェイスでマルチキャストルーティングを有効にするには、管理インターフェイスでマルチキャスト境界を明示的に設定する必要があります。

（注） マルチキャストルーティングでは、UDP トランスポート レイヤだけがサポートされています。

以下の一覧に、特定のマルチキャストテーブルに追加されるエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

- MFIB：30,000
- IGMP グループ：30,000
- PIM ルート：72,000

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** の順に選択します。

ステップ 2 [Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにします。

このチェックボックスをオンにすると、ASA 上で IP マルチキャスト ルーティングがイネーブルになります。このチェックボックスをオフにすると、IP マルチキャスト ルーティングが無効になります。デフォルトでは、マルチキャストは無効になっています。マルチキャスト ルーティングを有効にすると、すべてのインターフェイス上でマルチキャストが有効になります。マルチキャストはインターフェイスごとに無効にできます。

マルチキャスト ルーティングのカスタマイズ

ここでは、マルチキャスト ルーティングをカスタマイズする方法について説明します。

スタブ マルチキャスト ルーティングの設定と IGMP メッセージの転送

（注） スタブ マルチキャスト ルーティングは、PIM スパース モードおよび双方向モードと同時にはサポートされません。

スタブ エリアへのゲートウェイとして動作している ASA は、PIM スパース モードまたは双方向モードに参加する必要はありません。その代わりに、そのセキュリティ アプライアンスを IGMP プロキシ エージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送することができます。ASA を IGMP プロキシ エージェントとして設定するには、ホスト加入（join）メッセージおよびホスト脱退（leave）メッセージをスタブ エリアからアップストリーム インターフェイスに転送します。スタブ モードのマルチキャスト ルーティングに参加しているインターフェイスでも、PIM を有効にする必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** の順に選択します。

ステップ 2 [Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックして変更内容を保存します。

ステップ 4 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Protocol]** の順に選択します。

ステップ 5 どのインターフェイスから IGMP メッセージを転送するかを変更するには、インターフェイスを選択して [Edit] をクリックします。

[Configure IGMP Parameters] ダイアログボックスが表示されます。

ステップ 6 [Forward Interface] ドロップダウン リストで、どのインターフェイスから IGMP メッセージを送信するかを選択します。

ステップ 7 [OK] をクリックしてこのダイアログボックスを閉じてから、[Apply] をクリックして変更内容を保存します。

スタティック マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2 つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、ASA は、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[MRoute]** の順に選択します。

ステップ 2 [Add] または [Edit] を選択します。

[Add Multicast Route] または [Edit Multicast Route] ダイアログボックスが表示されます。

ASA に新しいスタティック マルチキャスト ルートを追加する場合は、[Add Multicast Route] ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更する場合は、[Edit Multicast Route] ダイアログボックスを使用します。

ステップ 3 [Source Address] フィールドに、マルチキャスト送信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。

ステップ 4 [Source Mask] ドロップダウン リストからマルチキャスト送信元の IP アドレスのネットワーク マスクを選択します。

ステップ 5 [Incoming Interface] 領域で、[RPF Interface] オプション ボタンをクリックしてルートを転送する RPF を選択するか、[Interface Name] オプション ボタンをクリックし、次に以下を入力します。

- [Source Interface] フィールドで、ドロップダウン リストからマルチキャスト ルートの着信インターフェイスを選択します。
- [Destination Interface] フィールドで、どの宛先インターフェイスを通してルートを転送するかをドロップダウン リストで選択します。

（注） インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。

ステップ 6 [Administrative Distance] フィールドで、スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスを選択します。スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスがユニキャスト ルートのアドミニストレーティブ ディスタンスと同じである場合は、スタティック マルチキャスト ルートが優先されます。

ステップ 7 [OK] をクリックします。

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

インターフェイスでの IGMP の有効化

IGMP は、特定のインターフェイスでディセーブルにできます。この情報は、特定のインターフェイスにマルチキャスト ホストがないことがわかっていて、ASA からそのインターフェイスにホスト クエリー メッセージを発信しないようにする場合に有用です。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Protocol]** の順に選択します。

[Protocol] ペインには、ASA 上の各インターフェイスの IGMP パラメータが表示されます。

ステップ 2 ディセーブルにするインターフェイスを選択して [Edit] をクリックします。

ステップ 3 指定したインターフェイスをディセーブルにするには、[Enable IGMP] チェックボックスをオフにします。

ステップ 4 [OK] をクリックします。

[Protocol] ペインに「Yes」と表示される場合は IGMP がそのインターフェイス上でイネーブルになっており、「No」の場合はそのインターフェイス上で IGMP がディセーブルになっています。

IGMP グループ メンバーシップの設定

ASA をマルチキャスト グループのメンバとして設定できます。マルチキャスト グループに加入するように ASA を設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注） 特定のグループのマルチキャスト パケットを特定のインターフェイスに転送する必要がある場合に、ASA がそのパケットをそのグループの一部として受け付けることがないようにする方法については、スタティック加入した IGMP グループの設定（1044 ページ）を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Join Group]** の順に選択します。

ステップ 2 [Join Group] ペインの [Add] または [Edit] をクリックします。 > > >

[Add IGMP Join Group] ダイアログボックスでは、インターフェイスをマルチキャスト グループのメンバーに設定することができます。[Edit IGMP Join Group] ダイアログでは、既存のメンバーシップ情報を変更することができます。

ステップ 3 [Interface Name] フィールドで、ドロップダウン リストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

ステップ 4 [Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 5 [OK] をクリックします。

スタティック加入した IGMP グループの設定

設定によってはグループ メンバがグループ内で自分のメンバーシップを報告できない場合があります。また、ネットワーク セグメント上にグループのメンバが存在しないこともあります。しかし、それでも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信することが必要になる場合があります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。

メイン ASDM ウィンドウで、[Configuration] > [Routing] > [Multicast] > [IGMP] > [Static Group] の順に選択すると、ASA をスタティックに接続されたグループ メンバーとして設定できます。この方法の場合、ASA はパケットそのものを受信せず、転送だけを実行します。そのため、スイッチングが高速に実施されます。発信インターフェイスは IGMP キャッシュ内に存在しますが、このインターフェイスはマルチキャスト グループのメンバーではありません。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Static Group]** の順に選択します。

ステップ 2 [Static Group] ペインの [Add] または [Edit] をクリックします。

インターフェイスに対してマルチキャスト グループをスタティックに割り当てる場合は、[Add IGMP Static Group] ダイアログボックスを使用します。既存のスタティック グループの割り当てを変更する場合は、[Edit IGMP Static Group] ダイアログボックスを使用します。

ステップ 3 [Interface Name] フィールドで、ドロップダウン リストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

ステップ 4 [Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 5 [OK] をクリックします。

マルチキャスト グループへのアクセスの制御

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Access Group]** の順に選択します。

[Access Group] ペインが表示されます。[Access Group] ペインのテーブル エントリは、上から下の順に処理されます。具体的なエントリはテーブルの上方に、一般的なエントリは下方に配置してください。たとえば、特定のマルチキャスト グループを許可するためのアクセス グループ エントリはテーブルの上方に配置し、許可ルールに指定されたグループなど、一定のまとまりを持った複数のマルチキャスト グループを拒否するようなアクセス グループ エントリは下方に配置します。ただし、拒否ルールよりも許可ルールの方が優先的に適用されるため、許可ルールに指定されているグループは、拒否ルールが適用されて場合でも許可されます。

テーブルのエントリをダブルクリックすると、選択したエントリの [Add/Edit Access Group] ダイアログボックスが開きます。

ステップ 2 [Add] または [Edit] をクリックします。

[Add Access Group] または [Edit Access Group] ダイアログボックスが表示されます。[Add Access Group] ダイアログボックスでは、新しいアクセス グループを [Access Group] テーブルに追加できます。[Edit Access Group] ダイアログボックスでは、既存のアクセス グループ エントリの情報を変更できます。既存のエントリを編集するときは、一部のフィールドがグレー表示されることがあります。

ステップ 3 アクセス グループを関連付けるインターフェイスの名前を [Interface] ドロップダウン リストで選択します。既存のアクセス グループを編集しているときは、関連インターフェイスは変更できません。

ステップ 4 [permit] を [Action] ドロップダウン リストで選択すると、選択されているインターフェイス上でそのマルチキャスト グループが許可されます。[deny] を [Action] ドロップダウン リストで選択すると、選択されているインターフェイスからそのマルチキャスト グループがフィルタリングされます。

ステップ 5 [Multicast Group Address] フィールドで、そのアクセス グループの適用先となるマルチキャスト グループのアドレスを入力します。

ステップ 6 マルチキャスト グループ アドレスのネットワーク マスクを入力するか、一般的なネットワーク マスクの 1 つを [Netmask] ドロップダウン リストから選択します。

ステップ 7 [OK] をクリックします。

インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Protocol]** の順に選択します。

ステップ 2 [Protocol] ペインのテーブルから限定するインターフェイスを選択し、[Edit] をクリックします。

[Configure IGMP Parameters] ダイアログボックスが表示されます。

ステップ 3 [Group Limit] フィールドに、インターフェイス上で参加できる最大ホスト数を入力します。

デフォルト値は 500 です。有効な値は 0 ～ 500 です。

（注） この値を 0 に設定すると、学習したグループが追加されなくなりますが、手動で定義したメンバーシップは引き続き許可されます。

ステップ 4 [OK] をクリックします。

（注） アクティブな結合があるインターフェイスで IGMP 制限を変更した場合、新しい制限は既存のグループには適用されません。ASA では、新しいグループがインターフェイスに追加されたときと IGMP join タイマーが期限切れになったときにのみ制限を検証します。新しい制限をすぐに適用するには、インターフェイスで IGMP を無効にしてから再度有効にする必要があります。

マルチキャスト グループに対するクエリー メッセージの変更

ASA は、クエリー メッセージを送信して、インターフェイスに接続されているネットワークにメンバを持つマルチキャスト グループを検出します。メンバーは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリ メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、ASA に保存されているメンバーシップ情報はリフレッシュされます。ASA で、ローカル メンバがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャス

トパケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上の PIM 代表ルータがクエリ メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリ応答時間を変更する場合は、IGMP クエリでアドバタイズする最大クエリ応答所要時間はデフォルトで 10 秒になります。ASA がこの時間内にホスト クエリーの応答を受信しなかった場合、グループを削除します。

クエリー間隔、クエリー応答時間、クエリータイムアウト値を変更するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration] > [Device Setup] > [Routing] > [Multicast] > [IGMP] > [Protocol]** の順に選択します。

ステップ 2 [Protocol] ペインのテーブルから限定するインターフェイスを選択し、[Edit] をクリックします。

[Configure IGMP Parameters] ダイアログボックスが表示されます。

ステップ 3 [Query Interval] フィールドに、指定したルータから IGMP ホストクエリー メッセージが送信される時間間隔を秒単位で入力します。

有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。

（注） 指定されたタイムアウト値の時間が経過しても、ASA がインターフェイス上でクエリー メッセージを検出できなかった場合は、その ASA が指定ルータになり、クエリー メッセージの送信を開始します。

ステップ 4 [Query Timeout] に、前のインターフェイスのリクエスタがリクエスタとしての動作を停止してから、ASA がそのインターフェイスのリクエスタの役割を引き継ぐまでの期間を秒単位で入力します。

有効な値の範囲は 60 ～ 300 秒です。デフォルト値は 255 秒です。

ステップ 5 [Response Time] フィールドには、IGMP クエリーでアドバタイズされる最大クエリー応答時間を秒数で入力します。

有効範囲は 1 ～ 25 秒です。デフォルト値は 10 秒です。

ステップ 6 [OK] をクリックします。

IGMP バージョンの変更

デフォルトでは、ASA は IGMP バージョン 2 を実行します。このバージョンでは などの、いくつかの追加機能を使用できます。

サブネットのマルチキャストルータはすべて、同じIGMPバージョンをサポートしている必要があります。ASAは、バージョン1ルータを自動的に検出してバージョン1に切り替えることはありません。しかし、サブネットにIGMPのバージョン1のホストとバージョン2のホストが混在しても問題はありません。IGMPバージョン2を実行しているASAは、IGMPバージョン1のホストが存在しても正常に動作します。

手順

ステップ1 メインASDMウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Protocol]** の順に選択します。

ステップ2 どのインターフェイスのIGMPバージョンを変更するかを[Protocol]ペインのテーブルで選択し、[Edit]をクリックします。

[Configure IGMP Interface]ダイアログボックスが表示されます。

ステップ3 バージョン番号を[Version]ドロップダウン リストから選択します。

ステップ4 [OK]をクリックします。

PIM 機能の設定

ルータはPIMを使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。Secure Firewall ASAでマルチキャスト ルーティングを有効にすると、PIMおよびIGMPがすべてのインターフェイスで自動的に有効になります。

（注） PIMは、PATではサポートされません。PIMプロトコルはポートを使用せず、PATはポートを使用するプロトコルに対してのみ動作します。

ここでは、任意のPIM設定を行う方法について説明します。

インターフェイスでの PIM の有効化またはディセーブル化

PIMは、特定のインターフェイスでイネーブルまたはディセーブルにできます。

手順

ステップ1 メインASDMウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Protocol]** の順に選択します。

ステップ2 どのインターフェイスでPIMをイネーブルにするかを[Protocol]ペインのテーブルで選択し、[Edit]をクリックします。

[Edit PIM Protocol]ダイアログボックスが表示されます。

ステップ 3 [Enable PIM] チェックボックスをオンにします。PIM をディセーブルにするには、このチェックボックスをオフにします。

ステップ 4 [OK] をクリックします。

スタティック ランデブー ポイント アドレスの設定

共通の PIM スパース モードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識している必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。

（注） ASA は、Auto-RP をサポートしていません。

複数のグループの RP として機能するように ASA を設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Rendezvous Points]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add Rendezvous Point] または [Edit Rendezvous Point] ダイアログボックスが表示されます。[Add Rendezvous Point] ダイアログボックスでは、新しいエントリを [Rendezvous Point] テーブルに追加できます。[Edit Rendezvous Point] ダイアログボックスでは、既存の RP エントリを変更できます。さらに、[Delete] をクリックして、選択されているマルチキャスト グループ エントリをテーブルから削除できます。

RP を使用する場合の制限事項は、次のとおりです。

- 同じ RP アドレスは、2 度使用できません。
- 複数の RP に対しては、[すべてのグループ（All Groups）] を指定できません。

ステップ 3 [Rendezvous Point Address] フィールドに、RP の IP アドレスを入力します。

既存の RP エントリを編集しているときは、この値は変更できません。

ステップ 4 [Use bi-directional forwarding] チェックボックスをオンにすると、指定されているマルチキャスト グループは双方向モードで動作します。[Rendezvous Point] ペインに「Yes」と表示されている場合は、指定されているマルチキャスト グループが双方向モードで動作し、「No」の場合はスパース モードで動作します。双方向モードでは、ASA がマルチキャスト パケットを受信

したときに、直接接続されたメンバーも PIM ネイバーも存在しない場合は、送信元にプルーニング メッセージが返されます。

ステップ 5 [Use this RP for All Multicast Groups] オプション ボタンをクリックすると、指定した RP がそのインターフェイス上のすべてのマルチキャスト グループに使用され、[Use this RP for the Multicast Groups as specified below] オプション ボタンをクリックすると、指定した RP をどのマルチキャスト グループで使用するかを指定できます。

マルチキャスト グループの詳細については、マルチキャスト グループの設定（1052 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

指定ルータのプライオリティの設定

DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、ASA の DR プライオリティは 1 です。この値を変更できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Protocol]** の順に選択します。

ステップ 2 [Protocol] ペインのテーブルから PIM にイネーブルにするインターフェイスを選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

ステップ 3 [DR Priority] フィールドに、選択されているインターフェイスの指定ルータ プライオリティの値を入力します。サブネット上のルータのうち、DR プライオリティが最も大きいものが指定ルータになります。有効な値の範囲は 0 ～ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値を 0 に設定した場合は、その ASA インターフェイスがデフォルトのルータになることはありません。

ステップ 4 [OK] をクリックします。

PIM 登録メッセージの設定とフィルタリング

ASA が RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。[Request Filter] ペインでは、ASA で PIM 登録メッセージが受け入れられるマルチキャスト ソースを定義できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Request Filter]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Request Filter Entry] ダイアログボックスでは、ASA が RP として動作する際に ASA に登録できるマルチキャスト送信元を定義できます。送信元 IP アドレスおよび宛先マルチキャスト アドレスに基づいて、フィルタ ルールを作成します。

ステップ 3 [Action] ドロップダウンリストで、[Permit] を選択すると、指定のマルチキャスト トラフィックの指定の送信元に ASA への登録を許可するルールが作成され、[Deny] を選択すると、指定のマルチキャスト トラフィックの指定の送信元による ASA への登録を禁止するルールが作成されます。

ステップ 4 [Source IP Address] フィールドに、登録メッセージの送信元の IP アドレスを入力します。

ステップ 5 [Source Netmask] フィールドに、登録メッセージの送信元のネットワーク マスクを入力するか、ドロップダウンリストから選択します。

ステップ 6 [Destination IP Address] フィールドに、マルチキャストの宛先アドレスを入力します。

ステップ 7 [Destination Netmask] フィールドに、マルチキャストの宛先アドレスのネットワーク マスクを入力するか、ドロップダウンリストから選択します。

ステップ 8 [OK] をクリックします。

PIM メッセージ間隔の設定

ルータ クエリー メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリ メッセージを送信します。デフォルトでは、ルータ クエリ メッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、ASA は PIM 加入メッセージおよびプルーニング メッセージを送信します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Protocol]** の順に選択します。

ステップ 2 [Protocol] ペインのテーブルから PIM にイネーブルにするインターフェイスを選択し、[Edit] をクリックします。

[Edit PIM Protocol] ダイアログボックスが表示されます。

ステップ 3 [Hello Interval] フィールドに、インターフェイスから PIM hello メッセージが送信される時間間隔を秒単位で入力します。

ステップ 4 [Prune Interval] フィールドに、インターフェイスから PIM 参加およびプルーニングのアドバタイズメントが送信され時間間隔を秒単位で入力します。

ステップ 5 [OK] をクリックします。

ルート ツリーの設定

デフォルトでは、PIM リーフ ルータは、新しい送信元から最初のパケットが到着した直後に、最短パス ツリーに加入します。この方法では、遅延が短縮されますが、共有ツリーに比べて多くのメモリが必要になります。すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスに対して、ASA を最短パス ツリーに加入させるか、共有ツリーを使用するかを設定できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Route Tree]** の順に選択します。

ステップ 2 次のいずれかのオプション ボタンをクリックします。

- [Use Shortest Path Tree for All Groups]：すべてのマルチキャスト グループに最短パス ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for All Groups]：すべてのマルチキャスト グループに共有ツリーを使用する場合は、このオプションを選択します。
- [Use Shared Tree for the Groups specified below]：[Multicast Groups] テーブルで指定したグループに共有ツリーを使用する場合は、このオプションを選択します。[Multicast Groups] テーブルで指定されていないグループには最短パス ツリーが使用されます。

  [Multicast Groups] テーブルには、共有ツリーを使用するマルチキャスト グループが表示されます。

  テーブル エントリは、上から下の順で処理されます。ある範囲のマルチキャスト グループが含まれるエントリを作成し、その範囲の中から特定のグループを除外するには、その除外するグループに対する拒否ルールをテーブルの先頭に配置し、その範囲内のマルチキャスト グループ全体に対する許可ルールを deny 文の下に配置します。

  マルチキャスト グループを編集するには、マルチキャスト グループの設定（1052 ページ）を参照してください。

マルチキャスト グループの設定

マルチキャスト グループとは、どのマルチキャスト アドレスがグループの一部であるかを定義するアクセス ルールのリストです。1 つのマルチキャスト グループに、マルチキャスト アドレスが 1 つだけ含まれることも、特定の範囲のマルチキャスト アドレスが含まれることもあります。新しいマルチキャスト グループ ルールを作成する場合は、[マルチキャスト グループの追加（Add Multicast Group）] ダイアログボックスを使用します。既存のマルチキャスト グ

ループ ルールを修正する場合は、[マルチキャスト グループの編集（Edit Multicast Group）] ダイアログボックスを使用します。

マルチキャスト グループを設定するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[設定（Configuration）] > [デバイスの設定（Device Setup）] > [ルーティング（Routing）] > [マルチキャスト（Multicast）] > [PIM（PIM）] > [ランデブー ポイント（Rendezvous Points）]** の順に選択します。

ステップ 2 [ランデブー ポイント（Rendezvous Point）] ペインが表示されます。設定するグループをクリックします。

[ランデブー ポイントの編集（Edit Rendezvous Point）] ダイアログボックスが表示されます。

ステップ 3 [次に指定するようにマルチキャスト グループに対してこの RP を使用する（Use this RP for the Multicast Groups as specified below）] オプション ボタンをクリックすると、指定の RP とともに使用するマルチキャスト グループを指定できます。

ステップ 4 [追加（Add）] または [編集（Edit）] をクリックします。

[マルチキャスト グループの追加（Add Multicast Group）] または [マルチキャスト グループの編集（Edit Multicast Group）] ダイアログボックスが表示されます。

ステップ 5 [アクション（Action）] ドロップダウン リストで、[許可（Permit）] を選択すると指定のマルチキャスト アドレスを許可するグループ ルールが作成され、[拒否（Deny）] を選択すると指定のマルチキャスト アドレスをフィルタリングするグループ ルールが作成されます。

ステップ 6 [マルチキャスト グループ アドレス（Multicast Group Address）] フィールドに、このグループに関連付けるマルチキャスト アドレスを入力します。

ステップ 7 [ネットマスク（Netmask）] ドロップダウン リストで、マルチキャスト グループ アドレスのネットワーク マスクを選択します。

ステップ 8 [OK] をクリックします。

PIM ネイバーのフィルタリング

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Neighbor Filter]** の順に選択します。

ステップ 2 [Add]/[Edit]/[Insert] をクリックして、テーブルから設定する PIM ネイバーを選択します。

[Add/Edit/Insert Neighbor Filter Entry] ダイアログボックスが表示されます。このダイアログボックスでは、マルチキャスト境界 ACL の ACL エントリを作成できます。選択されている PIM ネイバー エントリを削除することもできます。

ステップ 3 [Interface Name] ドロップダウン リストからインターフェイス名を選択します。

ステップ 4 [Action] ドロップダウン リストから、ネイバー フィルタ ACL エントリに対して [Permit] または [Deny] を選択します。

[Permit] を選択すると、マルチキャスト グループ アドバタイズメントがこのインターフェイスを通過できるようになります。[Deny] を選択すると、指定したマルチキャスト グループ アドバタイズメントはこのインターフェイスを通過できなくなります。インターフェイスに対してマルチキャスト境界を設定すると、ネイバー フィルタ エントリで許可されていない限り、すべてのマルチキャスト トラフィックが、インターフェイスの通過を拒否されます。

ステップ 5 [IP Address] フィールドに、許可または拒否するマルチキャスト PIM グループの IP アドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 6 [Netmask] ドロップダウン リストで、マルチキャスト グループ アドレスのネットマスクを選択します。

ステップ 7 [OK] をクリックします。

双方向ネイバー フィルタの設定

ASA に PIM 双方向ネイバー フィルタが設定されている場合、[Bidirectional Neighbor Filter] ペインにそれらのフィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバー フィルタ設定が ASA に適用されると、実行コンフィギュレーションに *interface-name*_multicast という名前の ACL が表示されます。ここで、*interface-name* はマルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスが ASA の PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタを利用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。このフィルタで、DF 選定に参加するルータを指定する

一方で、引き続きすべてのルータにスパースモードドメインへの参加を許可できるからです。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタが有効な場合、その ACL によって許可されるルータは、双方向に対応しているとみなされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Bidirectional Neighbor Filter]** の順に選択します。

ステップ 2 [PIM Bidirectional Neighbor Filter] テーブルのエントリの 1 つをダブルクリックすると、そのエントリの [Edit Bidirectional Neighbor Filter Entry] ダイアログボックスが表示されます。

ステップ 3 [Add]/[Edit]/[Insert] をクリックして、テーブルから設定する PIM ネイバーを選択します。

[Add/Edit/Insert Bidirectional Neighbor Filter Entry] ダイアログボックスが表示され、ここで PIM 双方向ネイバー フィルタ ACL の ACL エントリを作成できます。

ステップ 4 [Interface Name] ドロップダウン リストからインターフェイス名を選択します。どのインターフェイスに対して PIM 双方向ネイバー フィルタ ACL エントリを設定するかを選択します。

ステップ 5 [Action] ドロップダウン リストから、ネイバー フィルタ ACL エントリに対して [Permit] または [Deny] を選択します。

[Permit] を選択すると、指定したデバイスが DF 選定に参加できるようになります。指定したデバイスを DF 選定プロセスに参加させない場合は、[Deny] を選択します。

ステップ 6 許可または拒否するマルチキャスト PIM グループの IP アドレスを入力します。[IP Address] フィールドで有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

ステップ 7 [Netmask] ドロップダウン リストで、マルチキャスト グループ アドレスのネットマスクを選択します。

ステップ 8 [OK] をクリックします。

BSR 候補としての ASA の設定

ASA を BSR 候補として設定できます。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[PIM]** > **[Bootstrap Router]** の順に選択します。

ステップ 2 [Configure this ASA as a candidate bootstrap router (CBSR)] チェックボックスをオンにして CBSR 設定を行います。

a) [Select Interface] ドロップダウン リストから、ASA 上のインターフェイスのうち、ASA を候補にする BSR アドレスを抽出するために使用するインターフェイスを選択します。

（注） このインターフェイスは PIM を使用してイネーブルにする必要があります。

b) [Hash mask length] フィールドに、ハッシュ関数が呼び出される前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）を入力します。ハッシュ元が同じであるすべてのグループは、同じランデブー ポイント（RP）に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。これにより、複数のグループについて 1 つの RP を取得できます。

c) [Priority] フィールドに、BSR 候補のプライオリティを入力します。プライオリティが大きな BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。デフォルト値は 0 です

ステップ 3 （オプション）[Configure this ASA as a Border Bootstrap Router] セクションで、PIM BSR メッセージを送受信しないインターフェイスを選択します。

ステップ 4 [Apply] をクリックします。

マルチキャスト境界の設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界を設定できます。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープ アドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であるとみなされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

管理スコープ境界でAuto-RP検出メッセージと通知メッセージを設定、検証、フィルタリングできます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合

は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Routing]** > **[Multicast]** > **[MBoundary]** の順に選択します。

[MBoundary] ペインでは、管理スコープ マルチキャスト アドレスのマルチキャスト境界を設定できます。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。インターフェイスに対してマルチキャスト境界が定義されている場合、フィルタ ACL により許可されたマルチキャスト トラフィックだけが、そのインターフェイスを通過します。

ステップ 2 [Edit] をクリックします。

[Edit Boundary Filter] ダイアログボックスに、マルチキャスト境界フィルタ ACL が表示されます。このダイアログボックスを使用すれば、境界フィルタ ACL エントリを追加したり削除したりできます。

境界フィルタのコンフィギュレーションが ASA に適用されると、実行コンフィギュレーションに *interface-name*_multicast という名前の ACL が追加されます。*interface-name* は、マルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。

ステップ 3 どのインターフェイスに対してマルチキャスト境界フィルタ ACL を設定するかを [Interface] ドロップダウン リストで選択します。

ステップ 4 [Remove any Auto-RP group range] チェックボックスをオンにすると、境界 ACL で拒否された送信元からの Auto-RP メッセージがフィルタリングされます。[Remove any Auto-RP group range] チェックボックスがオフの場合は、すべての Auto-RP メッセージが通過できます。

ステップ 5 [OK] をクリックします。

PIM のモニターリング

さまざまな PIM ルーティング統計情報をモニターまたはディセーブル化するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[PIM]** > **[BSR Router]** の順に選択します。

BSR ルータ設定情報が表示されます。

ステップ 2 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[PIM]** > **[Multicast Routing Table]** の順に選択します。

マルチキャスト ルーティング テーブルの内容が表示されます。

ステップ 3 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[PIM]** > **[MFIB]** の順に選択します。

IPv4 PIM マルチキャスト転送情報ベースのエントリおよびインターフェイスの数に関する要約情報が表示されます。

ステップ 4 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[PIM]** > **[MFIB Active]** の順に選択します。

アクティブなマルチキャスト送信元がマルチキャスト グループに送信している速度を示す、マルチキャスト転送情報ベース（MFIB）からの要約情報が表示されます。

ステップ 5 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[PIM]** > **[Group Map]** の順に選択します。

アクティブなマルチキャスト送信元がマルチキャスト グループに送信している速度を示す、マルチキャスト転送情報ベース（MFIB）からの要約情報が表示されます。

a) [Select PIM Group] ドロップダウン リストから [RP Timers] を選択して、それぞれのグループ/PIM モード マッピングに関するタイマー情報を表示します。

ステップ 6 メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[PIM]** > **[Neighbors]** の順に選択します。

PIM（Protocol Independent Multicast）ネイバーの情報が表示されます。

マルチキャスト ルーティングの例

次の例に、さまざまなオプションのプロセスを使用してマルチキャスト ルーティングをイネーブルにし、設定する方法を示します。

1. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** の順に選択します。
2. [Multicast] ペインで、[Enable Multicast routing] チェックボックスをオンにして [Apply] をクリックします。
3. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[MRoute]** の順に選択します。
4. [Add] または [Edit] をクリックします。

   [Add Multicast Route] または [Edit Multicast Route] ダイアログボックスが表示されます。

   ASA に新しいスタティック マルチキャスト ルートを追加する場合は、[Add Multicast Route] ダイアログボックスを使用します。既存のスタティック マルチキャスト ルートを変更する場合は、[Edit Multicast Route] ダイアログボックスを使用します。

5. [Source Address] フィールドに、マルチキャスト送信元の IP アドレスを入力します。既存のスタティック マルチキャスト ルートを編集しているときは、この値は変更できません。

6. [Source Mask] ドロップダウン リストからマルチキャスト送信元の IP アドレスのネットワーク マスクを選択します。

7. [Incoming Interface] 領域で、[RPF Interface] オプション ボタンをクリックしてルートを転送する RPF を選択するか、[Interface Name] オプション ボタンをクリックし、次に以下を入力します。

   - [Source Interface] フィールドで、ドロップダウン リストからマルチキャスト ルートの着信インターフェイスを選択します。
   - [Destination Interface] フィールドでは、選択されているインターフェイスからどの宛先インターフェイスにルートを転送するかをドロップダウン リストで選択します。

(注) インターフェイスまたはRPF ネイバーを指定できますが、同時に両方は指定できません。

8. [Administrative Distance] フィールドで、スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスを選択します。スタティック マルチキャスト ルートのアドミニストレーティブ ディスタンスがユニキャスト ルートのアドミニストレーティブ ディスタンスと同じである場合は、スタティック マルチキャスト ルートが優先されます。

9. [OK] をクリックします。

10. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Multicast]** > **[IGMP]** > **[Join Group]** の順に選択します。

    [Join Group] ペインが表示されます。

11. [Add] または [Edit] をクリックします。

    [Add IGMP Join Group] ダイアログボックスでは、インターフェイスをマルチキャスト グループのメンバーに設定することができます。[Edit IGMP Join Group] ダイアログボックスでは、既存のメンバーシップ情報を変更することができます。

12. [Interface Name] フィールドで、ドロップダウン リストからインターフェイス名を選択します。既存のエントリを編集しているときは、この値は変更できません。

13. [Multicast Group Address] フィールドで、インターフェイスが属するマルチキャスト グループのアドレスを入力します。有効なグループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

14. [OK] をクリックします。

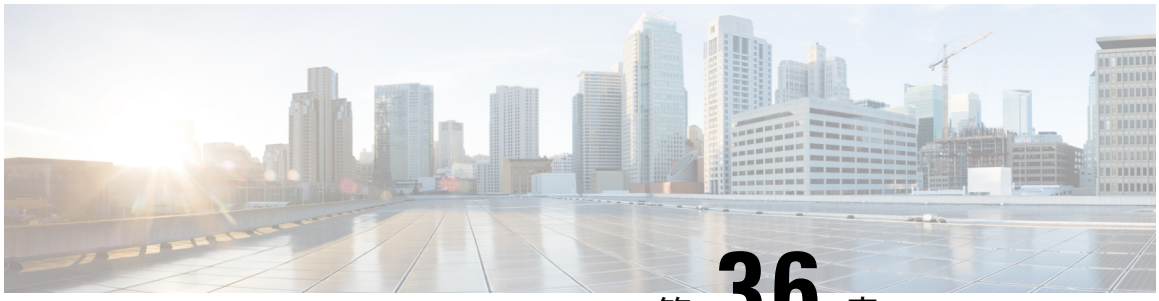
マルチキャスト ルーティングの履歴

表 *43 :* マルチキャスト ルーティングの機能履歴

機能名	プラットフォームリリース	機能情報
マルチキャスト ルーティング サポート	7.0(1)	マルチキャスト ルーティング プロトコルを使用した、データのマルチキャスト ルーティング データ、認証、およびルーティング情報の再配布とモニターリングのサポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [Multicast]。
クラスタリングのサポート	9.0(1)	クラスタリングのサポートが追加されました。
Protocol Independent Multicast Source-Specific Multicast（PIM-SSM）パススルーのサポート	9.5(1)	ASA が最後のホップ ルータである場合を除いて、マルチキャスト ルーティングが有効になっているときに PIM-SSM パケットが通過できるようサポートを追加しました。これにより、さまざまな攻撃から保護すると同時に、マルチキャスト グループをより柔軟に選択できるようになりました。ホストは、明示的に要求された送信元からのトラフィックのみを受信します。 変更された画面はありません。
Protocol Independent Multicast ブートストラップルータ（BSR）	9.5(2)	ランデブー ポイント（RP）機能の候補ルータを使用して、ランデブーポイント情報をグループに伝達するためのダイナミックランデブーポイント選択モデルがサポートされました。この機能は、ランデブーポイントを動的に学習する手段を提供します。これは、RP が停止と起動を繰り返す複雑で大規模なネットワークに不可欠です。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [Multicast] > [PIM] > [Bootstrap Router]。

第 VI 部

AAA サーバーおよびローカル データベース



第 36 章

AAA サーバーとローカル データベース

この章では、認証、認可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章では、AAA 機能用にローカル データベースを設定する方法について説明します。外部 AAA サーバーについては、ご使用のサーバー タイプに関する章を参照してください。

AAA とローカル データベースについて

ここでは、AAA とローカル データベースについて説明します。

認証

認証はユーザーを特定する方法です。アクセスが許可されるには、ユーザーは通常、有効なユーザー名と有効なパスワードが必要です。AAA サーバは、ユーザのクレデンシャルとデータベースに保存されている他のユーザ クレデンシャルとを比較します。クレデンシャルが一致した場合は、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、Cisco ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - [Telnet]
  - SSH

- シリアル コンソール
- ASDM（HTTPS を使用）
- VPN 管理アクセス

- **enable** コマンド
- ネットワーク アクセス層
- VPN アクセス

認証

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザーが持っているのかを判断します。ユーザーが認証されると、そのユーザーはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

アカウンティング

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA サーバーおよびサーバーグループ

AAA サーバーは、アクセス制御に使用されるネットワーク サーバーです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実装します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

外部 AAA サーバーを使用する場合は、まず外部サーバーで使用するプロトコルに応じた AAA サーバーグループを作成し、そのグループにサーバーを追加する必要があります。プロトコルごとに複数のグループを作成し、使用するすべてのプロトコルについてグループを分けることができます。各サーバー グループは、あるサーバーまたはサービスに固有です。

グループの作成方法の詳細については、次のトピックを参照してください。

- RADIUS サーバー グループの設定 （1099 ページ）
- TACACS+ サーバー グループの設定 （1110 ページ）
- LDAP サーバー グループの設定 （1121 ページ）
- Kerberos AAA サーバーグループの設定 （1127 ページ）
- RSA SecurID AAA サーバーグループの設定 （1134 ページ）

Kerberos Constrained Delegation および HTTP Form の使用の詳細については、 VPN 構成ガイドを参照してください。

次の表に、ローカルデータベースを含むサポートされるサーバーのタイプとその用途の概要を示します。

表 *44 : AAA* サーバーでサポートされるサービス

サーバータイプとサービス	認証	許可	アカウンティング
ローカル データベース			
管理者	対応	対応	非対応
VPN ユーザー	対応	非対応	×
ファイアウォールセッション（AAA ルール）	対応	対応	非対応
RADIUS			
管理者	対応	対応	対応
VPN ユーザー	対応	対応	対応
ファイアウォールセッション（AAA ルール）	対応	対応	対応
TACACS+			
管理者	対応	対応	対応
VPN ユーザー	対応	非対応	対応
ファイアウォールセッション（AAA ルール）	対応	対応	対応

サーバータイプとサービス	認証	許可	アカウンティング
LDAP			
管理者	対応	非対応	×
VPN ユーザー	対応	対応	非対応
ファイアウォールセッション（AAA ルール）	対応	非対応	×
Kerberos			
管理者	対応	非対応	×
VPN ユーザー	対応	非対応	×
ファイアウォールセッション（AAA ルール）	対応	非対応	×
SDI（RSA SecurID）			
管理者	対応	非対応	×
VPN ユーザー	対応	非対応	×
ファイアウォールセッション（AAA ルール）	対応	非対応	×
HTTP Form			
管理者	非対応	×	×
VPN ユーザー	対応	非対応	×
ファイアウォールセッション（AAA ルール）	非対応	×	×

注記

- RADIUS：管理者のアカウンティングには、コマンドアカウンティングは含まれません。
- RADIUS：ファイアウォールセッションの認可は、ユーザー固有のアクセスリストでだけサポートされます。このアクセスリストは RADIUS 認証応答で受信または指定されます。
- TACACS+：管理者のアカウンティングには、コマンドアカウンティングが含まれます。
- HTTP Form：クライアントレス SSL VPN ユーザーセッションの場合に限り、認証と SSO 操作がサポートされます。

ローカル データベースについて

ASAは、ユーザープロファイルを取り込むことができるローカルデータベースを管理します。AAA サーバーの代わりにローカル データベースを使用して、ユーザー認証、認可、アカウンティングを提供することもできます。

次の機能にローカル データベースを使用できます。

- ASDM ユーザーごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、Cisco ASDM ログインには影響しません。
- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、Cisco ASA では、ユーザー特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。 ASDM には、コマンドへの割り当てをイネーブルにできる特権レベルが事前に定義されています。割り当てることができるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の3種類です。事前定義済みのレベルを使用する場合は、ユーザーを3種類の特権レベルのいずれかに割り当てます。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザー名を設定し、**login** コマンドを使用してCLIで個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

（注） ローカル データベースはネットワーク アクセス認可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないように設計されています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバーから、応答があるまでグループ内のサーバーが順に 1 つずつアクセスされます。グループ内のすべてのサーバーが使用できない場合、ローカルデータベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASAはローカルデータベースに接続しようとします。フォー

ルバック方式として設定されていない場合、ASA は引き続き AAA サーバーにアクセスしようとします。

フォールバック サポートを必要とするユーザーについては、ローカル データベース内のユーザー名およびパスワードと、AAA サーバー上のユーザー名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザーは、AAA サーバーとローカルデータベースのどちらがサービスを提供しているかが判別できないので、ローカルデータベースのユーザー名およびパスワードとは異なるユーザー名およびパスワードを AAA サーバーで使用することは、指定するべきユーザー名とパスワードをユーザーが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバーがすべて使用できない場合、ASA ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバーがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバーが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバー グループが使用できない場合でも、ローカルデータベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバーを使用したフォールバックの仕組み

サーバー グループ内に複数のサーバーを設定し、サーバー グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASAからの認証要求に対してグループ内のどのサーバーからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバー 1、サーバー 2 の順で、LDAP サーバー グループに 2 台の Active Directory サーバーを設定します。リモート ユーザーがログインすると、ASA によってサーバー 1 に対する認証が試みられます。

サーバー 1 から認証エラー（「user not found」など）が返されると、ASA によるサーバー 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバーからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

ローカル データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASA からのロックアウトを必ず防止してください。

ローカル データベースへのユーザー アカウントの追加

ユーザーをローカル データベースに追加するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** を選択し、次に [Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

ステップ 2 4 ～ 64 文字の長さのユーザー名を入力します。

ステップ 3 （オプション）3 ～ 127 文字のパスワードを入力します。パスワードでは大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。 SSH 公開キー認証を使用している場合など、パスワードを指定せずにユーザー名を作成することもできます。

（注） [User Accounts] ペインでイネーブル パスワードを設定する場合は、ユーザー名 enable_15 に対するパスワードを変更します。ユーザー名 enable_15 は常に [User Accounts] ペインに表示され、デフォルト ユーザー名を表します。この方法は、ASDM のシステム コンフィギュレーションでイネーブル パスワードを設定する唯一の方法です。CLI で他のイネーブル レベル パスワード（enable password 10 など）を設定すると、そのユーザー名は enable_10 という形式で表示されます。

ステップ 4 パスワードを再度入力します。

セキュリティ上の理由から、パスワードを入力するこの 2 つのフィールドには、アスタリスクだけが表示されます。

ステップ 5 MSCHAP を認証に使用している場合は、[User authenticated using MSCHAP] チェックボックスをオンにします。

ステップ 6 [Access Restriction] 領域で、ユーザーの管理アクセス レベルを設定します。まず、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** タブの順に移動し、[Perform authorization for exec shell access] オプションをクリックして、管理認可を有効にする必要があります。

次のいずれかのオプションを選択します。

- [Full Access (ASDM, Telnet, SSH and console)]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザーはASDM、SSH、Telnet、

およびコンソール ポートを使用できます。さらに認証もイネーブルにすると、ユーザーはグローバル コンフィギュレーション モードにアクセスできます。

- [Privilege Level]：ASDM およびローカル コマンド認可用の特権レベルを設定します。範囲は、0（最低）～ 15（最高）です。無制限の管理者アクセス権を付与するには、15 を指定します。事前定義された ASDM ロールでは、管理者用の 15、読み取り専用の 5、およびモニター専用の 3（ユーザーによる [Home] ペインと [Monitoring] ペインの使用を制限する）が使用されます。

- [CLI login prompt for SSH, Telnet and console (no ASDM access)]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザーは SSH、Telnet、およびコンソール ポートを使用できます。ユーザーは設定に ASDM を使用できません（HTTP 認証を設定している場合）。ASDM 監視は可能です。さらにイネーブル認証も設定すると、ユーザーはグローバル コンフィギュレーション モードにアクセスできません。

- [No ASDM, SSH, Telnet, or console access]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定すると、ユーザーは認証用に設定した管理アクセス方式を利用できなくなります（ただし、[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。

ステップ 7 （オプション）ユーザー単位で ASA への SSH 接続の公開キー認証をイネーブルにする方法については、ASDM、その他のクライアントの HTTPS アクセスの設定 （1140 ページ） を参照してください。

ステップ 8 [VPN Policy] をクリックして、このユーザーの VPN ポリシー属性を設定します。VPN 構成ガイドを参照してください。

ステップ 9 [Apply] をクリックします。

ユーザーがローカルデータベースに追加され、変更内容が実行コンフィギュレーションに保存されます。

ヒント **[Configuration]** > **[Device Management]** > [Users/AAA] > [User Accounts] ペインの各カラムで特定のテキストを検索できます。[Find] ボックスに検索する特定のテキストを入力し、[Up] または [Down] 矢印をクリックします。テキスト検索にアスタリスク（「*」）と疑問符（「?」）をワイルドカードとして使用することもできます。

ローカル データベースの認証および認可のテスト

ASA がローカル データベースに接続してユーザーを認証または許可できるかどうか確認するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** > **[AAA Server Groups]** テーブルで、サーバーが含まれるサーバー グループをクリックします。

ステップ 2 [Servers in the Selected Group] テーブルでテストするサーバーをクリックします。

ステップ 3 [Test] をクリックします。

選択したサーバーに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5 ユーザー名を入力します。

ステップ 6 認証をテストする場合は、ユーザー名のパスワードを入力します。

ステップ 7 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

ローカル データベースのモニターリング

ローカル データベースのモニターリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインには、AAA サーバーの統計情報が表示されます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

ローカル データベースの履歴

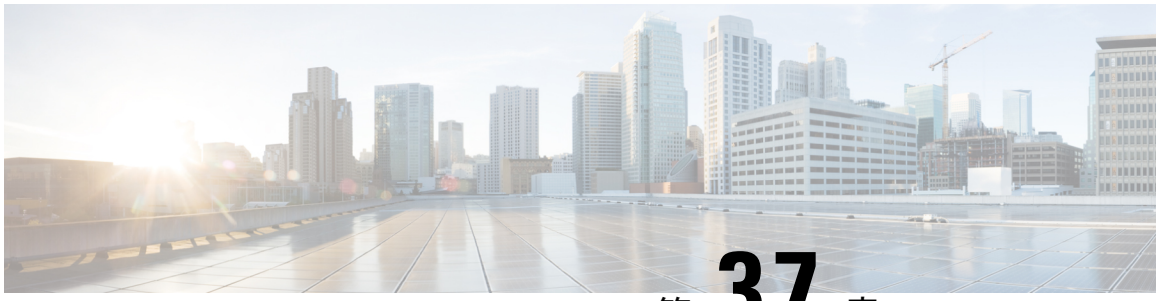
表 *45 :* ローカル データベースの履歴

機能名	プラットフォームリリース	説明
AAA のローカル データベース設定	7.0(1)	AAA 用にローカル データベースを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts]
SSH 公開キー認証のサポート	9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザー単位で有効にできるようになりました。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication][Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。 *8.4(4.1)* でも使用可能。*PKF* キー形式は *9.1(2)* でのみサポートされます。

機能名	プラットフォームリリース	説明
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** > **[Enable Password]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]** > **[Identity]**
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカル ユーザーデータベース（）を使用してAAA SSH認証を有効にしなくても、SSH公開キー認証（）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザーが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザー名を作成できるようになりました。 次の画面が変更されました。 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]**

機能名	プラットフォームリリース	説明
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	9.7(1)	長さ制限内のすべてのローカル **username** および **enable** パスワードは、PBKDF2（パスワード ベース キー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザーが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次の画面が変更されました。 **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** > **[Enable Password]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]** > **[Identity]**

機能名	プラットフォームリリース	説明
SSH 公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザー データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザーに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカルデータベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更された画面はありません。



第 37 章

AAA の RADIUS サーバー

この章では、AAA 用に RADIUS サーバーを設定する方法について説明します。

AAA 用の RADIUS サーバーについて

Cisco ASA は AAA について、次の RFC 準拠 RADIUS サーバーをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine（ISE）
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバーでの次の認証方式をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続の場合。
- MS-CHAPv2：L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシ モード：RADIUS から Active Directory、RADIUS から RSA/SDI、Radius からトークン サーバー、RSA/SDI から RADIUS の各接続。

(注) MS-CHAPv2 を、ASA と RADIUS サーバーの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバーへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバーが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバーが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザー認証

ASA は、RADIUS サーバーを使用して、ダイナミック ACL またはユーザーごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザー許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバーを設定する必要があります。ユーザーを認証する場合、RADIUS サーバーによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA は ACL を削除します。

ACL に加えて、ASA は、VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションの認証およびアクセス許可の設定を行うための多くの属性をサポートしています。

RADIUS 属性のサポートされるセット

ASA は次の RADIUS 属性のセットをサポートしています。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA

• RFC 2548 に定義されている Microsoft VSA

サポートされる RADIUS 認証属性

認可では、権限または属性を使用するプロセスを参照します。認証サーバーとして定義されているRADIUSサーバーは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

次の表に、ユーザー認可に使用可能な、サポートされているRADIUS属性の一覧を示します。

（注） RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA は、属性名ではなく数値の属性 ID に基づいて RADIUS 属性を使用します。

次の表に示した属性はすべてダウンストリーム属性であり、RADIUS サーバーから ASA に送信されます。ただし、属性番号 146、150、151、および 152 を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバーに送信されます。RADIUS 属性 146 および 150 は、認証および認可の要求の場合に ASA から RADIUS サーバーに送信されます。前述の 4 つの属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバーに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

表 *46 :* サポートされる *RADIUS* 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカルプールの名前
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = 無効1 = 有効
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	はい	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列。Banner2 文字列は Banner1 文字列に連結されます（設定されている場合）。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Client Type	Y	150	整数	シングル	1 = Cisco VPN Client（IKEv1） 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = 無効1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。完全に割り当てられた IPv6 アドレスを作成するために、Framed-IPv6-Prefix と組み合わせます。例：Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8::/64 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Framed-IPv6-Prefix	Y	97	文字列	シングル	割り当てられた IPv6 プレフィックスと長さ。完全に割り当てられた IPv6 アドレスを作成するために、Framed-Interface-Id と組み合わせます。例：プレフィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。この属性を使用して、フレームインターフェイス Id を使用せずに IP アドレスを割り当てることができます。これには、プレフィックス長/128 を使用して完全な IPv6 アドレスを割り当てます（たとえば、フレーム化された IPv6 プレフィックス＝2001:0db8:: 1/128）。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Group-Policy	Y	25	文字列	シングル	リモートアクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2.x 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバー アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1=クライアントが設定したリストを使用する 2 = クライアントリストをディセーブルにして消去する 3 = バックアップ サーバー リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメイン名を 1 つだけ指定します（1 ～ 255 文字）。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバーからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティアソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリットトンネルの包含リストを記述したネットワークまたはACLの名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用できる管理属性。グループ ポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = いいえ 1 = はい
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client-Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 =クライアントレス 2=クライアント 3=クライアントのみ Session Subtype が適用されるのは、Session Type（151）属性の値が 1、2、3、または 4 の場合のみです。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Session Type	Y	151	整数	シングル	0 = なし 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN（IKEv2） 3 = クライアントレス SSL VPN 4 = クライントレス電子メールプロキシ 5 = Cisco VPN Client（IKEv1） 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロードバランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマートトンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
SmartTunnelAutoSignonEnable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効1 = 有効
SVC-Ask	Y	131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルトサービスをイネーブルにする 5 = デフォルトクライアントレスをイネーブルにする （2 と 4 は使用しない）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 と 4 は相互排他。0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効1 = 有効
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効1 = 有効
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	整数	シングル	0 = 無効1 = 有効
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example.example.com）
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = 無効1 = 有効
WebVPN-Cache-HTTP-HTTPS-Proxy-Exceptions	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用したカンマ区切りの DNS/IP（たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-HomePageUseSmartTunnel	Y	228	ブール	シングル	クライアントレスホームページをスマートトンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP:ポート（例：http=10.10.10.10:80、https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。 このテキストでクライアントレス ポータル ホーム ページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN SmartCard-Removal-Disconnect	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネル自動サインオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Smart-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマートトンネル ネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = 無効1 = 有効
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネル）
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザー ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認証属性

次の表に、サポートされる IETF RADIUS 属性の一覧を示します。

表 47 : サポートされる *IETF RADIUS* 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降では、Group-Policy 属性（VSA 3076、#25）を使用することをお勧めします。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	n/a	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	n/a	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	Seconds

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービス タイプの値： • .Administrative：ユーザーは configure プロンプトへのアクセスを許可されています。 • .NAS-Prompt：ユーザーは exec プロンプトへのアクセスを許可されています。 • .remote-access：ユーザーはネットワークアクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	Seconds

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6

切断の理由コード
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA の RADIUS サーバーのガイドライン

ここでは、AAA 用の RADIUS サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

- シングルモードで最大200個のサーバーグループ、またはマルチモードでコンテキストごとに 4 つのサーバーグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。

AAA 用の RADIUS サーバーの設定

ここでは、AAA 用に RADIUS サーバーを設定する方法について説明します。

手順

ステップ 1 ASA の属性を RADIUS サーバーにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバーのタイプによって異なります。

- Cisco ACS を使用している場合：サーバーには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバー（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

ステップ 2 RADIUS サーバー グループの設定 （1099 ページ）。

ステップ 3 グループへの RADIUS サーバーの追加 （1102 ページ）。

ステップ 4 （任意） 認証プロンプトの追加 （1104 ページ）。

RADIUS サーバー グループの設定

認証、許可、またはアカウンティングに外部 RADIUS サーバーを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバー グループを作成して、各グループに 1 つ以上のサーバーを追加する必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウン リストから RADIUS サーバー タイプを選択します。

ステップ 5 [Accounting Mode] を選択します。

- [Simultaneous]：グループ内のすべてのサーバーにアカウンティング データを送信します。
- [Single]：1 つのサーバーにだけアカウンティング データを送信します。

ステップ 6 グループ内で障害の発生したサーバーを再度アクティブ化する方法（[Reactivation Mode]）を設定します。

- [Depletion]、[Dead Time]：グループ内のすべてのサーバーが非アクティブになった後に、障害の発生したサーバーを再度アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。

• [timed]：30 秒のダウン時間の後、障害が発生したサーバーを再度アクティブ化します。

ステップ 7 [Max Failed Attempts] で、次のサーバーを試す前にグループ内の RADIUS サーバーでの AAA トランザクションの失敗の最大数を指定します。

範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間続くと（デフォルトの再アクティブ化モードとデッド時間を使用する場合）、ただちにフォールバック方式が使用されます。非応答時間をデフォルト値から変更するには、[Dead Time] の変更方法を参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバーにアクセスしようとします。

ステップ 8 （任意）適切なオプションを選択して、RADIUS 中間アカウンティング更新メッセージの定期的な生成をイネーブルにします。

これらのオプションが関連するのは、このサーバー グループを AnyConnect またはクライアントレス SSL VPN に使用している場合のみです。

• [Enable interim accounting update]：[Update Interval] オプションを選択せずにこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。

• [Update Interval]：対象のサーバー グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。これらの更新を送信する間隔を時間単位で変更できます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 です。

（注） ISE サーバが含まれるサーバ グループには、両方のオプションを選択します。ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいて、アクティブ セッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウンティング メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブ セッションについて ISE に定期的に中間アカウンティング更新メッセージを送信するように、グループを設定します。

ステップ 9 （任意）このグループに AD エージェントまたは Cisco Directory Agent（CDA）サーバーしか含まれていない場合は、[Enable Active Directory Agent Mode] を選択します。

CDA または AD エージェントはアイデンティティ ファイアウォールで使用されるサーバーであり、完全な機能を備えた RADIUS サーバーではありません。このオプションを選択すると、このグループをアイデンティティ ファイアウォール専用として使用できます。

ステップ 10 （任意）このサーバー グループをリモート アクセス VPN で ISE ポリシーを適用するために使用する場合、次のオプションを設定します。

- [Enable dynamic authorization]：AAA サーバー グループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。VPN トンネルでサーバー グループを使用すると、対応する RADIUS サーバー グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。
- [Dynamic Authorization Port]：動的認可をイネーブルにする場合、RADIUS CoA 要求のリスニング ポートを指定できます。デフォルト値は 1700 です。有効な範囲は 1024 ～ 65535 です。
- [Use authorization only mode]：認証に ISE を使用しない場合は、RADIUS サーバー グループに対し認可専用モードをイネーブルにします。これは、サーバー グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバー用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。RADIUS サーバーの共通パスワードを設定すると、そのパスワードは無視されます。

  たとえば、認証にこのサーバー グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバー グループを使用する可能性があるからです。

ステップ 11 （任意）[VPN3K Compatibility Option] を設定して、RADIUS パケットから受信したダウンロード可能 ACL を Cisco AV ペアの ACL と結合するかどうかを指定します。

このオプションは、VPN 接続にのみ適用されます。VPN ユーザーの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

- [Do not merge]：ダウンロード可能 ACL は Cisco AV ペアの ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。これがデフォルトのオプションです。
- **Place the downloadable ACL after Cisco AV-pair ACL**
- **Place the downloadable ACL before Cisco AV-pair ACL**

ステップ 12 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバー グループが [AAA Server Groups] テーブルに追加されます。

ステップ 13 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

グループへの RADIUS サーバーの追加

RADIUS サーバーをグループに追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバーを追加するサーバー グループをクリックします。

ステップ 2 [Servers in the Selected Group] 領域（下側のペイン）で、[Add] をクリックします。

サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 認証サーバーが存在するインターフェイス名を選択します。

ステップ 4 グループに追加するサーバーのサーバー名または IP アドレスを追加します。

ステップ 5 サーバーへの接続試行のタイムアウト値を指定します。

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the retry interval）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー（設定されている場合）への要求の送信を開始します。

ステップ 6 ダウンロード可能な ACL で受信されたネットマスクを ASA でどのように処理するかを指定します。次のオプションから選択します。

- [Detect automatically]：ASA で、使用されているネットマスク表現のタイプが判定されます。ASA は、ワイルドカード ネットマスク表現を検出した場合、標準ネットマスク表現に変換します。

  （注） 一部のワイルドカード表現は明確な検出が困難なため、この設定を選択した場合には、ワイルドカードネットマスク表現が誤って標準ネットマスク表現として検出されることもあります。

- [Standard]：ASA は、RADIUS サーバーから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカードネットマスク表現からの変換は実行されません。
- [Wildcard]：ASA は、RADIUS サーバーから受信したダウンロード可能 ACL に、ワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

ステップ 7 この ASA を介して RADIUS 認可サーバーにアクセスするユーザーに共通のパスワードを指定します。このパスワードは大文字と小文字が区別されます。この情報は、RADIUS サーバー管理者に伝えてください。

（注） RADIUS認証サーバー（認可サーバーではない）に対しては、共通のパスワードは設定しないでください。

このフィールドを空白のままにした場合は、RADIUS認可サーバーにアクセスする際のパスワードには、各ユーザー名が使用されます。

RADIUS 認可サーバーを認証に使用することは避けてください。共通パスワードやユーザー名を転用したパスワードは、ユーザーごとに一意のパスワードに比べ、安全性が低くなります。

このパスワードは、RADIUS プロトコルや RADIUS サーバーによって要求されますが、ユーザーが知っている必要はありません。

ステップ 8 二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバーが MS-CHAPv2 をサポートしていない場合、このチェックボックスをオンにすれば、そのサーバーから非 MS-CHAPv2 認証要求が送信されるようにできます。

ステップ 9 ASA からサーバーへ接続を試行した後、次に試行するまでの待機時間を、1 ～ 10 秒の間で指定します。

（注） RADIUS プロトコルの場合、サーバーが ICMP ポート到達不能メッセージで応答すると、再試行間隔の設定が無視され、AAA サーバーはただちに障害状態になります。このサーバーが AAA グループ内の唯一のサーバーである場合は、サーバーが再アクティブ化され、別の要求がサーバーに送信されます。これは意図された動作です。

ステップ 10 [Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバーにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバーに送信されます。

ステップ 11 ユーザーのアカウンティングに使用するサーバー ポートを指定します。デフォルトのポートは 1646 です。

ステップ 12 ユーザーの認証に使用するサーバー ポートを指定します。デフォルトのポートは 1645 です。

ステップ 13 ASA でRADIUSサーバーを認証する際に使用される共有秘密キーを指定します。設定したサーバー秘密キーは、RADIUS サーバーで設定されたサーバー秘密キーと一致する必要があります。サーバー秘密キーが不明の場合は、RADIUSサーバーの管理者に問い合わせてください。最大フィールド長は、64 文字です。

ステップ 14 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバーが AAA サーバー グループに追加されます。

ステップ 15 [AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

RADIUS サーバーからのユーザー認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワードプロンプトの上に表示されます。認証プロンプトを指定しなかった場合は、ユーザが RADIUS サーバで認証中に以下の内容が表示されます。

Connection Type	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Authentication Prompt]** の順に選択します。

ステップ 2 ログイン時にユーザー名とパスワードプロンプトの上に表示するメッセージとして追加するテキストを、[Prompt] フィールドに入力します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	文字制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 3 [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザー認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証の試みが RADIUS サーバーによって承認または拒否されたことを示す、異なる状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、ASA では、RADIUS サーバーにより認証されたユーザーに対しては [User accepted message] テキストが表示され、認証されなかったユーザーに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。**ユーザー承認メッセージ** テキストおよび**ユーザー拒否メッセージ** テキストは表示されません。

ステップ 4 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

RADIUS サーバーの認証および認可のテスト

ASA が RADIUS サーバーに接続してユーザーを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の順に選択します。

ステップ 2 サーバーが [AAA Server Groups] テーブル内に存在するサーバー グループをクリックします。

ステップ 3 [Servers in the Selected Group] テーブルでテストするサーバーをクリックします。

ステップ 4 [Test] をクリックします。

選択したサーバーに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 6 ユーザー名を入力します。

ステップ 7 認証をテストする場合は、ユーザー名に対応するパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。テストが失敗した場合は、エラー メッセージが表示されます。

AAA 用の RADIUS サーバーのモニターリング

AAA 用の RADIUS サーバーのステータスのモニターリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインには、RADIUS サーバーの実行コンフィギュレーションが表示されます。

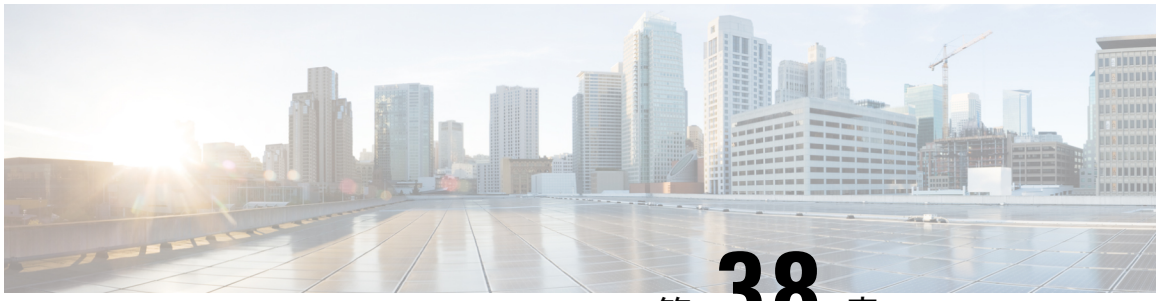
- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

AAA 用の RADIUS サーバーの履歴

表 *48 : AAA* 用の *RADIUS* サーバーの履歴

機能名	プラットフォームリリース	説明
AAA の RADIUS サーバー	7.0(1)	AAA 用の RADIUS サーバーを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]
ASA からの RADIUS アクセス要求パケットおよびアカウンティング要求パケットでの主なベンダー固有属性（VSA）の送信	8.4(3)	4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type（151）および Session Subtype（152）は、ASA からの RADIUS アカウンティング要求パケットで送信されます。4 つのすべての属性が、すべてのアカウンティング要求パケット タイプ（開始、中間アップデート、および終了）に送信されます。RADIUS サーバー（ACS や ISE など）は、認可属性やポリシー属性を強制適用したり、アカウンティングや課金のためにそれらの属性を使用したりできます。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングル コンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに8台のサーバーを設定できます（以前の制限はグループごとに4台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。



第 38 章

AAA 用の TACACS+ サーバー

この章では、AAA で使われる TACACS+ サーバーの設定方法について説明します。

AAA 用の TACACS+ サーバーについて

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバー認証をサポートします。

TACACS+ 属性

Cisco ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの2種類の属性をサポートします。サーバーとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザーに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注） TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

次の表に、カットスループロキシ接続に対してサポートされる TACACS+ 許可応答属性の一覧を示します。

表 *49 :* サポートされる *TACACS+* 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザー セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザー セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

次の表に、サポートされる TACACS+ アカウンティング属性の一覧を示します。

。

表 *50 :* サポートされる *TACACS+* アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティインターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。

属性	説明
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザーの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザーの名前を示します。

AAA 用の TACACS+ サーバーのガイドライン

ここでは、AAA 用の TACACS+ サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバーは、IPv4 または IPv6 アドレスを使用できます。

その他のガイドライン

- シングルモードで最大 200 個のサーバーグループ、またはマルチモードでコンテキストごとに 4 つのサーバーグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。

TACACS+ サーバーの設定

ここでは、TACACS+ サーバーを設定する方法について説明します。

手順

ステップ 1 TACACS+ サーバー グループの設定 （1110 ページ）。
ステップ 2 グループへの TACACS+ サーバーの追加 （1111 ページ）。
ステップ 3 （オプション）認証プロンプトの追加 （1112 ページ）。

TACACS+ サーバー グループの設定

認証、許可、アカウンティングに TACACS+ サーバーを使用する場合は、まず TACACS+ サーバー グループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバーを追加する必要があります。TACACS+ サーバー グループは名前で識別されます。

TACACS+ サーバー グループを追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。
ステップ 4 [Protocol] ドロップダウン リストから、[TACACS+] サーバー タイプを選択します。
ステップ 5 [Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。

[Single] モードの場合、ASA ではアカウンティング データが 1 つのサーバーにだけ送信されます。

[Simultaneous] モードの場合、ASA ではアカウンティング データがグループ内のすべてのサーバーに送信されます。

ステップ 6 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバーが非アクティブになった場合、そのサーバーは、グループの他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 7 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 8 サーバーで許可される AAA トランザクションの失敗の最大数を追加します。

このオプションで設定するのは、応答のないサーバーを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 9 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバー グループが [AAA Server Groups] テーブルに追加されます。

ステップ 10 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

グループへの TACACS+ サーバーの追加

TACACS+ サーバーをグループに追加するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 サーバーを追加するサーバー グループをクリックします。

ステップ 3 [Servers in the Selected Group] 領域で、[Add] をクリックします。

サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 4 認証サーバーが存在するインターフェイス名を選択します。

ステップ 5 グループに追加するサーバーのサーバー名または IP アドレスを追加します。

ステップ 6 サーバーへの接続試行のタイムアウト値を指定します。

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the retry interval）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー（設定されている場合）への要求の送信を開始します。

ステップ 7 サーバー ポートを指定します。サーバー ポートは、ポート番号 139、または ASA によって TACACS+ サーバーとの通信に使用される TCP ポートの番号です。

ステップ 8 サーバー秘密キーを指定します。ASA で TACACS+ サーバーを認証する際に使用される共有秘密キーを指定します。ここで設定したサーバー秘密キーは、TACACS+ サーバーで設定されたサーバー秘密キーと一致する必要があります。サーバー秘密キーが不明の場合は、TACACS+ サーバーの管理者に問い合わせてください。最大フィールド長は、64 文字です。

ステップ 9 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバーが AAA サーバー グループに追加されます。

ステップ 10 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

認証プロンプトの追加

AAA 認証チャレンジ プロセスの実行中にユーザーに表示するテキストを指定できます。TACACS+ サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザーのログイン時に、ユーザー名プロンプトとパスワード プロンプトの上に表示されます。

認証プロンプトを指定しない場合、TACACS+ サーバーでの認証時にユーザーに対して表示される内容は次のようになります。

Connection Type	デフォルトのプロンプト
FTP	FTP authentication
HTTP	HTTP 認証
Telnet	なし

認証プロンプトを追加するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Authentication Prompt]** の順に選択します。

ステップ 2 ログイン時にユーザーに表示されるユーザー名とパスワードのプロンプトの上に表示するテキストを追加します。

次の表に、認証プロンプトの文字数制限を示します。

アプリケーション	認証プロンプトの文字数制限
Microsoft Internet Explorer	37
Telnet	235
FTP	235

ステップ 3 [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザー認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバーにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージ テキストをそれぞれ指定した場合、ASA では、AAA サーバーにより認証されたユーザーに対しては [User accepted message] テキストが表示され、認証されなかったユーザーに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよびFTPセッションの認証では、プロンプトにチャレンジテキストのみが表示されます。ユーザー承認メッセージテキストおよびユーザー拒否メッセージテキストは表示されません。

ステップ 4 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

TACACS+ サーバーの認証および許可のテスト

ASA が TACACS+ サーバーに接続してユーザーを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の順に選択します。

ステップ 2 サーバーが存在するサーバー グループをクリックします。

ステップ 3 テストするサーバーをクリックします。

ステップ 4 [Test] をクリックします。

選択したサーバーに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 6 ユーザー名を入力します。

ステップ 7 認証をテストする場合は、ユーザー名のパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。テストが失敗した場合は、エラー メッセージが表示されます。

AAA 用の TACACS+ サーバーのモニターリング

AAA 用の TACACS+ サーバーのモニターリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

このペインには、設定された TACACS+ サーバーの統計情報が表示されます。

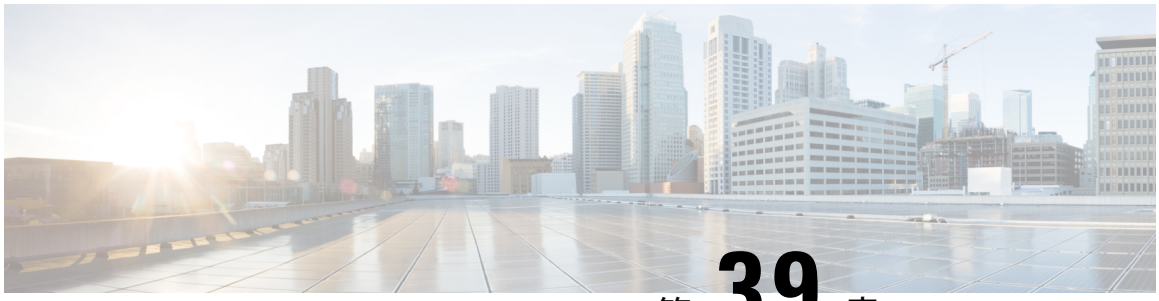
- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

AAA 用の TACACS+ サーバーの履歴

表 *51 : AAA* 用の *TACACS+* サーバーの履歴

機能名	プラットフォームリリース	説明
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバーを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt]。
AAA 向けの IPv6 アドレス TACACS+ サーバー	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。



第 39 章

AAA の LDAP サーバー

この章では、AAA で使用される LDAP サーバーの設定方法について説明します。

LDAP および ASA について

Cisco ASA はほとんどの LDAPv3 ディレクトリ サーバーと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server（現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server）
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバーに接続しているかどうかが自動検出されます。ただし、LDAP サーバー タイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP での認証方法

認証中、ASA は、ユーザーの LDAP サーバーへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバーに対する認証を行います。デフォルトで、ASA は、通常はユーザー名とパスワードである認証パラメータを LDAP サーバーにプレーン テキストで渡します。

ASA では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：ASA は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：ASA は、GSSAPI Kerberos メカニズムを使用して、ユーザー名とレルムを送信することで LDAP サーバーに応答します。

ASA と LDAP サーバーは、これらの SASL メカニズムの任意の組み合わせをサポートします。複数のメカニズムを設定した場合、ASA ではサーバーに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバーの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバーと ASA の両方がこれら両方のメカニズムをサポートしている場合、ASA は、強力な方の Kerberos メカニズムを選択します。

ユーザー LDAP 認証が成功すると、LDAP サーバーは認証されたユーザーの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される認可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。

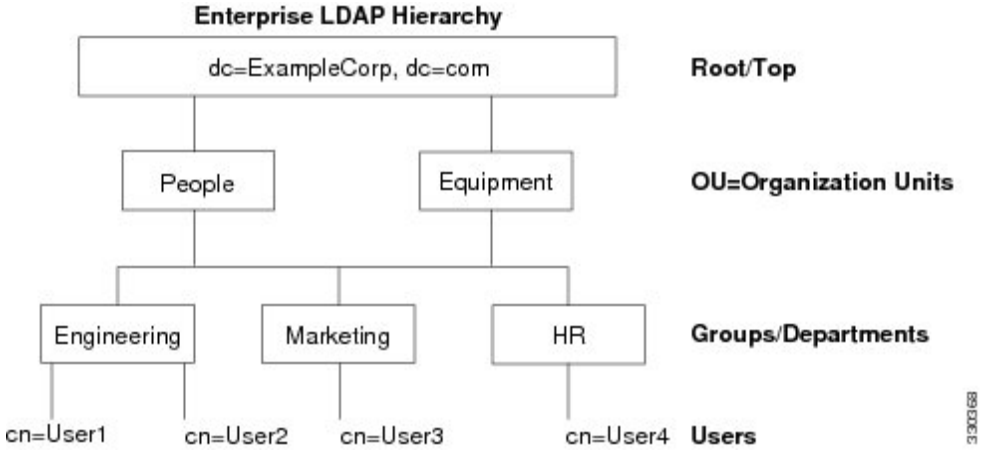
（注） LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 階層

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、次の図を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 *71* : マルチレベルの *LDAP* 階層



LDAP 階層の検索

ASA は、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザーの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバーが ASA から認可要求を受信したときに LDAP 階層内のどの場所からユーザー情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバーによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバーのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

次の図に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。次の表に、2つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 認可が必要であるため、ASA から LDAP サーバーに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 *52 :* 検索コンフィギュレーションの例

番号	LDAP Base DN	検索範囲	名前属性	結果
1	group=Engineering,ou=People,dc=ExampleCorporation,dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバーへのバインド

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバーとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、Login DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、Login DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP（LDAP-S）
- Simple Authentication and Security Layer（SASL）MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。

（注） LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP 属性マップ

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザー
- ファイアウォール ネットワークのアクセス/カットスルー プロキシ セッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定

- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザー属性を Cisco ASA 属性に変換します。それらの属性マップを LDAP サーバーにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザーが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザー定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザー定義の属性のタイプは次のとおりです。

- IETF-Radius-Class（ASA バージョン 8.2 以降における Group_Policy）：ディレクトリ部門またはユーザー グループ（たとえば、Microsoft Active Directory memberOf）属性値に基づいてグループ ポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりに group-policy 属性が使用されます。
- IETF-Radius-Filter-Id：VPN クライアント、IPSec、SSL に対するアクセス コントロール リスト（ACL）に適用されます。
- IETF-Radius-Framed-IP-Address：VPN リモート アクセス クライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1：VPN リモート アクセス ユーザーのログイン時にテキスト バナーを表示します。
- Tunneling-Protocols：アクセス タイプに基づいて、VPN リモート アクセス セッションを許可または拒否します。

注 1 つの LDAP 属性マップに、1 つ以上の属性を含めることができます。特定の LADP サーバーからは、1 つの LDAP 属性のみをマップすることができます。

AAA の LDAP サーバーのガイドライン

この項では、AAA の LDAP サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバーは、IPv4 または IPv6 アドレスを使用できます。

その他のガイドライン

- Sunディレクトリ サーバーにアクセスするためにASAに設定されているDNが、サーバーのデフォルトパスワードポリシーにアクセスできる必要があります。DNとして、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。
- Microsoft Active DirectoryおよびSunサーバーでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA は、Novell、OpenLDAP およびその他の LDAPv3 ディレクトリ サーバーによるパスワード管理をサポートしません。
- バージョン 7.1（x）以降、ASA はネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。
- シングル モードで最大 200 個のサーバー グループ、またはマルチ モードでコンテキストごとに 4 つのサーバー グループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。
- ユーザーがログインすると、コンフィギュレーション内で指定されている最初のサーバーから順に、サーバーが応答するまでLDAPサーバーが1つずつアクセスされます。グループ内のすべてのサーバーが使用できない場合、ASA は、ローカル データベースがフォールバック方式として設定されていると、ローカルデータベースに接続しようとします（管理認証および認可限定）。フォールバック メソッドとして設定されていない場合、ASA は LDAP サーバーに引き続きアクセスしようとします。

AAA の LDAP サーバーの設定

この項では、AAA に LDAP サーバーを設定する方法について説明します。

手順

ステップ 1 LDAP属性マップを設定します。LDAP属性マップの設定（1120ページ）を参照してください。

ステップ 2 LDAPサーバー グループを追加します。LDAPサーバー グループの設定（1121ページ）を参照してください。

ステップ 3 サーバーをグループに追加し、サーバー パラメータを設定します。LDAPサーバーのサーバーグループへの追加 （1122 ページ）を参照してください。

LDAP 属性マップの設定

LDAP 属性マップを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル ユーザーの場合は **[Configuration]** > **[Remote Access VPN]** > **[AAA Local Users]** > **[LDAP Attribute Map]** の順に選択し、その他すべてのユーザーの場合は **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[LDAP Attribute Map]** の順に選択して、**Add** をクリックします。

[Map Name] タブが表示された状態で [Mapping of Attribute Name] ダイアログボックスが開きます。

ステップ 2 この属性マップの名前を作成します。

ステップ 3 マッピングする LDAP 属性の 1 つの名前を追加します。

ステップ 4 Cisco 属性を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 さらに属性をマップする場合は、ステップ 1～5 を繰り返します。

ステップ 7 [Mapping of Attribute Value] タブをクリックして、マップされた Cisco 属性の新しい値に LDAP 属性の値をマッピングします。

ステップ 8 [Add] をクリックして、[Add Mapping of Attribute Value] ダイアログボックスを表示します。

ステップ 9 LDAP サーバーから返されると予想されるこの LDAP 属性の値を入力します。

ステップ 10 この LDAP 属性が以前の LDAP 属性値を含める場合に、Cisco 属性で使用する値を入力します。

ステップ 11 [Add] をクリックします。

ステップ 12 さらに属性値をマップする場合は、ステップ 8 ～ 11 を繰り返します。

ステップ 13 [OK] を 2 回クリックして、各ダイアログボックスを閉じます。

ステップ 14 [Apply] をクリックし、実行コンフィギュレーションの設定を保存します。

LDAP サーバー グループの設定

LDAP サーバー グループを作成して設定し、LDAP サーバーをそのグループに追加するには、次の手順を実行します。

始める前に

LDAP サーバーを LDAP サーバー グループに追加する前に、属性マップを追加する必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]、または VPN ユーザーの場合は **[Configuration]** > **[Remote Access VPN]** > **[AAA/Local Users]** > **[AAA Server Groups]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 AAA サーバー グループの名前を入力します。

ステップ 4 [Protocol] ドロップダウンリストから LDAP サーバー タイプを選択します。

ステップ 5 使用する再アクティブ化モードのオプション ボタン（[Depletion] または [Timed]）をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

a) [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 6 サーバーで許容できる AAA トランザクションの失敗の最大回数を追加します。

これは、応答のないサーバーを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 7 [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバー グループが AAA サーバー グループに追加されます。

ステップ 8 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

LDAP サーバーのサーバー グループへの追加

LDAP サーバーをサーバー グループに追加するには、次の手順を実行します。

手順

ステップ 1 次のいずれかを選択します。

- VPN ユーザーの場合は、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups]。
- [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]

ステップ 2 サーバーを追加するサーバー グループを選択し、**Add** をクリックします。

選択したサーバー グループに対応する [Add AAA Server] ダイアログボックスが表示されます。

ステップ 3 LDAP サーバーに接続するインターフェイスの名前を選択します。

ステップ 4 LDAP サーバーのサーバー名または IP アドレスを追加します。

ステップ 5 タイムアウト値を追加するか、デフォルト値をそのまま使用します。[Timeout] フィールドには、バックアップ サーバーへ要求を送信する前に、ASA がプライマリ サーバーからの応答を待機する時間を秒単位で指定します。

ステップ 6 [LDAP Parameters for authentication/authorization] 領域で、次の設定を行います。

- [Enable LDAP over SSL]（セキュア LDAP または LDAP-S とも呼ばれる）：ASA と LDAP サーバーの間のセキュアな通信に SSL を使用する場合に、このチェックボックスをオンにします。

  （注） SASL プロトコルを設定しない場合は、SSL を使用して LDAP 通信のセキュリティを確保することを強く推奨します。

- [Server Port]：ASA から LDAP サーバーへアクセスする際、単純認証（セキュアでない認証）に使用される TCP ポート番号 389 またはセキュアな認証（LDAP-S）に使用される TCP ポート番号 636 を指定します。LDAP サーバーはすべて、認証および認可をサポートしています。Microsoft AD サーバーおよび Sun LDAP サーバーに限っては、さらに、LDAP-S を必要とする VPN リモート アクセス パスワード管理機能もサポートしています。

- [Server Type]：ドロップダウン リストから LDAP サーバー タイプを指定します。使用できるオプションは、次のとおりです。

  - **Detect Automatically/Use Generic Type**
  - **Microsoft**
  - **Novell**
  - **OpenLDAP**
  - **Sun（現在では Oracle Directory Server Enterprise Edition の一部）**

- [Base DN]：ベース識別名（DN）、または LDAP 要求を受け取ったサーバーで検索が開始される LDAP 階層内の位置を指定します（例：OU=people, dc=cisco, dc=com）。

- [Scope]：ドロップダウン リストからの認証要求を受信する場合に、LDAP 階層内でサーバーの実行が必要な検索範囲を指定します。次のオプションを使用できます。

  - [One Level]：ベース DN の 1 つ下のレベルだけが検索対象となります。このオプションを選択すると、検索の実行時間が短縮されます。
  - [All Levels]：ベース DN の下にあるすべてのレベル（つまりサブツリー階層全体）が検索対象となります。このオプションを選択すると、検索の実行に時間がかかります。

- [Naming Attribute（s）]：LDAP サーバーのエントリを一意に識別する相対識別名属性を入力します。共通の名前付き属性は、Common Name（CN）、sAMAccountName、userPrincipalName、および User ID（uid）です。

- [Login DN and Login Password]：ASA は、LDAP サーバーとの信頼（バインド）を確立するために、ログイン DN とログイン パスワードを使用します。ログイン DN のユーザー アカウントのパスワードをログイン パスワードとして指定します。
- [LDAP Attribute Map]：この LDAP サーバーで使用するために作成された属性マップの 1 つを選択します。これらの属性マップは、LDAP 属性名をシスコの属性名と値にマップします。
- [SASL MD5 authentication]：ASA と LDAP サーバーの間の通信を認証するための SASL の MD5 メカニズムをイネーブルにします。
- [SASL Kerberos authentication]：ASA と LDAP サーバーの間のセキュアな認証通信のための SASL の Kerberos メカニズムをイネーブルにします。このオプションを有効にするためには、Kerberos サーバーを定義しておく必要があります。
- [LDAP Parameters for Group Search]：この領域のフィールドは、ASA が AD グループを要求する方法を設定します。
  - [Group Base DN]：この DN により、LDAP 階層内で AD グループ（つまり、memberOf 列挙のリスト）の検索を開始する位置が指定されます。このフィールドの設定を行わない場合、ASA では、AD グループの取得にベース DN が使用されます。ASDM では、取得した AD グループのリストに基づいて、ダイナミック アクセス ポリシーの AAA 選択基準が定義されます。詳細については、**show ad-groups** コマンドを参照してください。
  - [Group Search Timeout]：使用できるグループについてのクエリーに対して AD サーバーから応答があるまでの最長待機時間を指定します。

ステップ 7 [OK] をクリックします。

[Add AAA Server] ダイアログボックスが閉じ、AAA サーバーが AAA サーバー グループに追加されます。

ステップ 8 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

LDAP サーバーによる認証および許可のテスト

ASA が LDAP サーバーに接続してユーザーを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の順に選択します。

ステップ 2 サーバーが存在するサーバー グループを選択します。

ステップ 3 テストするサーバーを選択します。

ステップ 4 [Test] をクリックします。

選択したサーバーに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 5 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 6 ユーザー名を入力します。

ステップ 7 認証をテストする場合は、ユーザー名のパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。テストが失敗した場合は、エラー メッセージが表示されます。

AAA の LDAP サーバーのモニターリング

AAA の LDAP サーバーのモニターリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインは、設定された AAA サーバーの統計情報を表示します。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

AAA の LDAP サーバーの履歴

表 *53 : AAA* サーバーの履歴

機能名	プラットフォームリリース	説明
AAA の LDAP サーバー	7.0(1)	LDAP サーバーの AAA のサポートと LDAP サーバーの設定方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map]。
AAA 向けの IPv6 アドレス LDAP サーバー	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。

機能名	プラットフォームリリース	説明
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。

第 40 章

AAA の Kerberos サーバー

ここでは、AAA で使用する Kerberos サーバーの設定方法について説明します。管理接続、ネットワークアクセス、および VPN ユーザーアクセスの認証に Kerberos サーバーを使用できます。

AAA の Kerberos サーバーのガイドライン

- シングルモードで最大 200 個のサーバーグループ、またはマルチモードでコンテキストごとに 8 つのサーバーグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。ユーザーがログインすると、コンフィギュレーション内で指定されている最初のサーバーから順に、サーバーが応答するまでこれらのサーバーが 1 つずつアクセスされます。

AAA の Kerberos サーバーの設定

ここでは、Kerberos サーバーグループの設定方法について説明します。管理アクセスや VPN を設定するときに、これらのグループを使用できます。

Kerberos AAA サーバーグループの設定

認証に Kerberos サーバーを使用する場合は、最初に少なくとも 1 つの Kerberos サーバーグループを作成し、各グループに 1 つ以上のサーバーを追加する必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウンリストから、[Kerberos] サーバータイプを選択します。

ステップ 5 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバーが非アクティブになった場合、そのサーバーは、グループの他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 6 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 7 次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

このオプションで設定するのは、応答のないサーバーを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 8 （任意）Kerberos キー発行局（KDC）の検証を有効にするには、[Validate KDC] を選択します。

認証を実行するには、Kerberos キー発行局（KDC）からエクスポートしたキータブファイルもインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザークレデンシャルが攻撃者の Kerberos サーバーに対して認証されるようにする攻撃を防ぐことができます。

キータブファイルのアップロード方法については、Kerberos キー発行局の検証の設定（1130 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

Kerberos サーバーグループへの Kerberos サーバーの追加

Kerberos サーバーグループを使用する前に、少なくとも 1 つの Kerberos サーバーをグループに追加する必要があります。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 サーバーを追加するサーバーグループを選択します。

ステップ 3 [Servers in the Selected Group] 領域で、[Add] をクリックします。

サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 4 [Interface Name] で、認証サーバーが存在するインターフェイス名を選択します。

ステップ 5 グループに追加するサーバーの名前または IP アドレスを入力します。

ステップ 6 サーバーへの接続試行のタイムアウト値を指定します。

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the retry interval）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー（設定されている場合）への要求の送信を開始します。

ステップ 7 再試行間隔を選択します。システムはこの時間待機してから接続要求を再試行します。1 ー 10 秒の範囲で選択できます。デフォルトは 10 秒です。

ステップ 8 サーバー ポートを指定します。サーバーポートは、ポート番号 88、または ASA によって Kerberos サーバーとの通信に使用される TCP ポートの番号です。

ステップ 9 Kerberos レルムを設定します。

Kerberos レルム名では数字と大文字だけを使用し、64 文字以内にする必要があります。Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Active Directory サーバー上で実行する場合は、name の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

ASA では、name に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

ステップ 10 [OK] をクリックします。

例

```
hostname(config)# aaa-server watchdogs protocol kerberos
```

```
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Kerberos キー発行局の検証の設定

グループ内のサーバーを認証するように Kerberos AAA サーバーグループを設定できます。認証を実行するには、Kerberos キー発行局（KDC）からエクスポートしたキータブファイルをインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザークレデンシャルが攻撃者の Kerberos サーバーに対して認証されるようにする攻撃を防ぐことができます。

KDC の検証を有効にすると、チケット認可チケット（TGT）を取得してユーザーを検証した後、システムはホスト/ASA_hostname のユーザーに代わってサービスチケットも要求します。次にシステムは、返されたサービスチケットを KDC の秘密鍵に対して検証します。これは、KDC から生成され、ASA にアップロードされたキータブファイルに保存されます。KDC 認証に失敗すると、サーバーは信頼できないと見なされ、ユーザーは認証されません。

次の手順では、KDC 認証を実行する方法について説明します。

始める前に

Kerberos 制約付き委任（KCD）とともに KDC 検証を使用することはできません。サーバーグループが KCD に使用されている場合、KDC 検証オプションは無視されます。

手順

ステップ 1 （KDC 上。）Microsoft Active Directory で ASA のユーザーアカウントを作成します（**[Start]** > **[Programs]** > **[Administrative Tools]** > **[Active Directory Users and Computers]** に移動します）。たとえば、ASA の完全修飾ドメイン名（FQDN）が asahost.example.com の場合は、asahost という名前のユーザーを作成します。

ステップ 2 （KDC 上。）FQDN とユーザーアカウントを使用して、ASA のホストサービスプリンシパル名（SPN）を作成します。

```
C:> setspn -A HOST/asahost.example.com asahost
```

ステップ 3 （KDC 上。）ASA のキータブファイルを作成します（わかりやすくするために改行を追加）。

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

ステップ 4 （ASA 上。）**[Tools]** > **[File Management]** の順に選択し、ファイルがワークステーションにあるかリモートサーバーにあるかに応じて、[File Transfer] メニューの該当するオプションを選択してキータブファイルをフラッシュにアップロードします。

ステップ 5 （ASA 上。）**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Kerberos]** の順に選択し、[Browse Flash] をクリックして、アップロードしたキータブファイルを選択します。

ステップ 6 （ASA 上。）Kerberos AAA サーバグループ設定に [Validate KDC] オプションを追加します。キータブファイルは、このオプションが設定されたサーバグループでのみ使用されます。

a) **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の順に選択します。

b) Kerberos サーバグループを選択して [Edit] をクリックします。または、この時点で新しいグループを作成できます。

c) [Validate KDC] オプションを選択します。

d) [OK] をクリックします。

AAA の Kerberos サーバーのモニターリング

次のコマンドを使用して、Kerberos 関連情報をモニターおよびクリアできます。コマンドは **[Tools]** > **[Command Line Interface]** ウィンドウで入力します。

- **[Monitoring]** > **[Properties]** > **[AAA Servers]**

  このウィンドウに AAA サーバーの統計情報が表示されます。

- **show aaa-server**

  AAA サーバーの統計情報を表示します。サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを使用します。

- **show running-config aaa-server**

  システムに設定されている AAA サーバーを表示します。AAA サーバー コンフィギュレーションを削除するには、**clear configure aaa-server** コマンドを使用します。

- **show aaa kerberos** ［**username** *user*］

  すべての Kerberos チケットまたは特定のユーザー名のチケットを表示します。

- **clear aaa kerberos tickets** ［**username** *user*］

  すべての Kerberos チケットまたは特定のユーザー名のチケットをクリアします。

- **show aaa kerberos keytab**

  Kerberos キータブファイルに関する情報を表示します。

- **clear aaa kerberos keytab**

  Kerberos キータブファイルをクリアします。

AAA の Kerberos サーバーの履歴

機能名	プラットフォームリリース	説明
Kerberos サーバー	7.0(1)	AAA の Kerberos サーバーのサポート。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]**
AAA の IPv6 アドレス	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。
Kerberos キー発行局（KDC）認証。	9.8(4) およびそれ以降の 9.14(1) までの暫定リリース	Kerberos キー配布局（KDC）からキータブファイルをインポートできます。システムは、Kerberos サーバーを使用してユーザーを認証する前にサーバーがスプーフィングされていないことを認証できます。KDC 認証を実行するには、Kerberos KDC で**ホスト**/*ASA_hostname* サービス プリンシパル名（SPN）を設定してから、その SPN のキータブをエクスポートする必要があります。その後に、キータブを ASA にアップロードし、KDC を検証するように Kerberos AAA サーバーグループを設定する必要があります。 次の画面が追加または変更されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Kerberos]**、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の Kerberos サーバーグループの [Add/Edit] ダイアログボックス。

第 41 章

AAA の RSA SecurID サーバー

ここでは、AAA で使用する RSA SecurID サーバーの設定方法について説明します。RSA SecureID サーバーは、通信に SDI プロトコルを使用することから、SDI サーバーとも呼ばれます。管理接続、ネットワークアクセス、および VPN ユーザーアクセスの認証に RSA SecurID サーバーを使用できます。

RSA SecurID サーバーについて

RSA SecurID サーバは、認証に直接使用することも、認証の第 2 要素として間接的に使用することもできます。後者の場合は、SecurID サーバーと RADIUS サーバーの間で SecurID サーバーとの関係を設定し、RADIUS サーバーを使用するように ASA を設定します。

一方、SecurID サーバーに対して直接認証する場合は、SDI プロトコルの AAA サーバーグループを作成します。これは、それらのサーバーとの通信に使用されるプロトコルです。

SDI を使用する場合は、AAA サーバーグループを作成するときにプライマリ SecurID サーバーを指定するだけで済みます。ASA からサーバーに最初に接続したときに、すべての SecurID サーバーのレプリカをリストした sdiconf.rec ファイルを取得します。以降にプライマリサーバが応答しない場合、それらのレプリカが認証に使用されます。

さらに、ASA を認証エージェントとして RSA Authentication Manager に登録する必要があります。ASA を登録していないと認証の試行は失敗します。

AAA の RSA SecurID サーバーのガイドライン

- シングルモードで最大 200 個のサーバーグループ、またはマルチモードでコンテキストごとに 8 つのサーバーグループを持つことができます。

- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。ユーザーがログインすると、コンフィギュレーション内で指定されている最初のサーバーから順に、サーバーが応答するまでこれらのサーバーが 1 つずつアクセスされます。

AAA の RSA SecurID サーバーの設定

ここでは、RSA SecurID サーバーグループの設定方法について説明します。管理アクセスや VPN を設定するときに、これらのグループを使用できます。

RSA SecurID AAA サーバーグループの設定

認証に RSA SecurID サーバーとの直接通信を使用する場合は、最初に少なくとも 1 つの SDI サーバーグループを作成し、各グループに 1 つ以上のサーバーを追加する必要があります。RADIUS サーバーとプロキシ関係が確立された SecurID サーバーを使用する場合は、ASA で SDI AAA サーバーグループを設定する必要はありません。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウンリストから、[SDI] サーバータイプを選択します。

ステップ 5 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバーが非アクティブになった場合、そのサーバーは、グループの他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 6 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 7 次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

このオプションで設定するのは、応答のないサーバーを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 8 [OK] をクリックします。

SDI サーバーグループへの RSA SecurID サーバーの追加

SDI サーバーグループを使用する前に、少なくとも 1 つの RSA SecurID サーバーをグループに追加する必要があります。

SDI サーバーグループのサーバーは、ASA との通信に認証およびサーバー管理プロトコル（ACE）を使用します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 サーバーを追加するサーバーグループを選択します。

ステップ 3 [Servers in the Selected Group] 領域で、[Add] をクリックします。

サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 4 [Interface Name] で、認証サーバーが存在するインターフェイス名を選択します。

ステップ 5 グループに追加するサーバーの名前または IP アドレスを入力します。

ステップ 6 サーバーへの接続試行のタイムアウト値を指定します。

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the retry interval）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー（設定されている場合）への要求の送信を開始します。

ステップ 7 再試行間隔を選択します。システムはこの時間待機してから接続要求を再試行します。1ー10 秒の範囲で選択できます。デフォルトは 10 秒です。

ステップ 8 サーバー ポートを指定します。サーバーポートは、デフォルトのポート番号である 5500 か、ASA で RSA SecurID サーバーとの通信に使用する TCP ポートの番号です。

ステップ 9 [OK] をクリックします。

AAA の RSA SecurID サーバーのモニターリング

次のコマンドを使用して、RSA SecurID 関連情報をモニターおよびクリアできます。コマンドは **[Tools]** > **[Command Line Interface]** ウィンドウで入力します。

- **[Monitoring]** > **[Properties]** > **[AAA Servers]**

  このウィンドウに AAA サーバーの統計情報が表示されます。

- **show aaa-server**

  AAA サーバーの統計情報を表示します。サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを使用します。

- **show running-config aaa-server**

  システムに設定されている AAA サーバーを表示します。AAA サーバー コンフィギュレーションを削除するには、**clear configure aaa-server** コマンドを使用します。

AAA の RSA SecurID サーバーの履歴

機能名	プラットフォームリリース	説明
SecurID サーバー	7.2(1)	AAA の SecurID サーバーの管理認証でのサポート。以前のリリースでは、SecurID は VPN 認証でサポートされていました。
AAA の IPv6 アドレス	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバー グループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。

第 VII 部

システム管理

第 42 章

管理アクセス

この章では、Telnet、SSH、および HTTPS（ASDM を使用）経由でシステム管理を行うために Cisco ASA にアクセスする方法と、ユーザーを認証および許可する方法、ログイン バナーを作成する方法について説明します。

管理リモート アクセスの設定

ここでは、ASDM 用の ASA アクセス、Telnet または SSH、およびログイン バナーなどのその他のパラメータの設定方法について説明します。

HTTPS、Telnet、または SSH の ASA アクセスの設定

この項では、ASDM および CSM、Telnet、または SSH など、HTTPS に ASA アクセスを設定する方法について説明します。次のガイドラインを参照してください。

- ASA インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。必要なのは、この章の各項の説明に従って管理アクセスを設定することだけです。ただし、HTTP リダイレクトを設定して HTTP 接続を HTTPS に自動的にリダイレクトするには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。

- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定 （1149 ページ）を参照してください。

- ASA では以下の接続が許可されます。

- コンテキストごとに最大 5 つの同時 Telnet 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
- コンテキストごとに最大 5 つの同時 SSH 接続を許可し、可能な場合は、最大 100 の接続がすべてのコンテキストの間で分割されます。
- シングルコンテキストモードでは、最大 30 の ASDM 同時セッション。マルチコンテキストモードでは、コンテキストごとに最大 5 つの同時 ASDM セッションを使用でき、全コンテキスト間で最大 32 の ASDM インスタンスの使用が可能です。

  ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニタ用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、マルチコンテキストモードシステムの ASDM セッションの制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
- シングルコンテキストモードまたはコンテキストごとに最大 6 つの非 ASDM HTTPS 同時セッション（使用可能な場合）、すべてのコンテキスト間で最大または 100 の HTTPS セッション。

ASDM、その他のクライアントの HTTPS アクセスの設定

この項では、ASDM や CSM など、HTTPS に ASA アクセスを設定する方法について説明します。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [ASDM/HTTPS] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定（1149 ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

ステップ 4 証明書認証を要件にするには、[Specify the interface requires client certificate to access ASDM] 領域で [Add] をクリックし、インターフェイスとオプションで証明書マップを指定します。証明書マップを指定する場合、その証明書マップと一致しなければ、認証は成功しません。証明書マップを作成するには、**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Advanced]** > **[IPSec]** > **[Certificate to Connection Map]** > **[Rules]** を表示します。詳細については、ASDM 証明書認証の設定 （1161 ページ）を参照してください。

ステップ 5 [HTTP Settings] を設定します。

- [Enable HTTP Server]：HTTPS サーバーを有効にします。
- [Port Number]：ポート番号を設定します。デフォルトは 443 です。
- [Idle Timeout]：ASDM 接続のアイドルタイムアウトを 1 ～ 1440 分の範囲で設定します。デフォルトは 20 分です。ASA は、設定した期間アイドル状態の ASDM 接続を切断します。
- [Session Timeout]：ASDM セッションのセッションタイムアウトを 1 ～ 1440 分の範囲で設定します。このタイムアウトはデフォルトで無効になっています。ASA は、設定した期間を超えた ASDM 接続を切断します。
- [Connection Session Timeout]：ASDM、WebVPN、および他のクライアントを含むすべての HTTPS 接続のアイドルタイムアウトを 10 ～ 86400 秒の範囲で設定します。このタイムアウトはデフォルトで無効になっています。ASA は、設定した期間アイドル状態の接続を切断します。[Idle Timeout] と [Connection Session Timeout] の両方を設定した場合は、[Connection Session Timeout] が優先されます。

ステップ 6 [Apply] をクリックします。

ステップ 7 （任意） 非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。

多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。

a) **[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Non-Browser Client Support]** を選択し、[Add] をクリックします。

b) [User-Agent String from the HTTP Header] フィールドに、HTTP 要求の HTTP ヘッダーにあるクライアントの User-Agent 文字列を指定します。

完全な文字列または部分文字列を指定できます。部分文字列については、User-Agent 文字列の先頭と一致している必要があります。セキュリティを強化するために完全な文字列をお勧めします。文字列では大文字と小文字が区別されることに注意してください。

たとえば、 **curl** は次の User-Agent 文字列と一致します。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

curl は、次の User-Agent 文字列とは一致しません。

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

CURL は、次の User-Agent 文字列とは一致しません。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

SSH アクセスの設定

この項では、SSH に ASA アクセスを設定する方法について説明します。次のガイドラインを参照してください。

- ASA インターフェイスに SSH アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの SSH アクセスはサポートされません。たとえば、SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定（1149 ページ）を参照してください。
- ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 SSH 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。ただし、設定コマンドは変更されるリソースをロックする可能性があるため、すべての変更が正しく適用されるように、一度に 1 つの SSH セッションで変更を行う必要があります。
- SSH バージョン 2 のみがサポートされます。
- （8.4 以降）SSH デフォルト ユーザー名はサポートされなくなりました。**pix** または **asa** ユーザー名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、AAA 認証を設定し（**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authentication]** の順に選択）、続いてローカルユーザーを定義する必要があります（**[Configuration]** > **[Device Management]** > **[Users/AAA]** の順に選択）。ローカル データベースの代わりに AAA サーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [SSH] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定（1149 ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

ステップ 4 （任意） [SSH Settings] を設定します。

- [Allowed SSH Versions]：サポートされているのはバージョン 2 のみです。
- [SSH Timeout]：1 ～ 60 分にタイムアウトを設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。
- [DHキー交換（DH Key Exchange）]（管理コンテキストのみ）：該当するオプションボタンをクリックして、Diffie-Hellman（DH）キー交換グループを選択します。DH グループ キー交換方式を指定しないと、DH グループ 14 SHA256 のキー交換方式が使用されます。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。キー交換は管理コンテキストでのみ設定できます。この値はすべてのコンテキストで使用されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 SSH ユーザー認証を設定します。

a) （パスワード アクセス用）**[Configuration]** > **[Device Management]** > **[Users/AAA]** > [AAA Access] > [Authentication] の順に選択します。

AAA 認証は、[Public Key Using PKF] オプションが指定されたユーザー名に対するローカル公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカルデータベースを暗黙的に使用します。SSH 認証は、パスワードを持つユーザー名にのみ影響します。ローカルユーザーが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワードアクセスを許可する必要があります。

b) [SSH] チェックボックスをオンにします。

c) [Server Group] ドロップダウン リストから [LOCAL] データベース（または AAA サーバー）を選択します。

d) [Apply] をクリックします。

e) ローカル ユーザーを追加します。ユーザー アクセスに AAA サーバーを使用することもできますが、ローカル ユーザー名の使用を推奨します。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** の順に選択し、[Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

f) ユーザー名とパスワードを入力し、パスワードを確認します。ユーザーにパスワード認証ではなく公開キー認証を強制する場合は、パスワードなしでユーザーを作成することを推奨します。公開キー認証およびパスワードの両方を設定した場合、ユーザーはいずれの方法でもログインできます（この手順で AAA 認証を明示的に設定した場合）。

g) （任意）個々のユーザーごとに、パスワード認証ではなく公開キー認証のみ、またはこれら両方の認証を有効にするには、次のいずれかのペインを選択します。

- [Public Key Authentication]：Base64 でエンコードされた公開キーに貼り付けます。ssh-rsa raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。既存のキーを表示する場合は、キーは SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼りつける場合は、[Key is hashed] チェックボックスをオンにします。
- 認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。
- [Public Key Using PKF]：[Specify a new PKF key] チェックボックスをクリックして、公開キー ファイル（PKF）でフォーマットされたキー（4096 ビットまで）を貼りつけるかインポートします。Base64 形式で貼り付けるには大きすぎるキーにはこのフォーマットを使用します。たとえば、ssh の keygen を使用して 4096 ビット キーを生成し、PKF に変換して、このペインでインポートします。既存のキーを表示する場合は、SHA-256 ハッシュを使用して暗号化されます。ハッシュ キーをコピーして貼り付ける必要がある場合は、[Public Key Athentication] ペインからコピーし、[Key is hashed] チェックボックスをオンにした新しい ASA のペインに貼り付けます。

  認証キーを削除するには、[Delete Key] をクリックして、確認ダイアログボックスを表示します。認証キーを削除する場合は [Yes] をクリックし、認証キーを保持する場合は [No] をクリックします。

h) [OK] をクリックし、続いて [Apply] をクリックします。

ステップ 7 キーペアを生成します（物理 ASA の場合のみ）。

ASAv の場合、キーペアは導入後に自動的に作成されます。ASAv は RSA キーのみをサポートします。

a) **[構成（Configuration）]** > **[デバイス管理（Device Management）]** > **[証明書管理（Certificate Management）]** > **[ID証明書（Identity Certificates）]** の順に選択します。

b) [Add] をクリックし、[Add a new identity certificate] オプション ボタンをクリックします。

c) [New] をクリックします。

d) [キーペアを追加（Add Key Pair）] ダイアログボックスで、タイプとサイズを指定して [今すぐ生成（Generate Now）] をクリックします。

使用されるデフォルトのキーペアは、RSA。

キーペアを生成するだけであるため、証明書のダイアログボックスをキャンセルできます。

ステップ 8 （任意） SSH 暗号の暗号化アルゴリズムと整合性アルゴリズムを設定します。

a) **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** の順に選択します。
b) [Encryption] を選択し、[Edit] をクリックします。
c) [SSH cipher security level] ドロップダウンリストから、次のいずれかのレベルを選択します。

暗号方式は、リストされた順に使用されます。事前定義されたリストでは、暗号方式が最も高いの順で、最も低いセキュリティに割り当てられています。

- [すべて（All）]：すべての暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、このオプションを選択します
- [Custom]：カスタム暗号ストリングを設定する場合はこのオプションを選択し、[Cipher algorithms/custom string] フィールドに各暗号ストリングをコロンで区切って入力します。
- [Fips]：FIPS 対応の暗号方式（aes128-cbc aes256-cbc）のみを使用する場合は、このオプションを選択します
- [高（High）]：強度が高の暗号方式のみ（aes256-cbc aes256-ctr）を使用する場合は、このオプションを選択します
- [Low]：強度が低、中、高の暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、このオプションを選択します。
- [Medium]：強度が中および高の暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、このオプションを選択します（デフォルト）。

d) [Integrity] を選択し、[Edit] をクリックします。
e) [SSH cipher security level] ドロップダウン リストから、次のいずれかのレベルを選択します。

- [All]：すべての暗号方式（hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96）を使用することを指定します。
- [Custom]：カスタム暗号ストリングを設定する場合はこのオプションを選択し、[Cipher algorithms/custom string] フィールドに各暗号ストリングをコロンで区切って入力します。
- [Fips]：FIPS 対応の暗号方式のみ（hmac-sha1 hmac-sha2-256 ）を指定します。
- [High]：強度が高の暗号方式のみ（ hmac-sha2-256）を指定します（デフォルト）。
- [Low]：強度が低、中、高の暗号方式（hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96）を使用する場合は、このオプションを選択します。

• [Medium]：強度が中および高の暗号方式（hmac-sha1 hmac-sha1-96）を指定します。

例

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

1. コンピュータで 4096 ビットの RSA 公開キーおよび秘密キーを生成します。

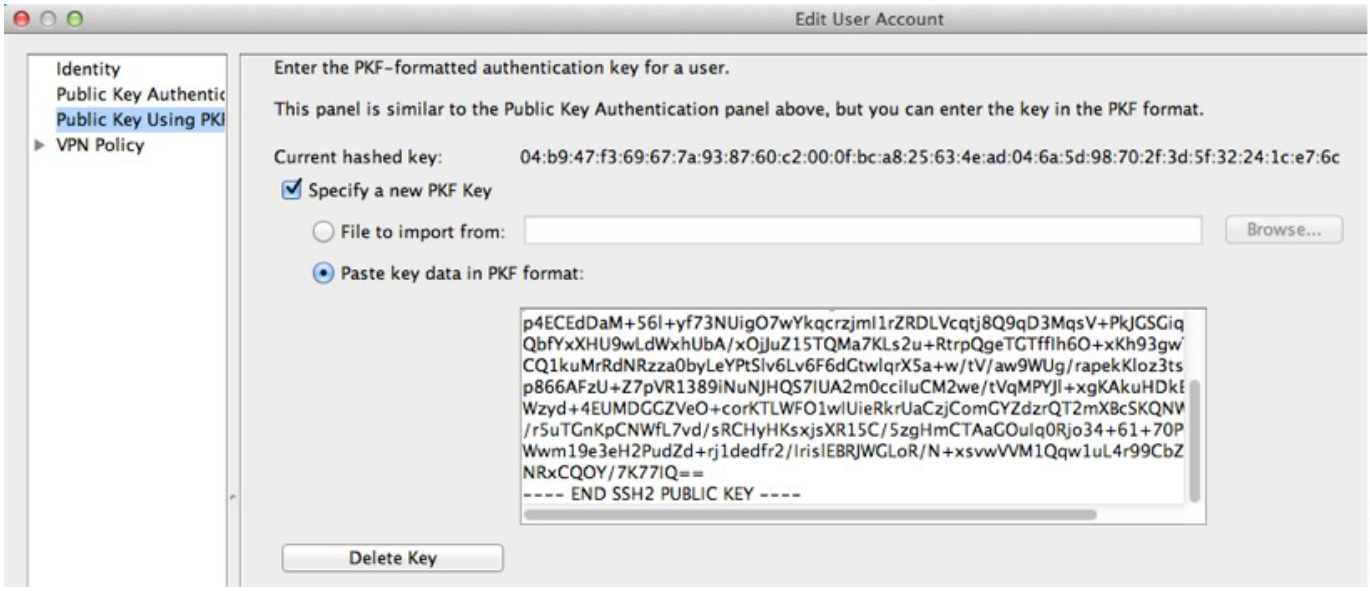
```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. キーをクリップボードにコピーします。

4. ASDM で、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** の順に選択し、ユーザー名を選択してから [Edit] をクリックします。[Public Key Using PKF] をクリックして、ウィンドウにキーを貼り付けます。



5. ユーザが ASA に SSH できることを確認します。パスワードには、キーペアの作成時に指定した SSH キーパスワードを入力します。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

次のダイアログボックスが、パスフレーズを入力するために表示されます。

一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Telnet アクセスの設定

この項では、Telnet に ASA アクセスを設定する方法について説明します。VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。
- ASA CLI に Telnet を使用してアクセスするには、ログイン パスワードを入力します。Telnet を使用する前に手動でパスワードを設定する必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択し、[Add] をクリックします。

[Add Device Access Configuration] ダイアログボックスが表示されます。

ステップ 2 [Telnet] を選択します。

ステップ 3 管理インターフェイスを選択し、許可するホスト IP アドレス設定して、[OK] をクリックします。

名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定（1149 ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

ステップ 4 （任意） [Telnet Timeout] を設定します。デフォルトのタイムアウト値は 5 分です。

ステップ 5 [Apply] をクリックします。

ステップ 6 Telnet で接続する前に、ログイン パスワードを設定します。デフォルトのパスワードはありません。

a) **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** の順に選択します。
b) [Telnet Password] 領域で [Change the password to access the console of the security appliance] チェックボックスをオンにします。
c) 古いパスワードを入力して（新しい ASA の場合はこのフィールドを空白にする）、新しいパスワードを入力してから、確認として新しいパスワードを再入力します。
d) [Apply] をクリックします。

ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定

ASDM またはクライアントレス SSL VPN を使用して ASA に接続するには、HTTPS を使用する必要があります。利便性のために、HTTP 管理接続を HTTPS にリダイレクトすることができます。たとえば、HTTP をリダイレクトすることによって、**http://10.1.8.4/admin/** または **https://10.1.8.4/admin/** と入力し、ASDM 起動ページで HTTPS アドレスにアクセスできます。

IPv4 と IPv6 の両方のトラフィックをリダイレクトできます。

始める前に

通常、ホスト IP アドレスを許可するアクセス ルールは必要ありません。ただし、HTTP リダイレクトのためには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[HTTP Redirect]** の順に選択します。

表には、現在設定されているインターフェイスと、リダイレクトがインターフェイスで有効化されているかどうかを示しています。

ステップ 2 ASDM に使用するインターフェイスを選択し、[Edit] をクリックします。

ステップ 3 [Edit HTTP/HTTPS Settings] ダイアログボックスで次のオプションを設定します。

- [Redirect HTTP to HTTPS]：HTTP 要求を HTTPS にリダイレクトします。
- [HTTP Port]：インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトは 80 です。

ステップ 4 [OK] をクリックします。

VPN トンネルを介した管理アクセスの設定

あるインターフェイスで VPN トンネルが終端している場合、別のインターフェイスにアクセスして ASA を管理するには、そのインターフェイスを管理アクセス インターフェイスとして指定する必要があります。たとえば、outside インターフェイスから ASA に入る場合は、この機能を使用して、ASDM、SSH、Telnet、または SNMP 経由で Inside インターフェイスに接続するか、outside インターフェイスから入るときに Inside インターフェイスに ping を実行できます。

（注） サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。次に、外部インターフェイスをポーリングして、SNMP が設定されている内部インターフェイスから情報を取得します。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの VPN アクセスはサポートされません。たとえば、VPN アクセスが外部インターフェイスにある場合、外部インターフェイスへの直接接続のみ開始できます。複数のアドレスを覚える必要がないように、ASA の直接アクセス可能インターフェイスの VPN を有効にし、名前解決を使用してください。

管理アクセスは、IPsec クライアント、IPsec サイト間、Easy VPN、AnyConnect SSL VPN クライアントの VPN トンネル タイプ経由で行えます。

始める前に

別個の管理/データ ルーティング テーブルでのルーティングを考慮すると、VPN の端末インターフェイスと管理アクセスインターフェイスは同じ種類である（つまり両方とも管理専用インターフェイスであるか、通常のデータ インターフェイスである）必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Interface]** の順に選択します。

ステップ 2 [Management Access Interface] ドロップダウン リストからセキュリティが最も高いインターフェイス（内部インターフェイス）を選択します。

Easy VPN およびサイト間トンネルでは、名前付き BVI を指定できます（ルーテッド モード）。

ステップ 3 [Apply] をクリックします。

管理インターフェイスが割り当てられ、変更内容が実行コンフィギュレーションに保存されます。

Firepower 2100 プラットフォーム モード データ インターフェイスでの FXOS の管理アクセスの設定

データインターフェイスからプラットフォームモードの Firepower 2100 の FXOS を管理する場合、SSH、HTTPS、および SNMP アクセスを設定できます。この機能は、デバイスをリモートで管理しつつ、管理 1/1 を隔離されたネットワークに維持する場合に役立ちます。これは、隔離されたネットワーク上の FXOS にアクセスするためのネイティブな方法です。この機能を有効にすると、ローカルアクセスに対してのみ管理 1/1 を使用し続けることができます。ただし、この機能を使用しながら FXOS の管理 1/1 からのリモートアクセスは許可することはでき

ません。この機能には、内部パス（デフォルト）を使用した ASA データ インターフェイスへのトラフィックの転送が必要で、FXOS 管理ゲートウェイを 1 つだけ指定できます。

ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタ フェースで ASA が使用するため予約されています。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。パケット宛先 IP アドレス（ASA インターフェイス IP アドレス）も、FXOS で使用する内部アドレスに変換されます。送信元アドレスは変更されません。トラフィックを返す場合、ASA は自身のデータ ルーティング テーブルを使用して正しい出力インターフェイスを決定します。管理アプリケーションの ASA データ IP アドレスにアクセスする場合、FXOS ユーザー名を使用してログインする必要があります。ASA ユーザー名は ASA 管理アクセスのみに適用されます。

ASA データ インターフェイスで FXOS 管理トラフィック開始を有効にすることもできます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバー アクセスなどに必要です。デフォルトでは、FXOS 管理トラフィック開始は、DNS および NTP のサーバー通信（スマート ソフトウェア ライセンシング通信で必要）用の ASA 外部インターフェイスで有効になっています。

始める前に

- シングル コンテキスト モードのみ。
- ASA 管理専用インターフェイスは除外します。
- ASA データ インターフェイスに VPN トンネルを使用して、FXOS に直接アクセスすることはできません。SSH の回避策として、ASA に VPN 接続し、*ASA* CLI にアクセスし、**connect fxos** コマンドを使用して FXOS CLI にアクセスします。SSH、HTTPS、および SNMPv3 は暗号化できるため、データ インターフェイスへの直接接続は安全です。
- FXOS ゲートウェイが ASA データインターフェイス（デフォルト）にトラフィックを転送するように設定されていることを確認します。ゲートウェイの設定の詳細については、『getting started guide』を参照してください。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Firewall]** > **[Advanced]** > **[FXOS Remote Management]** を選択します。

ステップ 2 FXOS リモート管理を有効にします。

a) ナビゲーション ウィンドウで、[HTTPS]、[SNMP]、または [SSH] を選択します。

b) [Add] をクリックし、管理を許可する [Interface] を設定し、接続を許可する [IP Address] を設定し、[OK] をクリックします。

プロトコル タイプごとに複数のエントリを作成できます。以下のデフォルト値を使用しない場合は、[Port] を設定します。

- HTTPS デフォルト ポート：3443

- SNMP デフォルト ポート：3061
- SSH デフォルト ポート：3022

ステップ 3 FXOS が ASA インターフェイスから管理接続を開始できるようにします。

a) ナビゲーション ウィンドウで [FXOS Traffic Initiation] を選択します。
b) [Add] をクリックし、FXOS 管理トラフィックを送信する必要がある ASA インターフェイスを有効にします。デフォルトでは、外部インターフェイスは有効になっています。

ステップ 4 [Apply] をクリックします。

ステップ 5 管理 1/1 上の Firepower Chassis Manager に接続します（デフォルトでは、https://192.168.45.45、ユーザー名：**admin**、パスワード：**Admin123**）。

ステップ 6 [Platform Settings] タブをクリックし、[SSH]、[HTTPS]、または [SNMP] を有効にします。

SSH と HTTPS はデフォルトで有効になっています。

ステップ 7 [Platform Settings] タブで、管理アクセスを許可するように [Access List] を設定します。デフォルトでは、SSH および HTTPS は管理 1/1 192.168.45.0 ネットワークのみを許可します。ASA の [FXOS Remote Management] 設定で指定したアドレスを許可する必要があります。

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザー EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソール ポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

手順

ステップ 1 **[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Console Timeout]** の順に選択します。

ステップ 2 新しいタイムアウト値を分単位で定義します。無制限の時間を指定する場合は、「0」と入力します。デフォルト値は 0 です

ステップ 3 [Apply] をクリックします。

タイムアウト値の変更が実行コンフィギュレーションに保存されます。

CLI プロンプトのカスタマイズ

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。

state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、state キーワードに対して次の値が表示されます。 • [act]：フェールオーバーが有効であり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailover]：フェールオーバーは無効であり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーは無効であり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタリングの場合、制御とデータの値が表示されます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Command Line (CLI)]** > **[CLI Prompt]** の順に選択します。

ステップ 2 次のいずれかを実行してプロンプトをカスタマイズします。

- [Available Prompts] リストで属性をクリックしてから、[Add] をクリックします。プロンプトには複数の属性を追加できます。属性が [Available Prompts] リストから [Selected Prompts] リストに移動します。
- [Selected Prompts] リストで属性をクリックしてから、[Delete] をクリックします。属性が [Selected Prompts] リストから [Available Prompts] リストに移動します。
- [Selected Prompts] リストで属性をクリックして、[Move Up] または [Move Down] をクリックして属性の表示順序を変更します。

プロンプトが変化して、[CLI Prompt Preview] フィールドに表示されます。

ステップ 3 **Apply** をクリックします。

変更されたプロンプトが、実行コンフィギュレーションに保存されます。

ログイン バナーの設定

ユーザーが ASA に接続するとき、ログインする前、または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

始める前に

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。「ウェルカム」や「お願いします」などの表現は侵入者を招き入れているような印象を与えるので使用しないでください。以下のバナーでは、不正アクセスに対して正しい表現を設定しています。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- バナーが追加された後、次の場合に ASA に対する Telnet または SSH セッションが終了する可能性があります。
  - バナー メッセージを処理するためのシステム メモリが不足している場合。
  - バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。
- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Command Line (CLI)]** > **[Banner]** の順に選択します。

ステップ 2 CLI 用に作成するバナー タイプ用のフィールドにバナー テキストを追加します。

- [session (exec)] バナーは、ユーザーが CLI で特権 EXEC モードにアクセスした場合に表示されます。
- [login] バナーは、ユーザが CLI にログインした場合に表示されます。
- [message-of-the-day (motd)] バナーは、ユーザーが CLI に初めて接続する場合に表示されます。
- [ASDM] バナーは、ユーザーが認証を受けた後 ASDM に接続した場合に表示されます。ユーザーは、次のいずれかのオプションを使用して、表示されたバナーを消去できます。
  - [Continue]：バナーを消去して、ログインを完了します。

- [Disconnect]：バナーを消去して、接続を終了します。

- 使用できるのは、改行（Enter キー）も含めて ASCII 文字だけです。ただし、改行文字は 2 文字に相当します。
- また、タブ文字は、CLI バージョンでは無視されるため、バナーには使用しないでください。
- RAM およびフラッシュ メモリに関するもの以外、バナーに長さ制限はありません。
- ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。
- システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** という文字列を使用することにより、コンテキスト内でバナー テキストを使用できます。

ステップ 3 [Apply] をクリックします。

新しいバナーが、実行コンフィギュレーションに保存されます。

管理セッション クォータの設定

ASA で許可する ASDM、SSH、および Telnet の同時最大セッション数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソール セッションをブロックできません。

（注） マルチコンテキストモードではASDMセッションの数を設定することはできず、最大セッション数は 5 で固定されています。

（注） また、最大管理セッション（SSHなど）のコンテキストあたりのリソース制限を設定した場合は、小さい方の値が使用されます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下のコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]** の順に選択します。

ステップ 2 同時セッションの最大数を入力します。

- **Aggregate**：1 ～ 15 のセッションの集約数を設定します。デフォルトは 15 です。
- **HTTP Sessions**：1 ～ 5 の HTTPS（ASDM）セッションの最大数を設定します。デフォルトは 5 分です。
- **SSH Sessions**：1 ～ 5 の SSH セッションの最大数を設定します。デフォルトは 5 分です。
- **Telnet Sessions**：1 ～ 5 の Telnet セッションの最大数を設定します。デフォルトは 5 分です。
- **User Sessions**：1 ～ 5 のユーザーごとのセッションの最大数を設定します。デフォルトは 5 分です。

ステップ 3 [Apply] をクリックして、設定の変更を保存します。

システム管理者用 AAA の設定

この項では、システム管理者の認証、管理許可、コマンド許可を設定する方法について説明します。

管理認証の設定

CLI および ASDM アクセスの認証を設定します。

管理認証について

ASA へのログイン方法は、認証を有効にしているかどうかによって異なります。

SSH 認証の概要

認証ありまたは認証なしでの SSH アクセスについては、次の動作を参照してください。

- 認証なし：SSH は認証なしでは使用できません。
- 認証あり：SSH 認証を有効にした場合は、AAA サーバーまたはローカルユーザーデータベースに定義されているユーザー名とパスワードを入力します。公開キーの認証では、ASA はローカル データベースのみをサポートします。 SSH 公開キー認証を設定した場合、ASA ではローカル データベースを暗黙的に使用します。ログインにユーザー名とパスワードを使用する場合に必要なのは、SSH 認証を明示的に設定することのみです。ユーザー EXEC モードにアクセスします。

Telnet 認証の概要

認証の有無にかかわらず、Telnet アクセスについては、次の動作を参照してください。

- 認証なし：Telnet の認証を有効にしていない場合は、ユーザー名を入力しません。ログイン パスワードを入力します。デフォルトのパスワードはありません。したがって、ASA へ Telnet 接続するには、パスワードを設定する必要があります。ユーザー EXEC モードにアクセスします。
- 認証あり：Telnet認証を有効にした場合は、AAA サーバーまたはローカルユーザーデータベースに定義されているユーザー名とパスワードを入力します。ユーザー EXEC モードにアクセスします。

ASDM 認証の概要

認証ありまたは認証なしでのASDMアクセスに関しては、次の動作を参照してください。AAA 認証の有無にかかわらず、証明書認証を設定することも可能です。

- 認証なし：デフォルトでは、ブランクのユーザー名と **enable password** コマンドを使用して ASDM にログインできます。空白のままにしないように、できるだけ早くイネーブル パスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （749 ページ）を参照してください。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDMにログインしたときには、この動作は適用されません。ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力した場合は、ASDMによってローカル データベースで一致がチェックされることに注意してください。
- 証明書認証（シングル、ルーテッドモードのみ）：ユーザーに有効な証明書を要求できます。証明書のユーザー名とパスワードを入力すると、ASA が PKI トラストポイントに対して証明書を検証します。
- AAA 認証：ASDM（HTTPS）認証を有効にした場合は、AAA サーバーまたはローカル ユーザーデータベースに定義されているユーザー名とパスワードを入力します。これで、ブランクのユーザー名とイネーブル パスワードで ASDM を使用できなくなりました。
- AAA 認証と証明書認証の併用（シングル、ルーテッド モードのみ）：ASDM（HTTPS）認証を有効にした場合は、AAA サーバーまたはローカル ユーザー データベースに定義されているユーザー名とパスワードを入力します。証明書認証用のユーザー名とパスワードが異なる場合は、これらも入力するように求められます。ユーザー名を証明書から取得してあらかじめ入力しておくよう選択できます。

シリアル認証の概要

認証ありまたは認証なしでのシリアル コンソール ポートへのアクセスに関しては、次の動作を参照してください。

- 認証なし：シリアルアクセスの認証を有効にしていない場合は、ユーザー名、パスワードを入力しません。ユーザー EXEC モードにアクセスします。

- 認証あり：シリアルアクセスの認証を有効にした場合は、AAA サーバーまたはローカル ユーザーデータベースで定義されているユーザー名とパスワードを入力します。ユーザー EXEC モードにアクセスします。

enable 認証の概要

ログイン後に特権EXECモードに入るには、**enable**コマンドを入力します。このコマンドの動作は、認証がイネーブルかどうかによって異なります。

- 認証なし：enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力します。デフォルトは空白です。**enable** コマンドを最初に入力したときに、それを変更するように求められます。ただし、enable 認証を使用しない場合、**enable**コマンドを入力した後は、特定のユーザーとしてログインしていません。これにより、コマンド認可などユーザーベースの各機能が影響を受けることがあります。ユーザー名を維持するには、enable 認証を使用してください。
- 認証あり：enable 認証を設定した場合は、ASA はプロンプトにより AAA サーバーまたはローカルユーザーデータベースで定義されているユーザー名とパスワードを要求します。この機能は、ユーザーが入力できるコマンドを判別するためにユーザー名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** コマンドによりユーザー名が維持されますが、認証をオンにするための設定は必要ありません。

⚠

注意 CLI にアクセスできるユーザーや特権 EXEC モードを開始できないようにするユーザーをローカルデータベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザーは、CLI で自分のパスワードを使用して特権EXECモード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理でローカルデータベースではなく AAA サーバーを使用してログイン コマンドを回避するか、またはすべてのローカル ユーザーをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザーを制御できます。

ホスト オペレーティング システムから ASA へのセッション

一部のプラットフォームでは、ASAの実行を別のアプリケーションとしてサポートしています（例：Firepower 4100/9300 の ASA）。ホスト オペレーティング システムから ASA へのセッションの場合、接続のタイプに応じてシリアルおよびTelnet認証を設定できます。たとえば、プラットフォームモードの Firepower 2100 では、**connect asa** コマンドはシリアル接続を使用します。

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はこれらのセッションにも適用されます。この場合、管理コンテキストの AAA サーバーまたはローカル ユーザー データベースが使用されます。

CLI、ASDM、および enable コマンド アクセス認証の設定

始める前に

- Telnet、SSH、または HTTP アクセスを設定します。
- 外部認証の場合は、AAA サーバー グループを設定します。ローカル認証の場合は、ローカル データベースにユーザーを追加します。
- HTTP 管理認証では、AAA サーバー グループの SDI プロトコルをサポートしていません。
- この機能は、**ssh authentication** コマンドによるローカル ユーザー名に関する SSH 公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。この機能は、ユーザー名とパスワードにのみ影響します。ローカル ユーザーが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワード アクセスを許可する必要があります。

手順

ステップ 1 **enable** コマンドを使用するユーザーを認証する場合は、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authentication]** の順に選択し、次の設定を行います。

a) [Enable] チェックボックスを選択します。
b) サーバー グループ名または LOCAL データベースを選択します。
c) （オプション）AAA サーバーを選択する場合は、AAA サーバーが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。

ステップ 2 CLI または ASDM にアクセスするユーザーを認証する場合は、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authentication]** の順に選択し、次の設定を行います。

a) 次のチェックボックスをオンにします（複数可）。
   - [HTTP/ASDM]：HTTPS を使用して ASA にアクセスする ASDM クライアントを認証します。
   - [Serial]：コンソール ポートを使用して ASA にアクセスするユーザーを認証します。プラットフォーム モードの Firepower 2100 の場合、このキーワードは **connect asa** コマンドを使用して FXOS からアクセスする仮想コンソールに影響します。
   - **SSH**：SSH を使用して ASA にアクセスするユーザーを認証します（パスワードのみ。公開キー認証では暗黙のうちにローカル データベースが使用されます）。
   - [Telnet]：Telnet を使用して ASA にアクセスするユーザーを認証します。

b) チェックボックスをオンにしたサービスごとに、サーバー グループ名または LOCAL データベースを選択します。

c) （オプション）AAA サーバーを選択する場合は、AAA サーバーが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。[Use LOCAL when server group fails] チェックボックスをオンにします。ローカル データベースでは AAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。

ステップ 3 [Apply] をクリックします。

ASDM 証明書認証の設定

AAA 認証の有無にかかわらず証明書認証を必須にできます。ASA は証明書を PKI トラストポイントに照合して検証します。

始める前に

この機能は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** の順に選択します。

ステップ 2 [Specify the interface requires client certificate to access ASDM] 領域で [Add] をクリックし、インターフェイスとオプションで証明書マップを指定します。認証が成功するには、その証明書マップと一致している必要があります。

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。証明書マップを作成するには、**[Configuration]** > **[Site-to-Site VPN]** > **[Advanced]** > **[IPSec]** > **[Certificate to Connection Map]** > **[Rules]** を表示します。

ステップ 3 （任意） ASDM で証明書からユーザー名を抽出する際に使用する属性を設定するには、**[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Certificate Rule]** の順に選択します。

次の方法の中から 1 つを選択してください。

- [Specify the Certificate Fields to be used]：[Primary Field] ドロップダウン リストと [Secondary Field] ドロップダウン リストから値を選択します。
- **[Use the entire DN as the username]**
- [Use script to select username]：[Add] をクリックし、スクリプトの内容を追加します。

認証を求めるプロンプトにユーザー名を事前入力するには、[Prefill Username] チェックボックスをオンにします。そのユーザー名が最初に入力したものと異なる場合、最初のユーザー名が事前入力された新しいダイアログボックスが表示されます。そこに、認証用のパスワードを入力できます。

デフォルトでは、ASDM は CN OU 属性を使用します。

ステップ 4 [Apply] をクリックします。

管理許可による CLI および ASDM アクセスの制限

ASA ではユーザーの認証時に管理アクセス ユーザーとリモート アクセス ユーザーを区別できるようになっています。ユーザー ロールを区別することで、リモート アクセス VPN ユーザーやネットワーク アクセス ユーザーが ASA に管理接続を確立するのを防ぐことができます。

始める前に

RADIUS または LDAP（マッピング済み）ユーザー

ユーザーが LDAP 経由で認証されると、ネイティブ LDAP 属性およびその値が Cisco ASA 属性にマッピングされ、特定の許可機能が提供されます。Cisco VSA CVPN3000-Privilege-Level の値を 0 ～ 15 の範囲で設定した後、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザーにどのタイプのサービスを付与するかを指定するために使用されます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザーの権限レベルを指定するために使用されます。

TACACS+ ユーザー

「service=shell」で許可が要求され、サーバーは PASS または FAIL で応答します。

ローカル ユーザー

指定したユーザー名の [Access Restriction] オプションを設定します。アクセス制限のデフォルト値は [Full Access] です。この場合、[Authentication] タブのオプションで指定されたすべてのサービスに対して、フル アクセスが許可されます。

管理許可の属性

管理許可の AAA サーバー タイプおよび有効な値については、次の表を参照してください。ASA ではこれらの値を使用して管理アクセス レベルを決定します。

Management Level	RADIUS/LDAP の（マッピングされた）属性	TACACS+ 属性	ローカル データベースの属性
[Full Access]： [Authentication] タブのオプションで指定されたすべてのサービスに対してフル アクセスが許可されます。	Service-Type 6（アドミニストレーティブ）、Privilege-Level 1	PASS、特権レベル 1	admin
[Partial Access]：**[Authentication]** タブのオプションで設定すると、CLI または ASDM に対するアクセスが許可されます。ただし、[Enable] オプションを使用して **enable** 認証を設定する場合、CLI ｙユーザーは **enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。	Service-Type 7（NAS プロンプト）、Privilege-Level 2 以上 Framed (2) および Login (1) サービス タイプは同様に扱われます。	PASS、特権レベル 2 以上	nas-prompt
[No Access]：管理アクセスが拒否されます。ユーザーは [Authentication] タブのオプションで指定されたいずれのサービスも使用できません（[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザーは、引き続き自身のリモート アクセス セッションを認証および終了できます。他のすべてのサービス タイプ（ボイス、ファクスなど）も同様に処理されます。	Service-Type 5（アウトバウンド）	FAIL	remote-access

その他のガイドライン

- シリアル コンソール アクセスは管理許可に含まれません。
- この機能を使用するには、管理アクセスに AAA 認証も設定する必要があります。CLI、ASDM、およびenable コマンド アクセス認証の設定 （1160 ページ）を参照してください。
- 外部認証を使用する場合は、この機能をイネーブルにする前に、AAA サーバー グループを設定しておく必要があります。
- HTTP 許可は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 HTTP セッションの管理許可をイネーブルにするには、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択し、[Enable Authorization for ASA Command Access] 領域の [HTTP] チェックボックスをオンにします。

（注） ASA コマンドアクセスを設定するには、ローカル コマンド許可の設定（1166ページ）を参照してください。

ステップ 2 Telnet および SSH セッションの管理許可をイネーブルにするには、**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択し、[Perform authorization for exec shell access] 領域の [Enable] チェックボックスをオンにします。

ステップ 3 [Remote] または [Local] オプション ボタンを選択して、EXEC シェル アクセスの許可に使用するサーバーを指定します。

ステップ 4 管理認可をイネーブルにするには、[Allow privileged users to enter into EXEC mode on login] チェックボックスをオンにします。

[auto-enable] オプションを選択すると、フル アクセスが許可されたユーザーが直接特権 EXEC モードを開始できます。それ以外では、ユーザーはユーザー EXEC モードになります。

コマンド認可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザーが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザー EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバー特権レベル

コマンド認可について

コマンド認可を有効にし、承認済みのユーザーにのみコマンド入力を許容することができます。

サポートされるコマンド認可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカル ユーザー、RADIUS ユーザー、または LDAP ユーザー（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザーをローカル データベース、RADIUS、または LDAP サーバーで定義されている特権レベルに所属させます。ユーザーは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザーは、初めてログインするときに、ユーザー EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザーは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザーが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可を有効にするまで使用されません。

- TACACS+ サーバー特権レベル：TACACS+ サーバーで、ユーザーまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザーが入力するすべてのコマンドは、TACACS+ サーバーで検証されます。

セキュリティ コンテキストとコマンド許可

AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。この設定により、異なるセキュリティ コンテキストに対して異なるコマンド許可を実行できます。

セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザー名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。

（注） システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

コマンド権限レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- **イネーブル化**
- **help**
- **show history**

- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、configure コマンドも同じレベルに移動してください。このようにしないと、ユーザーはコンフィギュレーション モードに入ることができません。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザーを特定の特権レベルに定義でき、各ユーザーは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカル データベース、RADIUS サーバー、または LDAP サーバー（LDAP 属性を RADIUS 属性にマッピングする場合）に定義されているユーザー特権レベルをサポートしています。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択します。

ステップ 2 **[Enable authorization for ASA command access]** > **[Enable]** チェック ボックスをオンにします。

ステップ 3 [Server Group] ドロップダウン リストから [LOCAL] を選択します。

ステップ 4 ローカル コマンド許可をイネーブルにすると、オプションで、特権レベルを個々のコマンドまたはコマンド グループに手動で割り当てたり、事前定義済みユーザー アカウント特権をイネーブルにしたりできます。

- 事前定義のユーザー アカウント特権を使用するには、[Set ASDM Defined User Roles] をクリックします。

  [ASDM Defined User Roles Setup] ダイアログボックスが表示されます。[Yes] をクリックすると、事前定義済みユーザー アカウント特権を使用できるようになります。事前定義済みユーザー アカウント特権には、[Admin]（特権レベル 15、すべての CLI コマンドへのフル アクセス権）、[Read Only]（特権レベル 5、読み取り専用アクセス権）、[Monitor Only]（特権レベル 3、[Monitoring] セクションへのアクセス権のみ）があります。

- コマンド レベルを手動で設定するには、[Configure Command Privileges] をクリックします。

[Command Privileges Setup] ダイアログボックスが表示されます。[Command Mode] ドロップダウン リストから [All Modes] を選択すると、すべてのコマンドを表示できます。代わりに、コンフィギュレーション モードを選択し、そのモードで使用可能なコマンドを表示することもできます。たとえば、[context] を選択すると、コンテキスト コンフィギュレーション モードで使用可能なすべてのコマンドを表示できます。コンフィギュレーション モードだけでなく、ユーザー EXEC モードや特権 EXEC モードでも入力が可能で、かつモードごとに異なるアクションが実行されるようなコマンドを使用する場合は、これらのモードに対して別個に特権レベルを設定できます。

[Variant] カラムには、[show]、[clear]、または [cmd] が表示されます。特権は、コマンドの show 形式、clear 形式、または configure 形式に対してのみ設定できます。コマンドの configure 形式は、通常、未修正コマンド（show または clear プレフィックスなしで）または no 形式として、コンフィギュレーションの変更を引き起こす形式です。

コマンドのレベルを変更する場合は、コマンドをダブルクリックするか、[Edit] をクリックします。レベルは 0 ～ 15 の範囲で設定できます。設定できるのは、main コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

表示されているすべてのコマンドのレベルを変更する場合は、[Select All] をクリックした後に、[Edit] をクリックします。

[OK] をクリックして変更内容を確定します。

ステップ 5 （任意） **[Perform authorization for exec shell access]** > **[Enable]** チェック ボックスをオンにして、コマンド認可のための AAA ユーザーを有効にします。このオプションを入力しない場合、ASA は、ローカル データベース ユーザの特権レベルだけをサポートし、他のタイプのユーザをすべてデフォルトでレベル 15 に割り当てます。

さらに、このコマンドは管理認証を有効にします。管理許可による CLI および ASDM アクセスの制限 （1162 ページ）を参照してください。

ステップ 6 [Apply] をクリックします。

許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

TACACS+ サーバーでのコマンドの設定

グループまたは個々のユーザーの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバーでコマンドを設定できます。サードパーティの TACACS+ サーバーの場合は、コマンド許可サポートの詳細については、ご使用のサーバーのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA は、シェル コマンドとして許可するコマンドを送信し、TACACS+サーバーでシェル コマンドとしてコマンドを設定します。

  注 Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

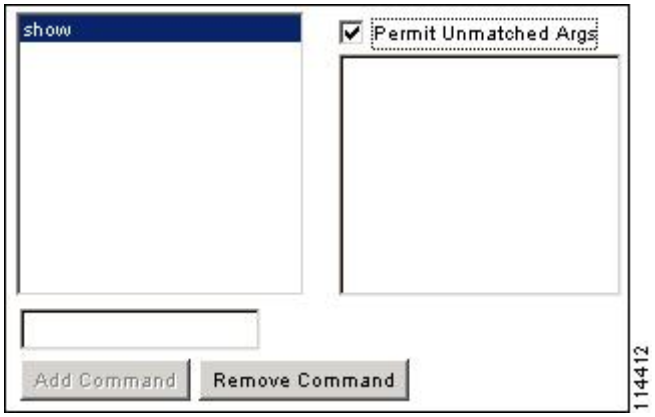
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド フィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

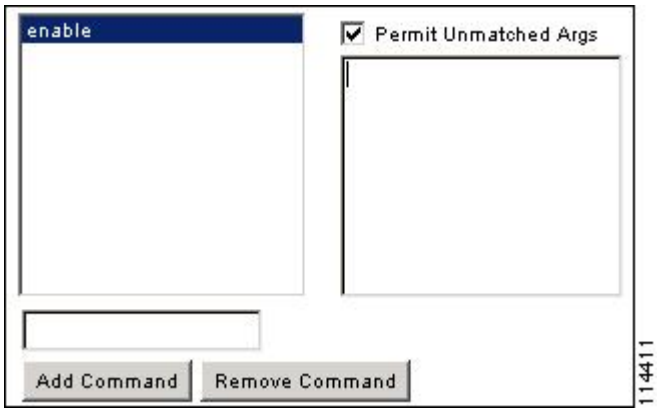
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（次の図を参照）。

  図 *72 :* 関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する必要があります（次の図を参照）。

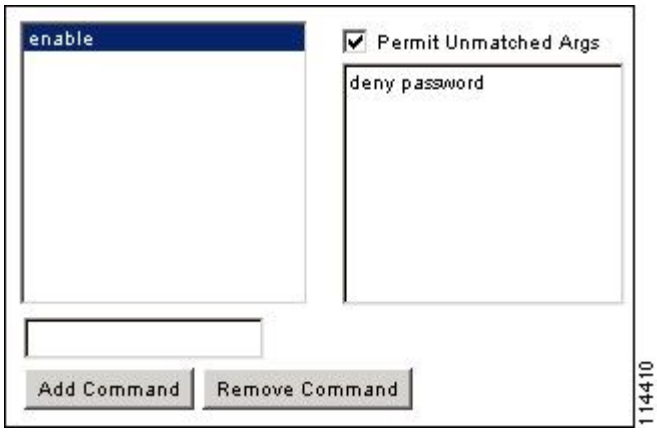
図 *73* : 単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンドフィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスをオンにしてください（次の図を参照）。

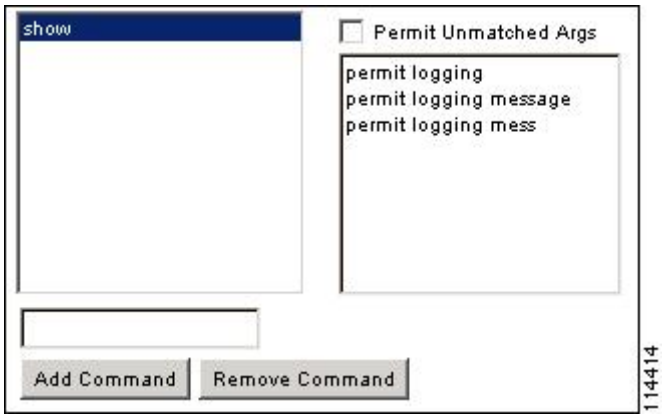
  図 *74* : 引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバーに送信します。

  たとえば、**sh log** と入力すると、ASA は完全なコマンド **show logging** を TACACS+ サーバーに送信します。一方、**sh log mess** と入力すると、ASA は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバーに送信します。省略形を予想して同じ引数の複数のスペルを設定できます（次の図を参照）。

図 *75 :* 省略形の指定



- すべてのユーザーに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - イネーブル化
  - **help**
  - **show history**
  - **login**
  - **logout**
  - **pager**
  - **show pager**
  - **clear pager**
  - **quit**
  - **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド認可をイネーブルにし、ユーザーが CLI でコマンドを入力すると、ASA はそのコマンドとユーザー名を TACACS+ サーバーに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバーで定義されたユーザーとして ASA にログインしていること、および ASA の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザーとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロック アウトされた場合、通常はASAを再始動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバー システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバー プールに、インターフェイス 1 に接続された 1 つのサーバーとインターフェイス 2 に接続された別のサーバーを含めます。TACACS+ サーバーが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。

TACACS+ サーバーを使用したコマンド許可を設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Authorization]** の順に選択します。

ステップ 2 **[Enable authorization for command access]** > **[Enable]** チェックボックスをオンにします。

ステップ 3 [Server Group] ドロップダウン リストから AAA サーバー グループ名を選択します。

ステップ 4 （オプション）AAA サーバーが使用不可になった場合のフォールバック方式としてローカル データベースが使用されるように ASA を設定できます。設定するには、[Use LOCAL when server group fails] チェックボックスをオンにします。ローカルデータベースではAAAサーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASAのプロンプトでは、どの方式が使用されているかが示されないためです。必ずローカルデータベースのユーザーとコマンド特権レベルを設定してください。

ステップ 5 [Apply] をクリックします。

コマンド許可設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ローカル データベース ユーザーのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。

パスワード ポリシーはローカル データベースを使用する管理ユーザーに対してのみ適用されます。ローカルデータベースを使用するその他のタイプのトラフィック（VPNやAAAによるネットワーク アクセスなど）や、AAA サーバーによって認証されたユーザーには適用されません。

パスワードポリシーの設定後は、自分または別のユーザーのパスワードを変更すると、新しいパスワードに対してパスワードポリシーが適用されます。既存のパスワードについては、現行のポリシーが適用されます。新しいポリシーは、[User Accounts] ペインおよび [Change My Password] ペインを使用したパスワードの変更に適用されます。

始める前に

- ローカル データベースを使用して CLI または ASDM アクセスの AAA 認証を設定します。
- ローカル データベース内にユーザー名を指定します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Password Policy]** の順に選択します。

ステップ 2 次のオプションを任意に組み合わせて設定します。

- [Minimum Password Length]：パスワードの最小長を入力します。有効値の範囲は 3 ～ 64 文字です。推奨されるパスワードの最小長は 8 文字です。
- [Lifetime]：リモート ユーザー（SSH、Telnet、HTTP）のパスワードの有効期間を日数で指定します。コンソール ポートのユーザーが、パスワードの有効期限切れでロックされることはありません。有効な値は、0 ～ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

  パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモート ユーザーのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。

  - 他の管理者にパスワードを変更してもらいます。
  - 物理コンソール ポートにログインして、パスワードを変更します。

- [Minimum Number Of]：次のタイプの最短文字数を指定します。
  - [Numeric Characters]：パスワードに含めなければならない数字の最小文字数を入力します。有効な値は、0 ～ 64 文字です。デフォルト値は 0 です
  - [Lower Case Characters]：パスワードに含めなければならない小文字の最小文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  - [Upper Case Characters]：パスワードに含めなければならない大文字の最小文字数を入力します。有効値の範囲は 0 ～ 64 文字です。デフォルト値は 0 です
  - [Special Characters]：パスワードに含めなければならない特殊文字の最小文字数を入力します。有効値の範囲は 0 ～ 64 文字です。特殊文字には、!、@、#、$、%、^、&、*、(および) が含まれます。デフォルト値は 0 です。
  - [Different Characters from Previous Password]：新しいパスワードと古いパスワードで変えなければならない最小文字数を入力します。有効な値は、0～64 文字です。デフォルト値は 0 です文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

- [Enable Reuse Interval]：以前に使用された 2 ～ 7 個のパスワードと一致するパスワードの再利用を禁止することができます。以前のパスワードは、**password-history** コマンドを使

用して、暗号化された形で各ユーザー名の設定に保存されます。このコマンドをユーザーが設定することはできません。

- [Prevent Passwords from Matching Usernames]：ユーザー名と一致するパスワードを禁止します。

ステップ 3 （オプション）[Enable Password and Account Protection] チェックボックスをオンにして、ユーザーが [User Accounts] ペインではなく、[Change My Password] ペインでパスワードを変更することを要件とします。デフォルト設定はディセーブルです。どちらの方法でも、ユーザーはパスワードを変更することができます。

この機能をイネーブルにして、[User Accounts] ペインでパスワードを変更しようとすると、次のエラー メッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

ステップ 4 [Apply] をクリックして、設定内容を保存します。

パスワードの変更

パスワードポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワードポリシー認証をイネーブルにした場合は、このパスワード変更のスキームが必須です。パスワードポリシー認証がイネーブルでない場合は、このメソッドを使用することも、直接ユーザーアカウントを変更することもできます。

username パスワードを変更するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Change Password]** の順に選択します。
ステップ 2 古いパスワードを入力します。
ステップ 3 新しいパスワードを入力します。
ステップ 4 確認のために新しいパスワードを再度入力します。
ステップ 5 [Make Change] をクリックします。
ステップ 6 [Save] アイコンをクリックして、実行コンフィギュレーションに変更を保存します。

ログインの履歴を有効にして表示する

デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。

始める前に

- ログイン履歴はユニット（装置）ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。
- ログインの履歴データは、リロードされると保持されなくなります。
- 1 つ以上の CLI 管理方式（SSH、Telnet、シリアル コンソール）でローカル AAA 認証をイネーブルにした場合、AAA サーバーのユーザー名またはローカルデータベースのユーザー名にこの機能が適用されます。ASDM のログインは履歴に保存されません。

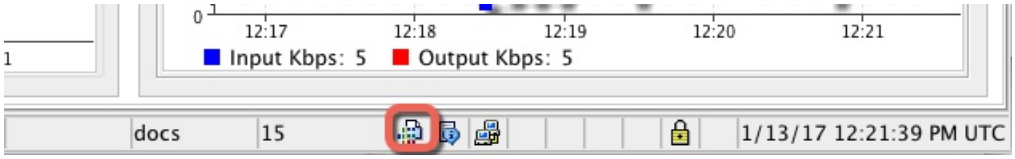
手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Login History]** の順に選択します。

ステップ 2 [管理者のログイン履歴レポート設定]チェックボックスをオンにします。この機能は、デフォルトでイネーブルにされています。

ステップ 3 [期間] を 1 ～ 365 日の間で設定します。デフォルトは 90 です。

ステップ 4 ログイン履歴を表示するには、いずれかの ASDM 画面で [Status] バーにある [Login History] アイコンをクリックします。



すべてのユーザーのログイン履歴がダイアログボックスに表示されます。

管理アクセス アカウンティングの設定

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバーに送信できます。ユーザーがログインするとき、ユーザーが **enable** コマンドを入力するとき、またはユーザーがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバーは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンド アカウンティングを設定するには、次の手順を実行します。

手順

ステップ 1 **enable** コマンドを入力したユーザーのアカウンティングを有効にするには、次の手順を実行します。

a) **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Access]** > **[Accounting]** の順に選択し、**[Require accounting to allow accounting of user activity]** > **[Enable]** チェックボックスをオンにします。

b) RADIUS または TACACS+ サーバー グループ名を選択します。

ステップ 2 ユーザーが Telnet、SSH、またはシリアル コンソールを使用して ASA にアクセスした場合にそのユーザーのアカウンティングを有効化するには、次の手順を実行します。

a) [Require accounting for the following types of connections] 領域で、[Serial]、[SSH]、または [Telnet] チェックボックスをオンにします。

b) 各接続タイプの RADIUS または TACACS+ サーバー グループ名を選択します。

ステップ 3 コマンド アカウンティングを設定するには、次の手順を実行します。

a) [Require accounting for the following types of connections] エリアで [Enable] チェックボックスをオンにします。

b) TACACS+ サーバー グループ名を選択します。RADIUS はサポートされていません。

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバーに送信できます。

c) [Command Privilege Setup] ダイアログボックスを使用してコマンド特権レベルをカスタマイズする際、[Privilege level] ドロップダウン リストで最小特権レベルを指定することで、ASA のアカウンティング対象となるコマンドを制限できます。最小特権レベルよりも下のコマンドは、ASA で処理の対象となりません。

ステップ 4 [Apply] をクリックします。

アカウンティング設定が割り当てられ、その変更内容が実行コンフィギュレーションに保存されます。

ロックアウトからの回復

状況によっては、コマンド許可やCLI認証をオンにすると、ASA CLIからロックアウトされる場合があります。通常は、ASAを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。

次の表に、一般的なロックアウト条件とその回復方法を示します。

表 *54 : CLI* 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザーが設定していない。	ローカル データベース内にユーザーが存在しない場合は、ログインできず、ユーザーの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザーを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバーがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバーが到達不能である場合は、ログインもコマンドの入力もできません。	**1.** ログインし、パスワードと AAA コマンドをリセットします。 **2.** サーバーがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	**1.** ASA でネットワーク コンフィギュレーションが正しくないためにサーバーが到達不能である場合は、スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 **2.** サーバーがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。
TACACS+ コマンド許可	十分な特権のないユーザーまたは存在しないユーザーとしてログインした。	コマンド許可がイネーブルになりますが、ユーザーはこれ以上コマンドを入力できなくなります。	TACACS+ サーバーのユーザー アカウントを修正します。 TACACS+ サーバーへのアクセス権がなく、ASA をすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル コマンド許可	十分な特権のないユーザーとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザーはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザー レベルを変更することができます。

デバイス アクセスのモニターリング

- **[Monitoring] > [Properties] > [Device Access] > [ASDM/HTTPS/Telnet/SSH Sessions]**

  上部ペインには、ASDM、HTTPS、およびTelnetのセッションを介して接続するユーザーの接続タイプ、セッション ID、および IP アドレスが示されます。特定のセッションを切断するには、[Disconnect] をクリックします。

  下部ペインには、クライアント、ユーザー名、接続ステータス、ソフトウェア バージョン、入力暗号化タイプ、出力暗号化タイプ、入力 HMAC、出力 HMAC、SSH セッション ID、残りのキー再生成データ、残りのキー再生成時間、データベースのキー再生成、時間ベースのキー再生成、最後のキー再生成の時間が表示されます。特定のセッションを切断するには、[Disconnect] をクリックします。

- **[Monitoring] > [Properties] > [Device Access] > [Authenticated Users]**

  このペインには、AAAサーバーによって認証されたユーザーのユーザー名、IPアドレス、ダイナミックACL、非活動タイムアウト（存在する場合）、および絶対タイムアウトが一覧表示されます。

- **[Monitoring] > [Properties] > [Device Access] > [AAA Locked Out Users]**

  このペインには、ロックアウトされたAAAローカル ユーザーのユーザー名、失敗した認証の試行回数、およびユーザーがロックアウトされた回数が一覧表示されます。ロックアウトされた特定のユーザーをクリアするには、[Clear Selected Lockout] をクリックします。ロックアウトされたすべてのユーザーをクリアするには、[Clear All Lockouts] をクリックします。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

管理アクセスの履歴

表 *55 :* 管理アクセスの履歴

機能名	プラットフォームリリース	説明
SNMP 向け管理アクセス	9.14(2)	サイト間 VPN 経由のセキュアな SNMP ポーリングを実現するための VPN 設定の一環として、VPN トンネル経由の管理アクセスを設定する際に、外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。
HTTPS アイドルタイムアウトの設定	9.14(1)	ASDM、WebVPN、および他のクライアントを含む、ASA へのすべての HTTPS 接続のアイドルタイムアウトを設定できるようになりました。これまでは、**http server idle-timeout** コマンドを使用して ASDM アイドルタイムアウトを設定することしかできませんでした。両方のタイムアウトを設定した場合は、新しいコマンドによる設定が優先されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** > **[HTTP Settings]** > **[Connection Idle Timeout]** チェックボックス。
事前定義されたリストに応じて最も高いセキュリティから最も低いセキュリティへという順序で SSH 暗号化の暗号を表示	9.13(1)	事前定義されたリストに応じて、SSH 暗号化の暗号が最も高いセキュリティから最も低いセキュリティへという順序（中または高）で表示されるようになりました。以前のリリースでは、最も低いものから最も高いものへの順序でリストされており、セキュリティが高い暗号よりも低い暗号が先に表示されていました。 新しい/変更された画面： **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
SSH キー交換モードの設定は、管理コンテキストに限定されています。	9.12(2)	管理コンテキストでは SSH キー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** > **[SSH Settings]** > **[DH Key Exchange]**

機能名	プラットフォームリリース	説明
enable ログイン時のパスワードの変更が必須に	9.12(1)	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 文字以上の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブル パスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 変更された画面はありません。
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[Management Session Quota]**
管理権限レベルの変更通知	9.12(1)	有効なアクセス（**aaa authentication enable console**）を認証するか、または特権 EXEC への直接アクセス（**aaa authorization exec auto-enable**）を許可すると、前回のログイン以降に割り当てられたアクセス レベルが変更された場合に ASA からユーザーへ通知されるようになりました。 新しい/変更された画面： [Status] バー > [Login History] アイコン

機能名	プラットフォームリリース	説明
SSH によるセキュリティの強化	9.12(1)	次の SSH セキュリティの改善を参照してください。 • Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルトになりました。以前のデフォルトは Group 1 SHA1 でした。 • HMAC-SHA256 整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（hmac-sha2-256 のみ）になりました。以前のデフォルトは中程度のセットでした。 新規/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** • **[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	9.12(1)	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。 新規/変更された画面： **[Configuration]** > **[Device Management]** > **[Management Access]** > **[HTTP Non-Browser Client Support]**
RSA キーペアは 3072 ビット キーをサポートしています	9.9(2)	モジュラス サイズを 3072 に設定できるようになりました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]**
ブリッジ型仮想インターフェイス（BVI）の VPN 管理アクセス	9.9(2)	VPN の **management-access** がその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で有効にできるようになりました。非 VPN 管理アクセスの場合は、ブリッジ グループ メンバ インターフェイスでこれらのサービスの設定を続行する必要があります。 新規または変更されたコマンド：**https**、**telnet**、**ssh**、**management-access**
SSH バージョン 1 の廃止	9.9(1)	SSH バージョン 1 は廃止され、今後のリリースで削除される予定です。デフォルト設定が SSH v1 と v2 の両方から SSH v2 のみに変更されました。 新しい/変更された画面： • **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能名	プラットフォームリリース	説明
SSH公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザー データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザーに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更された画面はありません。
ログイン履歴	9.8(1)	デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。1 つ以上の管理メソッド（SSH、ASDM、Telnet など）でローカル AAA 認証を有効にしている場合、この機能はローカル データベースのユーザー名にのみ適用されます。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Login History]**
パスワードの再利用とユーザー名と一致するパスワードの使用を禁止するパスワード ポリシーの適用	9.8(1)	最大 7 世代にわたるパスワードの再利用と、ユーザー名と一致するパスワードの使用を禁止できるようになりました。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[Password Policy]**
ASDM に対する ASA SSL サーバー モード マッチング	9.6(2)	証明書マップと照合するために、証明書で認証を行う ASDM ユーザーに対して証明書を要求できるようになりました。 次の画面を変更しました。**[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]**

機能名	プラットフォームリリース	説明
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカル ユーザー データベース（）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザーが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザー名を作成できるようになりました。 次の画面が変更されました。 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[ASDM/HTTPS/Telnet/SSH]** **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** > **[Add/Edit User Account]**
ASDM 管理認証	9.4(1)	HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。 次の画面が変更されました。**[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]**
証明書コンフィギュレーションの ASDM ユーザー名	9.4(1)	ASDM の証明書認証を有効にすると、ASDM が証明書からユーザー名を抽出する方法を設定できます。また、ログイン プロンプトでユーザー名を事前に入力して表示できます。 次の画面が導入されました。**[Configuration] > [Device Management] > [Management Access] > [HTTP Certificate Rule]**
改善されたワンタイムパスワード認証	9.2(1)	十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特権 EXEC モードに移行できます。**auto-enable** オプションが **aaa authorization exec** コマンドに追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]。
HTTP リダイレクトの IPv6 サポート	9.1(7)/9.6(1)	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6 アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次の画面に機能が追加されました。**[Configuration]** > **[Device Management]** > **[HTTP Redirect]**

機能名	プラットフォームリリース	説明
設定可能なSSH暗号機能と整合性アルゴリズム	9.1(7.4)、9.3(3)、9.6(1)	ユーザーはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対してHMACと暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASAは3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctrの順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbcなどの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc**を使用します。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**
SSHのAES-CTR暗号化	9.1(2)	ASAでのSSHサーバーの実装が、AES-CTRモードの暗号化をサポートするようになりました。
SSHキー再生成間隔の改善	9.1(2)	SSH接続は、接続時間60分間またはデータ トラフィック1 GBごとに再生成されます。 。
マルチコンテキストモードのASASMにおいて、スイッチからのTelnet認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチ コンテキスト モードのスイッチからASASMへの接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	8.4(4.1)、9.1(2)	ローカル データベースを使用してCLIまたはASDMアクセスの認証を設定する場合は、指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA] > [Password Policy]。

機能名	プラットフォームリリース	説明
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザー単位で有効にできます。公開キーファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication][Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。 *PKF* キー形式のサポートは *9.1(2)* 以降のみです。
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]。
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	同時 ASDM、SSH、Telnet セッションの最大数を設定できます。 次の画面が導入されました。[Configuration] > [Device Management] > [Management Access] > [Management Session Quota]。
SSH セキュリティが向上し、SSH デフォルトユーザー名はサポートされなくなりました。	8.4(2)	8.4(2) 以降、pix または asa ユーザー名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカルユーザーを定義する必要があります。定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

機能名	プラットフォームリリース	説明
管理アクセス	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH][Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner][Configuration] > [Device Management] > [Management Access] > [CLI PromptConfiguration] > [Device Management] > [Management Access] > [ICMP][Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client][Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server][Configuration] > [Device Management] > [Management Access] > [File Access] > [Mount-Points][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization][Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Accounting]。

第 43 章

ソフトウェアおよびコンフィギュレーション

この章では、Cisco ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

ソフトウェアのアップグレード

完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON を使用したイメージのロード（ASA 5506-X、5508-X、5516-X、および ISA 3000）

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 ASA ハードウェアまたは ISA 3000 コンソールへのアクセス （17 ページ）に従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

（注） ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、および ASA 5516-X プラットフォームで無視されるため、これらのプラットフォームで Management 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

ステップ 5 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6 TFTP サーバーに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
Updating NVRAM Parameters...
```

ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。ソフトウェアのアップグレード （1187 ページ） を参照してください。

ROMMON イメージのアップグレード（ASA 5506-X、5508-X、5516-X、および ISA 3000）

ASA 5506-X シリーズ、ASA 5508-X、ASA 5516-X、および ISA 3000 の ROMMON イメージをアップグレードするには、次の手順に従います。 ASA モデルの場合、システムの ROMMON バージョンは 1.1.8 以上である必要があります。最新バージョンへのアップグレードを推奨します。

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。

注意 ASA 5506-X、5508-X、5516-X の ROMMON 1.1.15 へのアップグレード、および ISA 3000 の ROMMON 1.0.5 へのアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカル サポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

始める前に

Cisco.com から新しい ROMMON イメージを取得して、サーバー上に置いて ASA にコピーします。ASA は、FTP サーバー、TFTP サーバー、SCP サーバー、HTTP（S）サーバー、および SMB サーバーをサポートしています。次の URL からイメージをダウンロードします。

- ASA 5506-X、5508-X、5516-X： https://software.cisco.com/download/home/286283326/type
- ISA 3000： https://software.cisco.com/download/home/286288493/type

手順

ステップ 1 ROMMON イメージを ASA フラッシュ メモリにコピーします。この手順では、FTP コピーを表示します。他のサーバータイプのシンタックスの場合は **copy ?** と入力します。

copy ftp://[*username*:*password*@]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

ステップ 2 現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

ステップ 3 ROMMON イメージをアップグレードします。

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
```

```
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASA が ROMMON イメージをアップグレードして、その後オペレーティングシステムをリロードします。

ASA 5506W-X ワイヤレス アクセス ポイントのイメージの回復およびロード

TFTP を使用してソフトウェア イメージを回復して ASA 5506W-X にロードするには、次の手順を実行します。

手順

ステップ 1 アクセス ポイント（AP）へのセッションを確立し、AP ROMMON（ASA ROMMON ではなく）を開始します。

```
ciscoasa# hw-module module wlan recover image
```

ステップ 2 Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド [英語] の手順に従います。

ソフトウェアのダウングレード

多くの場合、ASA ソフトウェアをダウングレードし、以前のソフトウェアバージョンからバックアップ設定を復元することができます。ダウングレードの方法は、ASA プラットフォームによって異なります。

ダウングレードに関するガイドラインおよび制限事項

ダウングレードする前に、次のガイドラインを参照してください。

- クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません。ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレー

ドに関する次の既知の問題を参照してください。この他の問題が原因でクラスタユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。

- クラスタリングを含む9.9(1)より前のリリースへのダウングレード：9.9(1)以降では、バックアップの配布が改善されています。クラスタに3つ以上のユニットがある場合は、次の手順を実行する必要があります。

  1. クラスタからすべてのセカンダリユニットを削除します（クラスタはプライマリユニットのみで構成されます）。
  2. 1つのセカンダリ ユニットをダウングレードし、クラスタに再参加させます。
  3. プライマリユニットでクラスタリングを無効にします。そのユニットをダウングレードし、クラスタに再参加させます。
  4. 残りのセカンダリユニットをダウングレードし、それらを一度に1つずつクラスタに再参加させます。

- クラスタ サイトの冗長性を有効にする場合は、9.9(1) より前のリリースにダウングレードします。ダウングレードする場合（または9.9(1) より前のユニットをクラスタに追加する場合）は、サイトの冗長性を無効にする必要があります。そうしないと、古いバージョンを実行しているユニットにダミーの転送フローなどの副作用が発生します。
- クラスタリングおよび暗号マップを使用する場合に9.8(1)からダウングレードする：暗号マップが設定されている場合に 9.8 (1) からダウングレードすると、ゼロ ダウンタイム ダウングレードはサポートされません。ダウングレード前に暗号マップ設定をクリアし、ダウングレード後に設定をもう一度適用する必要があります。
- クラスタリング ユニットのヘルスチェックを 0.3 ～ 0.7 秒に設定した状態で 9.8(1) からダウングレードする：（**health-check holdtime**で）ホールド時間を 0.3 ～ 0.7 秒に設定した後で ASA ソフトウェアをダウングレードすると、新しい設定はサポートされないため、設定値はデフォルトの 3 秒に戻ります。
- クラスタリング（CSCuv82933）を使用している場合に9.5(2)以降から9.5(1)以前にダウングレードする：9.5(2)からダウングレードする場合、ゼロ ダウンタイム ダウングレードはサポートされません。ユニットがオンラインに戻ったときに新しいクラスタが形成されるように、すべてのユニットをほぼ同時にリロードする必要があります。ユニットが順番にリロードされるのを待つと、クラスタを形成できなくなります。
- クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする：ゼロ ダウンタイム ダウングレードはサポートされません。

- プラットフォームモードでの 9.13/9.14 から 9.12 以前への Firepower 2100 のダウングレードの問題：プラットフォームモードに変換した 9.13 または 9.14 を新規インストールした Firepower 2100 の場合：9.12 以前にダウングレードすると、FXOS で新しいインターフェイスの設定や、既存のインターフェイスの編集ができなくなります（9.12以前ではプラットフォームモードのみがサポートされていたことに注意してください）。バージョンを9.13以降に戻すか、またはFXOSの erase configuration コマンドを使用して設定をクリアす

る必要があります。この問題は、元々以前のリリースから9.13または9.14にアップグレードした場合は発生しません。新しいデバイスや再イメージ化されたデバイスなど、新規インストールのみが影響を受けます。（CSCvr19755）

- スマート ライセンスの 9.10(1) からのダウングレード：スマート エージェントの変更により、ダウングレードする場合、デバイスを Cisco Smart Software Manager に再登録する必要があります。新しいスマートエージェントは暗号化されたファイルを使用するので、古いスマートエージェントが必要とする暗号化されていないファイルを使用するために再登録する必要があります。
- PBKDF2（パスワード ベースのキー派生関数 2）ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。9.7(1) では、すべての新しいパスワードは、長さに関わらず PBKDF2 ハッシュを使用します（既存のパスワードは引き続き MD5 ハッシュを使用します）。ダウングレードすると、**enable** パスワードがデフォルト（空白）に戻ります。ユーザー名は正しく解析されず、**username** コマンドが削除されます。ローカル ユーザーをもう一度作成する必要があります。
- ASAv 用のバージョン 9.5(2.200) からのダウングレード：ASAv はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。
- 元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェア バージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます。このシナリオは、ダウングレード時に発生します。その場合、VPN 接続を切断して再接続してください。

ダウングレード後に削除される互換性のない設定

以前のバージョンにダウングレードすると、それ以降のバージョンで導入されたコマンドは設定から削除されます。ダウングレードする前に、ターゲットバージョンに対して設定を自動的にチェックする方法はありません。新しいコマンドが ASA の新しい機能にいつ追加されたかをリリースごとに表示できます。

show startup-config errors コマンドを使用してダウングレードした後、拒否されたコマンドを表示できます。ラボデバイスでダウングレードを実行できる場合は、実稼働デバイスでダウングレードを実行する前にこのコマンドを使用して効果を事前に確認できます。

場合によっては、ASA はアップグレード時にコマンドを新しいフォームに自動的に移行するため、バージョンによっては新しいコマンドを手動で設定しなかった場合でも、設定の移行によってダウングレードが影響を受けることがあります。ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。ダウングレードに影響する可能性がある自動コマンド移行の詳細については、

『ASAアップグレードガイド』の「バージョン固有のガイドラインと移行」を参照してください。

ダウングレードに関するガイドラインおよび制限事項（1191 ページ）の既知のダウングレードの問題も参照してください。

たとえば、バージョン9.8(2) を実行している ASA には、次のコマンドが含まれています。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
```

9.0(4) にダウングレードすると、起動時に次のエラーが表示されます。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0

                                   ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                 ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
                                             ^
ERROR: % Invalid input detected at '^' marker.
```

この例では、**access-list extended** コマンドでの **sctp** のサポートがバージョン 9.5(2) で、**username** コマンドでの **pbkdf2** のサポートがバージョン 9.6(1) で、**snmp-server user** コマンドでの **engineID** のサポートがバージョン9.5(3) で追加されました。

アプライアンスモードでの Firepower 1000 または Firepower 2100 のダウングレード

ASA のバージョンを古いバージョンに設定し、バックアップ設定をスタートアップ コンフィギュレーションに復元してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 スタンドアロン、フェールオーバー、またはクラスタリング展開のために、『ASA Upgrade Guide』のアップグレード手順を使用して、ASA ソフトウェアの古いバージョンをロードしま

す。この場合は、ASAの新しいバージョンではなく、古いバージョンを指定します。**重要**：まだ ASAをリロードしないでください。

ステップ 2 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

ステップ 3 ASA をリロードします。

ASA CLI

reload

ASDM

[Tools] > **[System Reload]** を選択します。

プラットフォームモードでの Firepower 2100 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、またはクラスタリング展開のために、Firepower Chassis Manage または FXOS CLI を使用して、『ASA Upgrade Guide』のアップグレード手順に従い、ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

Firepower 4100/9300 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。
- ASA の古いバージョンが、FXOS の現在のバージョンと互換性があることを確認します。互換性がない場合は、古い ASA 設定を復元する前に最初の手順として FXOS をダウングレードします。ダウングレードされた FXOS も、（ダウングレードする前に）ASA の現在のバージョンと互換性があることを確認してください。互換性を実現できない場合は、ダウングレードを実行しないことをお勧めします。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーまたはクラスタリングの場合は、アクティブ/制御ユニットでこの手順を実行します。この手順では、コマンドをスタンバイ/データユニットに複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、またはクラスタリング展開のために、Firepower Chassis Manage または FXOS CLI を使用して、『ASA Upgrade Guide』のアップグレー

ド手順に従い、ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

ステップ 3 また、FXOS をダウングレードする場合は、スタンドアロン、フェールオーバー、またはクラスタリング展開のために、Firepower Chassis Manager または FXOS CLI を使用して、『ASA Upgrade Guide』 のアップグレード手順に従い、ASA ソフトウェアの古いバージョンを使います。

ASA 5500-X または ISA 3000 のダウングレード

ダウングレードでは、ASA 5500-X および ISA 3000 モデルで以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。
- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- 古いコンフィギュレーションのバックアップをスタートアップ コンフィギュレーションにコピーします（**copy** *old_config_ur* **startup-config**）。
- リロード（**reload**）。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。
- ASA FirePOWER モジュールのバージョンがインストールされている場合は、ASA の古いバージョンと互換性があることを確認します。FirePOWER モジュールを以前のメジャー バージョンにダウングレードすることはできません。

手順

ステップ 1 **[Tools]** > **[Downgrade Software]** を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

ステップ 2 ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 3 次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ 4 [Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します。

ステップ 5 （任意） バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

ステップ 6 [Downgrade] をクリックします。

ファイルの管理

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注） マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイル アクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバーとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバーとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバーは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client] ペインで、[Specify FTP mode as passive] チェックボックスをオンにします。

ステップ 2 [Apply] をクリックします。

FTP クライアントのコンフィギュレーションが変更され、その変更内容が実行コンフィギュレーションに保存されます。

セキュア コピー サーバーとしての ASA の設定

ASA 上でセキュア コピー（SCP）サーバーをイネーブルにできます。SSH による ASA へのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

始める前に

- サーバーにはディレクトリ サポートがありません。ディレクトリ サポートがないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- サーバーでは、バナーまたはワイルドカードがサポートされていません。
- ASDM、その他のクライアントの HTTPS アクセスの設定（1140 ページ）に従って、ASA で SSH を有効にします。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。
- 特に指定されていないかぎり、マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。
- セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、**[Configuration] > [Device Management] > [Advanced] > [SSH Ciphers]** ペインを使用します。たとえば、**[Custom]** を選択して aes128-cbc に設定します。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP)] の順に選択します。
- マルチ モードの場合、[Configuration] > [Device Management] > [Device Administration] > [Secure Copy] の順に選択します。

ステップ 2 [Enable secure copy server] チェック ボックスをオンにします。

ステップ 3 （オプション）ASA は接続先の各 SCP サーバーの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

キーを追加するには、次の手順を実行します。

a) 新しいサーバーの [Add] をクリックするか、または信頼できる SSH ホストのテーブルからサーバーを選択し、[Edit] をクリックします。
b) 新しいサーバーの [Host] フィールドに、サーバーの IP アドレスを入力します。
c) [Add public key for the trusted SSH host] チェックボックスをオンにします。
d) 次のいずれかのキーを指定します。

- フィンガープリント：すでにハッシュされているキーを入力します。たとえば、**show** コマンドの出力からコピーしたキーです。
- キー：SSH ホストの公開キーまたはハッシュ値を入力します。キー ストリングはリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

キーを削除するには、信頼できる SSH ホストのテーブルからサーバーを選択し、[Delete] をクリックします。

ステップ 4 （オプション）新しいホストキーが検出されたときに通知を受け取るには、[Inform me when a new host key is detected] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

ステップ 5 [適用（Apply）] をクリックします。

例

外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

scp -v -pw *password* [*path*/]*source_filename*
username@asa_address:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバー ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバーとの間でファイルをコピーできるように、ASA を

TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバーへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[TFTP Client]** の順に選択し、[Enable] チェックボックスをオンにします。

ステップ 2 [Interface Name] ドロップダウン リストから、TFTP クライアントとして使用するインターフェイスを選択します。

ステップ 3 コンフィギュレーション ファイルの保存先とする TFTP サーバーの IP アドレスを [IP Address] フィールドに入力します。

ステップ 4 コンフィギュレーション ファイルの保存先とする TFTP サーバーへのパスを [Path] フィールドに入力します。

例：/tftpboot/asa/config3

ステップ 5 **Apply** をクリックします。

マウント ポイントの追加

CIFS マウント ポイントまたは FTP マウント ポイントを追加できます。

CIFS マウント ポイントの追加

共通インターネット ファイル システム（CIFS）マウント ポイントを定義するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[Mount-Points]** の順に選択し、**[Add]** > **[CIFS Mount Point]** の順にクリックします。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

ステップ 2 [Enable mount point] チェックボックスをオンにします。

これにより、ASA 上の CIFS ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3 [Mount Point Name] フィールドに、既存の CIFS が存在する位置の名前を入力します。

ステップ 4 [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバーの名前または IP アドレスを入力します。

ステップ 5 [Share Name] フィールドに、CIFS サーバー上のフォルダの名前を入力します。

ステップ 6 [NT Domain Name] フィールドに、サーバーが常駐する NT ドメインの名前を入力します。

ステップ 7 サーバーに対するファイル システムのマウントを認可されているユーザーの名前を、[User Name] フィールドに入力します。

ステップ 8 サーバーに対するファイル システムのマウントを認可されているユーザーのパスワードを、[Password] フィールドに入力します。

ステップ 9 [Confirm Password] フィールドにパスワードを再入力します。

ステップ 10 [OK] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

FTP マウント ポイントの追加

FTP マウント ポイントの場合、FTP サーバーには UNIX のディレクトリ リスト スタイルが必要です。Microsoft FTP サーバーには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[Mount-Points]** の順に選択し、**[Add]** > **[FTP Mount Point]** の順にクリックします。

[Add FTP Mount Point] ダイアログボックスが表示されます。

ステップ 2 [Enable] チェックボックスを選択します。

これにより、ASA 上の FTP ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3 [Mount Point Name] フィールドに、既存の FTP が存在する位置の名前を入力します。

ステップ 4 [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバーの名前または IP アドレスを入力します。

ステップ 5 [Mode] フィールドで、オプション ボタン（[Active] または [Passive]）をクリックして FTP モードを選択します。[Passive] モードを選択した場合、クライアントでは、FTP コントロール接続とデータ接続がともに起動します。サーバーは、この接続をリッスンするポートの番号で応答します。

ステップ 6 FTP ファイル サーバへのディレクトリ パス名を [Path to Mount] フィールドに入力します。

ステップ 7 サーバーに対するファイル システムのマウントを認可されているユーザーの名前を、[User Name] フィールドに入力します。

ステップ 8 サーバーに対するファイル システムのマウントを認可されているユーザーのパスワードを、[Password] フィールドに入力します。

ステップ 9 [Confirm Password] フィールドにパスワードを再入力します。

ステップ 10 [OK] をクリックします。

[Add FTP Mount Point] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

ファイル管理ツールへのアクセス

ファイル管理ツールを使用するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。
- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名
  - サイズ（バイト単位）
  - 修正時刻
  - 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2 選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3 選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4 選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5 コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6 選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7 ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8 ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9 [File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「ファイルの転送 （1204 ページ）」を参照してください。

ステップ 10 [Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、マウント ポイントの追加 （1201 ページ）を参照してください。

ファイルの転送

File Transfer ツールにより、ローカルにあるファイルとリモートにあるファイルを転送できます。PC またはフラッシュ ファイル システムのローカル ファイルを ASA との間で転送できます。HTTP、HTTPS、TFTP、FTP、または SMB を使用して、ASA との間でファイルを転送できます。

（注） IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

ローカル PC とフラッシュ間でのファイル転送

ローカル PC とフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2 [File Transfer] の横にある下矢印をクリックし、続いて [Between Local PC and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3 ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、目的の場所にドラッグします。または、ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、右矢印または左矢印をクリックし、目的の場所にファイルを転送します。

ステップ 4 完了したら [Close] をクリックします。

リモート サーバーとフラッシュ間でのファイル転送

リモート サーバーとフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、**[Tools]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2 [File Transfer] ドロップダウン リストで下矢印をクリックし、[Between Remote Server and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3 リモート サーバーからファイルを転送するには、[Remote server] オプションをクリックします。

ステップ 4 転送対象になるソース ファイルを定義します。

a) （オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

b) サーバーの IP アドレスを含めたファイルの場所へのパスを選択します。

（注） ファイル転送は IPv4 および IPv6 のアドレスをサポートしています。

c) FTP の場合はリモート サーバーのタイプを、HTTP または HTTPS の場合はリモート サーバーのポート番号を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 5 フラッシュ ファイル システムからファイルを転送するには、[Flash file system] オプションを選択します。

ステップ 6 ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 7 また、CLI により、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**Copy** コマンドの使用方法については、CLI コンフィギュレーション ガイドを参照してください。

ステップ 8 転送するファイルの宛先を定義します。

a) フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。

b) ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9 リモート サーバーにファイルを転送するには、[Remote server] オプションを選択します。

a) （オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

b) ファイルの場所へのパスを入力します。

c) FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10 [Transfer] をクリックしてファイル転送を開始します。

[Enter Username and Password] ダイアログボックスが表示されます。

ステップ 11 リモート サーバーのユーザー名、パスワード、ドメイン（必要な場合）が表示されます。

ステップ 12 [OK] をクリックし、ファイル転送を続行します。

ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

ステップ 13 ファイル転送が完了したら [Close] をクリックします。

ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできないため、ASA イメージに対してこの手順を使用しないでください。ASA と FXOS を個別にアップグレードできます。この 2 つは FXOS ディレクトリ リストに別々に表示されます。ASA パッケージには必ず ASDM が含まれています。
- プラットフォーム モードの Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新は FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできな

いため、ASA イメージに対してこの手順を使用しないでください。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。

- アプライアンス モードの Firepower 1000 および 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新は、次の手順を使用して ASA によって管理されます。これらのプラットフォームでは、ブートするイメージを識別するために ASA が使用されますが、基盤となるメカニズムはレガシー ASA とは異なります。詳細については、以下のコマンドの説明を参照してください。
- Firepower モデルの ASDM：ASDM は ASA オペレーティング システム内からアップグレードできるため、バンドルされた ASDM イメージのみを使用する必要はありません。プラットフォームモードの Firepower 2100 ではFirepower 4100/9300、手動でアップロードする ASDM イメージは FXOS イメージリストに表示されません。ASA から ASDM イメージを管理する必要があります。

  注 ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドル イメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドル アップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

- ASAv：初期導入時の ASAv パッケージは、読み取り専用 boot:/ パーティション内に ASA イメージを配置します。ASAv をアップグレードする際は、フラッシュ メモリ内の別のイメージを指定します。後でコンフィギュレーションをクリアすると、ASAv は元の展開のイメージをロードするようになる点に注意してください。また、初期導入時の ASAv パッケージには、フラッシュ メモリ内に配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

次のデフォルト設定を参照してください。

- ASA イメージ：
  - Firepower 1000 およびアプライアンス モードの Firepower 2100：以前実行していたブート イメージをブートします。
  - その他の物理 ASA：内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
  - ASAv：最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。

- Firepower 4100/9300 シャーシ：どの ASA イメージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
- プラットフォーム モードの Firepower 2100：どの ASA/FXOS パッケージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。

- すべての ASA 上の ASDM イメージ：内部フラッシュ メモリ内で見つかった（この場所にイメージがない場合は外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。
- スタートアップ コンフィギュレーション：デフォルトで、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順

ステップ 1 **[設定（Configuration）] > [デバイス管理（Device Management）] > [システム イメージ/設定（System Image/Configuration）] > [ブート イメージ/設定（Boot Image/Configuration）]** を選択します。

アプライアンス モードの Firepower 1000、2100：1 つのイメージのみが追加できます。新しいイメージにアップグレードする場合は、以前に設定したイメージを削除する必要があります。この変更を適用すると、システムによってアクションが実行されます。システムはイメージを検証して解凍し、ブート場所 (FXOS によって管理される disk0 の内部ロケーション) にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードする前に注意してください。**ブートイメージの場所**を削除して再適用すると、ブートロケーションから新しいイメージを削除できます。そのため、現在のイメージは引き続き実行されます。この変更を適用した後、ASA のフラッシュメモリから元のイメージファイルを削除することもできます。また、ASA はブート場所から正しく起動します。他のモデルとは異なり、スタートアップコンフィギュレーション内のこのコマンドは、ブートイメージには影響しません。リロード時には、最後にロードされたブートイメージが常に実行されます。Cisco ダウンロードサイトからロードできるのは、元のファイル名のイメージのみです。ファイル名を変更した場合はロードされません。

他のモデル：起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバーのイメージを 1 つ指定して、そこからデバイスをブートできます。TFTP サーバーに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。デバイスが、イメージのロード元の TFTP サーバに到達できない場合は、フラッシュ メモリに保存されているリスト内の次のイメージ ファイルのロードが試行されます。

ステップ 2 [ブート イメージ/設定（Boot Image/Configuration）] ペインで [追加（Add）] をクリックします。

ステップ 3 ブートするイメージを参照します。TFTP イメージの場合は、[ファイル名（File Name）] フィールドに TFTP URL を入力します。[OK] をクリックします。

ステップ 4 [上へ移動（Move Up）] ボタンと [下へ移動（Move Down）] ボタンを使用してイメージの順番を並べ替えます。

ステップ 5 （オプション）[ブート設定ファイル パス（Boot Configuration File Path）] フィールドで、[フラッシュを参照（Browse Flash）]をクリックしてコンフィギュレーションを選択してスタートアップ コンフィギュレーション ファイルを指定します。[OK] をクリックします。

ステップ 6 [ASDM イメージ ファイル パス（ASDM Image File Path）] フィールドで、[フラッシュを参照（Browse Flash）] をクリックしてイメージを選択して ASDM イメージを指定します。[OK] をクリックします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションまたはその他のファイルのバックアップと復元

システム障害に備えて、コンフィギュレーション ファイルなどのシステム ファイルを定期的にバックアップすることを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zipバックアップ zip ファイルへのバックアップおよび復元方法と、そのファイルのローカル コンピュータへの転送方法について説明します。

バックアップまた復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- ASA は、シングル コンテキスト モードである必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。

- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、マスター パスフレーズの設定（756ページ）を参照して、バックアップを続行する前に、マスターパスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect（SVC）クライアントのイメージおよびプロファイル

    AnyConnect（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）
  - ブックマーク
  - カスタマイゼーション

- ダイナミック アクセス ポリシー（DAP）
- プラグイン
- 接続プロファイル用の事前入力スクリプト
- プロキシ自動設定
- 変換テーブル
- Web コンテンツ
- バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1 コンピュータ上にフォルダを作成し、バックアップ ファイルを保存します。こうすると、後で復元するときに探しやすくなります。

ステップ 2 **[Tools]** > **[Backup Configurations]** を選択します。

[Backup Configurations] ダイアログボックスが表示されます。[SSL VPN Configuration] 領域の下矢印をクリックし、SSL VPN コンフィギュレーションのバックアップ オプションを確認します。デフォルトでは、すべてのコンフィギュレーション ファイルがチェックされ、利用できる場合にはバックアップされます。リスト内のすべてのファイルをバックアップするには、手順 5 に進みます。

ステップ 3 バックアップするコンフィギュレーションを選択する場合は、[Backup All] チェックボックスをオフにします。

ステップ 4 バックアップするオプションの横にあるチェックボックスをオンにします。

ステップ 5 [Browse Local to specify a directory and file name for the backup .zip file] をクリックします。

ステップ 6 [Select] ダイアログボックスで、バックアップ ファイルを格納するディレクトリを選択します。

ステップ 7 [Select] をクリックします。[Backup File] フィールドにパスが表示されます。

ステップ 8 ディレクトリ パスの後にバックアップ ファイルの宛先の名前を入力します。バックアップ ファイルの名前の長さは、3 ～ 232 文字の間である必要があります。

ステップ 9 [Backup] をクリックします。証明書をバックアップする場合や、ASA でマスター パスフレーズを使用している場合を除き、すぐにバックアップが続行されます。

ステップ 10 ASA でマスター パスフレーズを設定し、イネーブルにしている場合、バックアップを続行する前に、マスターパスフレーズが不明な場合は変更することを推奨する警告メッセージが表示されます。マスター パスフレーズがわかっている場合は、[Yes] をクリックしてバックアップを続行します。ID 証明書をバックアップする場合を除き、すぐにバックアップが続行されます。

ステップ 11 ID 証明書をバックアップする場合は、証明書を PKCS12 形式でエンコーディングするために使用する別のパスフレーズを入力するように求められます。パスフレーズを入力するか、またはこの手順をスキップすることができます。

（注） ID 証明書だけがこのプロセスによってバックアップされます。

- 証明書を暗号化するには、[Certificate Passphrase] ダイアログボックスで証明書のパスフレーズを入力および確認し、[OK] をクリックします。証明書の復元時に必要となるため、このダイアログボックスに入力したパスワードを覚えておく必要があります。
- [Cancel] をクリックすると、この手順がスキップされ、証明書はバックアップされません。

[OK] または [Cancel] をクリックすると、すぐにバックアップが開始されます。

ステップ 12 バックアップが完了すると、ステータス ウィンドウが閉じ、[Backup Statistics] ダイアログボックスが表示され、成功または失敗のメッセージが示されます。

（注） バックアップの「失敗」メッセージは多くの場合、指定されたタイプの既存のコンフィギュレーションが存在しない場合に表示されます。

ステップ 13 [OK] をクリックし、[Backup Statistics] ダイアログボックスを閉じます。

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 **[Tools]** > **[Restore Configurations]** を選択します。

ステップ 2 [Restore Configurations] ダイアログボックスで、[Browse Local Directory] をクリックし、ローカル コンピュータ上の、復元するコンフィギュレーションが含まれている zip ファイルを選択し、[Select] をクリックします。[Local File] フィールドにパスと zip ファイル名が表示されます。

復元する zip ファイルは、[Tools] > [Backup Configurations] オプションを選択して作成したものである必要があります。

ステップ 3 [Next] をクリックします。2 つ目の [Restore Configuration] ダイアログボックスが表示されます。復元するコンフィギュレーションの横にあるチェックボックスをオンにします。使用可能なすべての SSL VPN コンフィギュレーションがデフォルトで選択されています。

ステップ 4 [Restore] をクリックします。

ステップ 5 バックアップ ファイルの作成時に、証明書の暗号化に使用する証明書パスフレーズを指定している場合は、このパスフレーズを入力するように ASDM から求められます。

ステップ 6 実行コンフィギュレーションの復元を選択した場合、実行コンフィギュレーションを結合するか、実行コンフィギュレーションを置換するか、または復元プロセスのこの部分をスキップするかを尋ねられます。

- コンフィギュレーションの結合では、現在の実行コンフィギュレーションとバックアップされた実行コンフィギュレーションが結合されます。
- 実行コンフィギュレーションの置換では、バックアップされた実行コンフィギュレーションのみが使用されます。
- この手順をスキップすると、バックアップされた実行コンフィギュレーションは復元されません。

ASDM では、復元操作が完了するまでステータス ダイアログボックスが表示されます。

ステップ 7 実行コンフィギュレーションを置換または結合した場合は、ASDM を閉じてから再起動します。実行コンフィギュレーションを復元しなかった場合は、ASDMセッションをリフレッシュして、変更を有効にします。

自動バックアップおよび復元の設定（ISA 3000）

ISA 3000 では、設定を保存するたびに、特定の場所への自動バックアップを設定できます。

自動復元では、完全な設定を SD フラッシュメモリカードにロードして、新しいデバイスを簡単に設定できます。工場出荷時のデフォルト設定では、自動復元が有効になっています。

自動バックアップの設定（ISA 3000）

ISA 3000 では、設定を保存するたびに、特定の場所への自動バックアップを設定できます。

始める前に

この機能は、ISA 3000 のみで使用できます。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [自動バックアップと復元の設定（Auto Backup & Restore Configuration）]** の順に選択します。

ステップ 2 [自動バックアップ設定（Automatic Restore Configuration）] をオンまたはオフにして、自動バックアップを有効または無効にします。

自動バックアップを有効にした場合、設定を保存すると、その設定は自動的にバックアップの場所とスタートアップコンフィギュレーションに保存されます。バックアップファイルの名前は「auto-backup-asa.tgz」です。

次のパラメータを設定します。

- [インターフェイス（Interface）]：オフデバイスストレージを指定した場合に、バックアップ URL に到達するためのインターフェイスを指定します。interface name を指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。
- [場所（Location）]：データのバックアップに使用するストレージメディアを指定します。URL またはローカルストレージを指定できます。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。自動復元のデフォルトは disk3: です。
- [パスフレーズ（Passphrase）]：バックアップデータを保護するためのパスフレーズを設定します。自動復元のデフォルトは「cisco」です。

自動復元の設定（ISA 3000）

自動復元モードは、ユーザの操作なしでデバイスのシステム設定を復元します。たとえば、保存したバックアップ設定を含む SD メモリカードを新しいデバイスに挿入し、デバイスの電源をオンにします。デバイスが起動すると、システム設定を復元する必要があるかどうかを判断するために SD カードがチェックされます。（復元は、バックアップファイルに別のデバイスの「フィンガープリント」がある場合にのみ開始されます。バックアップファイルのフィンガープリントは、バックアップまたは復元操作中に現在のデバイスに一致するように更新されます。そのため、デバイスがすでに復元を完了している場合、またはデバイスが独自のバックアップを作成している場合は、自動復元はスキップされます。）フィンガープリントに復元が必要であることが示されている場合、デバイスはシステム設定を置き換えます（startup-config、running-config、SSL VPN 設定など。バックアップの内容の詳細については、システムのバックアップ（1211 ページ）を参照してください）。デバイスの起動が完了すると、保存された設定が実行されます。

工場出荷時のデフォルト設定では自動復元が有効になっているため、デバイスの事前設定を実行しなくても、SD メモリカードにロードされた完全な設定で新しいデバイスを簡単に設定できます。

デバイスは、システム設定を復元する必要があるかどうかをブートプロセスの早い段階で決定する必要があるため、ROMMON 変数をチェックして、デバイスが自動復元モードかどうかを判断し、バックアップ設定の場所を取得します。次の ROMMON 変数が使用されます。

- **RESTORE_MODE =** {**auto** | **manual**}

  デフォルトは **auto** です。

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  デフォルトは **disk3:** です。

- **RESTORE_PASSPHRASE =** *key*

  デフォルトは **cisco** です。

自動復元設定を変更するには、次の手順を実行します。

始める前に

- この機能は、ISA 3000 のみで使用できます。
- デフォルトの復元設定を使用する場合は、SD メモリカード（部品番号 SD-IE-1GB=）を取り付ける必要があります。
- 自動復元を有効にするためにデフォルト設定を復元する必要がある場合は、**configure factory default** コマンドを使用します。このコマンドは、トランスペアレント ファイアウォール モードでのみ使用できます。そのため、ルーテッド ファイアウォール モードの場合は、最初に **firewall transparent** コマンドを使用します。

手順

ステップ 1 **[構成（Configuration）] > [デバイス管理（Device Management）] > [自動バックアップと復元の設定（Auto Backup & Restore Configuration）]** の順に選択します。

ステップ 2 [自動復元設定（Automatic Restore Configuration）] をオンまたはオフにして、自動復元を有効または無効にします。

復元されるファイルの名前は「auto-backup-asa.tgz」です。自動復元を有効にする場合は、次のパラメータを設定します。

- [場所（Location）]：データの復元に使用するストレージメディアを指定します。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。デフォルトは disk3 です。
- [パスフレーズ（Passphrase）]：バックアップデータを読み取るパスフレーズを設定します。デフォルトは「cisco」です。

TFTP サーバーへの実行コンフィギュレーションの保存

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバーに保存します。

手順

ステップ 1 **[File] > [Save Running Configuration to TFTP Server]** を選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2 TFTP サーバーの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバー上のファイル パスを入力して、[Save Configuration] をクリックします。

（注） デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバーの IP アドレスと TFTP サーバー上でのファイル パスが自動的に表示されます。

システム再起動のスケジュール

System Reload ツールにより、システムの再起動をスケジュールしたり、現在の再起動をキャンセルしたりできます。

手順

ステップ 1 **[Tools]** > **[System Reload]** を選択します。

ステップ 2 [Reload Scheduling] 領域で、次の設定を定義します。

a) [Configuration State] では、再起動時に実行コンフィギュレーションを保存するか、破棄するかのどちらかを選択します。

b) [Reload Start Time] では、次のオプションから選択します。

- 再起動をただちに実行するには、[Now] をクリックします。
- 指定した時間だけ再起動を遅らせるには、[Delay by] をクリックします。再起動開始までの時間を、時間と分単位、または分単位だけで入力します。
- 指定した時刻と日付に再起動を実行するようにスケジュールするには、[Schedule at] をクリックします。再起動の実行時刻を入力し、再起動のスケジュール日を選択します。

c) [Reload Message] フィールドに、再起動時に開いている ASDM インスタンスに送信するメッセージを入力します。

d) 再起動を再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e) 設定に従って再起動をスケジュールするには、[Schedule Reload] をクリックします。

[Reload Status] 領域には、再起動のステータスが表示されます。

ステップ 3 次のいずれかを選択します。

- スケジュールされた再起動を停止するには、[Cancel Reload] をクリックします。
- スケジュールされた再起動の終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。

• スケジュールされた再起動の詳細を表示するには、[Details] をクリックします。

Auto Update の設定

Auto Update は、Auto Update サーバーがコンフィギュレーションおよびソフトウェア イメージを多数の ASA にダウンロードすることを許可し、中央からの ASA の基本的なモニターリングを提供するプロトコル仕様です。

Auto Update について

この項では、Auto Update の実装方法と Auto Update が必要になる理由について説明します。

Auto Update クライアントまたはサーバー

ASA は、クライアントまたはサーバーとして設定できます。Auto Update クライアントとして動作する場合は、ソフトウェア イメージおよびコンフィギュレーション ファイルへのアップデートのため、Auto Update サーバーを定期的にポーリングします。Auto Update サーバーとして動作する場合は、Auto Update クライアントとして設定された ASA のアップデートを発行します。

Auto Update の利点

Auto Update は、次のように、管理者が ASA の管理で直面するさまざまな問題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点の解決。
- コンフィギュレーションの変更を 1 つのアクションでコミット。
- ソフトウェア更新用の信頼度の高い方式の提供。
- ハイ アベイラビリティ用の十分実績のある方式の活用（フェールオーバー）。
- オープン インターフェイスによる柔軟性の提供。
- サービス プロバイダ環境のセキュリティ ソリューションの簡素化。

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションにより ASA のコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うと、Auto Update サーバーから ASA にコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりすることも、ASA から Auto Update サーバーに定期的にポーリングすることによって、最新のコンフィギュレーション情報を引き出す（プルする）こともできます。また、Auto Update サーバーはいつでも ASA にコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバーと ASA の通

信では、通信パスとローカル CLI コンフィギュレーションをすべての ASA に設定する必要があります。

フェールオーバー設定での Auto Update サーバー サポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、アクティブ/スタンバイ フェールオーバー コンフィギュレーションの ASA に配置できます。アクティブ/スタンバイ フェールオーバー コンフィギュレーションでAuto Updateをイネーブルにするには、フェールオーバー ペアのプライマリ装置に Auto Update サーバーのコンフィギュレーションを入力します。

フェールオーバー コンフィギュレーションの Auto Update サーバー サポートには、次の制限と動作が適用されます。

- アクティブ/スタンバイ コンフィギュレーションがサポートされるのは、シングル モードだけです。
- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。
- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェールオーバー リンクのコンフィギュレーションが変更されると、装置間の通信は失敗します。
- Auto Update サーバへの Call Home を実行するのはプライマリ装置だけです。Call Home を実行するには、プライマリ装置がアクティブ状態である必要があります。そうでない場合、ASA は自動的にプライマリ装置にフェールオーバーします。
- ソフトウェアイメージまたはコンフィギュレーションファイルをダウンロードするのは、プライマリ装置だけです。その後、ソフトウェアイメージまたはコンフィギュレーション ファイルはセカンダリ装置にコピーされます。
- インターフェイス MAC アドレスとハードウェアのシリアル番号は、プライマリ装置のものです。
- Auto Update サーバーまたは HTTP サーバーに保存されたコンフィギュレーション ファイルは、プライマリ装置専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。装置がコンフィギュレーションを同期化している場合、SSM カードの不具合以外の理由でスタンバイ装置に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の装置は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。

2. プライマリ装置は Auto Update サーバーにアクセスします。プライマリ装置がアクティブ状態でない場合、ASA はプライマリ装置にフェールオーバーした後、Auto Update サーバーにアクセスします。
3. Auto Update サーバーは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ装置が、アクティブまたはスタンバイ装置のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
    1. プライマリ装置は、Auto Update サーバーの URL を使用して、HTTP サーバーから適切なファイルを取得します。
    2. プライマリ装置は、そのイメージをスタンバイ装置にコピーしてから、自身のイメージをアップデートします。
    3. 両方の装置に新しいイメージがある場合は、セカンダリ（スタンバイ）装置が最初にリロードされます。
        - セカンダリ装置のブート時にヒットレス アップグレードが可能な場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。リロードが終了すると、プライマリ装置がアクティブ装置になります。
        - スタンバイ装置のブート時にヒットレス アップグレードができない場合は、両方の装置が同時にリロードされます。
    4. セカンダリ（スタンバイ）装置だけに新しいイメージがある場合は、セカンダリ装置だけがリロードされます。プライマリ装置は、セカンダリ装置のリロードが終了するまで待機します。
    5. プライマリ（アクティブ）装置だけに新しいイメージがある場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。
    6. もう一度アップデート プロセスが手順 1 から開始されます。
5. ASA が、プライマリまたはセカンダリ装置の ASDM ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
    1. プライマリ装置は、Auto Update サーバーから提供された URL を使用して、HTTP サーバーから ASDM イメージ ファイルを取得します。
    2. プライマリ装置は、必要に応じてそのイメージをスタンバイ装置にコピーします。
    3. プライマリ装置は、自身の ASDM イメージをアップデートします。
    4. もう一度アップデート プロセスが手順 1 から開始されます。
6. プライマリ装置が、コンフィギュレーション ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
    1. プライマリ装置は、指定された URL を使用して、からコンフィギュレーション ファイルを取得します。

2. 両方の装置で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
3. もう一度アップデート プロセスが手順 1 から開始されます。

7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update のガイドライン

コンテキスト モード

Auto Update は、シングル コンテキスト モードでのみサポートされます。

クラスタ

クラスタリングはサポートされません。

モデル

次のモデルではサポートされません。

- ASA 5506-X、5508-X、5516-X
- Firepower 1000、 2100、 4100、および 9300
- ASAv

その他のガイドライン

- Auto Update サーバーから ASA のコンフィギュレーションが更新されても、ASDM には通知されません。**[Refresh]** または **[File] > [RefreshASDM** with the Running Configuration on the Device] を選択して、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバーと通信するためのプロトコルとして HTTPS が選択されている場合は、ASA は SSL を使用します。これは、ASA による DES または 3DES ライセンスの保有が必須です。

Auto Update サーバーとの通信の設定

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[System Image/Configuration]** > **[Auto Update]** を選択します。

[Auto Update] ペインには、[Auto Update Servers] テーブルの他に [Timeout] 領域と [Polling] 領域があります。

[Auto Update Servers] テーブルで、Auto Update サーバーにすでに設定されているパラメータを確認できます。ASA は、テーブルの一番上にあるサーバーを最初にポーリングします。

ステップ 2 テーブル内のサーバーの順序を変更するには、[Move Up] または [Move Down] をクリックします。

[Auto Update Servers] テーブルには次のカラムがあります。

- [Server]：Auto Update サーバーの名前または IP アドレス。
- [User Name]：Auto Update サーバーのアクセス時に使用されるユーザー名。
- [Interface]：Auto Update サーバーへの要求送信時に使用されるインターフェイス。
- [Verify Certificate]：Auto Update サーバが返した証明書を、ASA で CA のルート証明書と照合して確認するかどうかを指定します。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

ステップ 3 [Auto Update Server] テーブルの行のいずれかをダブルクリックすると、[Edit Auto Update Server] ダイアログボックスが開き、Auto Update サーバーのパラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには[Apply] をクリックする必要があります。

ステップ 4 [Timeout] エリアでは、ASA が Auto Update サーバーのタイムアウトを待つ時間を設定できます。[Timeout] 領域には次のフィールドがあります。

- [Enable Timeout Period]：ASA が Auto Update サーバーから応答を受信しなかった場合にタイムアウトするには、オンにします。
- [Timeout Period (Minutes)]：Auto Update サーバーから応答がなかった場合の ASA のタイムアウト時間（分単位）を指定します。

ステップ 5 [Polling] エリアで、ASA から Auto Update サーバーの情報をポーリングする頻度を設定できます。[Polling] 領域には次のフィールドがあります。

- [Polling Period (minutes)]：ASA から Auto Update サーバーに新しい情報をポーリングするときの待ち時間（分単位）。
- [Poll on Specified Days]：ポーリングのスケジュールを指定します。

- [Set Polling Schedule]：[Set Polling Schedule] ダイアログボックスが表示され、Auto Update サーバーをポーリングする日付と時刻を設定できます。
- [Retry Period (minutes)]：サーバーのポーリングに失敗した場合、ASA から Auto Update サーバーに新しい情報をポーリングするまでの待ち時間（分単位）。
- [Retry Count]：ASA から Auto Update サーバーに新しい情報をポーリングするときの再試行回数。

ステップ 6 ポーリング スケジュールの設定

[Set Polling Schedule] ダイアログボックスでは、ASA から Auto Update サーバーをポーリングする特定の日付と時刻を設定できます。

[Set Polling Schedule] ダイアログボックスには次のフィールドがあります。

[Days of the Week]：ASA から Auto Update サーバーをポーリングする曜日のチェックボックスを選択します。

[Daily Update] ペイン グループでは、ASA が Auto Update サーバーをポーリングする時刻を設定できます。次のフィールドがあります。

- [Start Time]：Auto Update のポーリング開始時刻を入力します。
- [Enable randomization]：ASA から Auto Update サーバーをランダムに選択した時刻にポーリングするには、オンにします。

Auto Update のモニターリング

Auto Update プロセスのモニターリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。**debug**ターミナル セッションからコマンドを実行します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
```

```
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

file は、失敗したアップデートに応じて “image”、“asdm”、または “configuration” になります。*version* は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォームリリース	機能情報
セキュアコピークライアントおよびサーバ	9.1(5)/9.2(1)	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP）クライアントおよびサーバをサポートするようになりました。 次の画面が変更されました。 [Tools] > [File Management] > [File Transfer] > [Between Remote Server and Flash] [Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server]
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)9.4(3)9.5(3)9.6(1)	ユーザーは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**

機能名	プラットフォームリリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバー証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 設定を移行する場合は、次のように確認なしを明示的に設定します。 次の画面が変更されました。[Configuration] > [Device Management] > [System/Image Configuration] > [Auto Update] > [Add Auto Update Server]。
CLIを使用したシステムのバックアップと復元	9.3(2)	CLIを使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。 変更された ASDM 画面はありません。
新しいASA 5506W-Xイメージの回復およびロード	9.4(1)	新しい ASA 5506W-X イメージのリカバリおよびロードがサポートされています。 変更された ASDM 画面はありません。
ISA 3000 の自動バックアップと復元	9.7(1)	バックアップ コマンドと復元コマンドのプリセット パラメータを使用して、自動バックアップ機能や自動復元機能を有効にできます。これらの機能は、外部メディアからの初期設定、デバイス交換、作動可能状態へのロールバックなどで使用されます。 次の画面が導入されました。**[Configuration] > [Device Management] > [Auto Backup & Restore Configuration]**

第 44 章

システム イベントに対する応答の自動化

この章では、Embedded Event Manager（EEM）を設定する方法について説明します。

EEM について

EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。

サポートされるイベント

EEM は次のイベントをサポートします。

- Syslog：ASA は、syslog メッセージの ID を使用して、イベント マネージャ アプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベント マネージャ アプレット内で syslog メッセージの ID が重複することはできません。
- タイマー：タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベント マネージャ アプレットに対して一度だけ設定できます。各イベント マネージャ アプレットには最大で 3 つのタイマーがあります。3 種類のタイマーは次のとおりです。
  - ウォッチドッグ（定期的）タイマーは、アプレットアクションの完了後に指定された期間が経過するとイベント マネージャ アプレットをトリガーし、自動的にリスタートします。

- カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベントマネージャアプレットを1回トリガーします。削除および再追加されない限りはリスタートしません。
- 絶対（1 日 1 回）タイマーは、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は hh:mm:ss です。

  各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを 1 つだけ設定できます。

- なし：CLI または ASDM を使用してイベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。**output** コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

イベント マネージャ アプレットのアクション

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先

output コマンドを使用すると、アクションの出力を指定した場所に送信できます。一度にイネーブルにできる出力値は1つだけです。デフォルト値は **output none** です。この値は、**action** コマンドによるすべての出力を破棄します。このコマンドは、特権レベル 15（最高）を持つユーザーとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。次の3つの場所のいずれかに **action** CLI コマンドの出力を送信できます。

- **なし**：デフォルトの設定です。出力を破棄します。
- **コンソール**：出力を ASA コンソールに送信します。
- **ファイル**：出力をファイルに送信します。次の 4 つのファイル オプションを使用できます。
  - **一意のファイルを作成する**：イベントマネージャアプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
  - **ファイルを作成する/ファイルを上書きする**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。

- **ファイルを作成する/ファイルに付加する**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
- **一連のファイルを作成する**：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

EEM のガイドライン

ここでは、EEM を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードではサポートされません。

その他のガイドライン

- 通常、クラッシュ時は、ASA の状態は不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。
- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は **output none** です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

EEM の設定

EEM の設定は、次のタスクで構成されています。

手順

ステップ 1 イベント マネージャ アプレットの作成とイベントの設定 （1230 ページ）。
ステップ 2 アクションおよびアクションの出力先の設定 （1231 ページ）を使用して無効にすることができます。
ステップ 3 イベントマネージャ アプレットの実行 （1232ページ）を使用して無効にすることができます。

ステップ 4 トラック メモリ割り当ておよびメモリ使用量（1232ページ）を使用して無効にすることができます。

イベント マネージャ アプレットの作成とイベントの設定

イベントマネージャアプレットを作成してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[Embedded Event Manager]** の順に選択します。

ステップ 2 [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。

ステップ 3 アプレット名（スペースを含まない）を入力し、そのアプレットに関する説明を入力します。説明の長さは最大256文字です。引用符内であれば、説明テキストにスペースを含めることができます。

ステップ 4 [Events] 領域にある [Add] をクリックして、[Add Event Manager Applet Event] ダイアログボックスを表示します。

ステップ 5 [Type] ドロップダウン リストから設定したいイベント タイプを選択します。使用可能なオプションは、[Crashinfo]、[None]、[Syslog]、[Once-a-day timer]、[One-shot timer]、および [Periodic timer] です。

- [Syslog]：単一の syslog メッセージまたは syslog メッセージの範囲を入力します。指定された個々の syslog メッセージまたは syslog メッセージの範囲に一致する syslog メッセージが発生すると、イベント マネージャ アプレットがトリガーされます。（オプション）イベント マネージャ アプレットを呼び出すために syslog メッセージが発生する必要がある回数を [Occurrences] フィールドに入力します。デフォルトの発生回数は 0 秒ごとに 1 回です。有効な値は、1 ～ 4294967295 です。（オプション）アクションを呼び出すために syslog メッセージが発生しなければならない許容時間（秒数）を [Period] フィールドに入力します。この値によって、イベント マネージャ アプレットが設定された期間に 1 回呼び出される際の最大の間隔が制限されます。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。
- [Periodic]：期間を秒単位で入力します。 秒数は、1 ～ 604800 の範囲で設定してください。
- [Once-a-day timer]：時刻を hh:mm:ss の形式で入力します。時刻の範囲は 00:00:00（真夜中）から 23:59:59 です。
- [One-shot timer]：期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
- [None]：イベント マネージャ アプレットを手動で呼び出すには、このオプションを選択します。

- [Crashinfo]：ASA のクラッシュ時にクラッシュ イベントをトリガーするには、このオプションを選択します。

アクションおよびアクションの出力先の設定

アクションおよびアクションの出力を送信する特定の宛先を設定するには、次の手順を実行します。

手順

ステップ 1 [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。

ステップ 2 アプレット名（スペースを含まない）を入力し、そのアプレットに関する説明を入力します。説明の長さは最大 256 文字です。

ステップ 3 [Actions] 領域にある [Add] をクリックして、[Add Event Manager Applet Action] ダイアログボックスを表示します。

ステップ 4 [Sequence #] フィールドに一意のシーケンス番号を入力します。有効なシーケンス番号の範囲は 0 ～ 4294967295 です。

ステップ 5 CLI コマンドを [CLI Command] フィールドに入力します。このコマンドは、特権レベル 15（最高）を持つユーザーとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。

ステップ 6 [OK] をクリックして、[Add Event Manager Applet Action] ダイアログボックスを閉じます。

新しく追加されたアクションが [Actions] リストに表示されます。

ステップ 7 [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを開きます。

ステップ 8 使用可能な出力先オプションを 1 つ選択します。

- **action** コマンドからの出力を破棄するには、[Output Location] ドロップダウン リストから [None] オプションを選択します。これがデフォルト設定です。
- **action** コマンドの出力をコンソールに送信するには、[Output Location] ドロップダウン リストから [Console] オプションを選択します。

  （注） このコマンドを実行すると、パフォーマンスに影響を及ぼします。

- **action** コマンドの出力を呼び出された各イベント マネージャ アプレットの新しいファイルに送信するには、[Output Location] ドロップダウン リストから [File] オプションを選択します。[Create a unique file] オプションがデフォルトとして自動的に選択されます。

  ファイル名の形式は、eem-*applet-timestamp*.log です。ここで、*applet* はイベント マネージャ アプレットの名前、*timestamp* は日付のタイム スタンプ（形式は YYYYMMDD-hhmmss）を示しています。

- ローテーションされる一連のファイルを作成するには、[Output Location] ドロップダウン リストから [File] オプションを選択し、続いてドロップダウン リストから [Create a set of files] オプションを選択します。

  新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数で示されます。有効なローテーションの値の範囲は 2 ～ 100 です。ファイル名の形式は、eem-*applet-x*.log です。ここで、*applet* はアプレットの名前、*x* はファイル番号を示しています。

- **action** コマンドの出力を毎回上書きされる単一のファイルに書き込むには、[Output Location] ドロップダウン リストから [File] オプションを選択し、続いてドロップダウン リストから [Create/overwrite a file] オプションを選択します。

- **action** コマンドの出力を毎回上書きされる単一のファイルに書き込むには、[Output Location] ドロップダウン リストから [File] オプションを選択し、続いてドロップダウン リストから [Create/append a file] オプションを選択します。

ステップ 9 [OK] をクリックして、[Add Event Manager Applet] ダイアログボックスを閉じます。

指定した出力先は [Embedded Event Manager] ペインに表示されます。

イベント マネージャ アプレットの実行

イベント マネージャ アプレットを実行するには、次の手順を実行します。

手順

ステップ 1 [Embedded Event Manager] ペインで、**None** イベントで設定されたイベント マネージャ アプレットをリストから選択します。

ステップ 2 [**実行（Run）**] をクリックします。

トラック メモリ割り当ておよびメモリ使用量

メモリ割り当てとメモリ使用量をログに記録するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Advanced]** > **[Embedded Event Manager]** の順に選択します。

ステップ 2 [Add] をクリックして、[Add Event Manager Applet] ダイアログボックスを表示します。

ステップ 3 もう一度 [Add] をクリックして、[Add Event Manager Applet Event] ダイアログボックスを表示します。

ステップ 4 ドロップダウン リストから [memory-logging-wrap] を選択します。

ステップ 5 [OK] をクリックして、それを [Events] リストに追加します。

ステップ 6 もう一度 [OK] をクリックして、それを [Applets] リストに追加します。

EEM のモニターリング

EEM をモニターするには、次のコマンドを参照してください。

- **.[Monitoring] > [Properties] > [EEM Applets]**

  このペインでは、EEM アプレットとそのヒット カウント値のリストを表示します。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

EEM の履歴

表 *56 : EEM* の履歴

機能名	プラットフォームリリース	説明
Embedded Event Manager（EEM）	9.2(1)	EEMサービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEMサービスには2つのコンポーネント、つまりEEMが応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。 次の画面が導入されました。[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager]、[Monitoring] > [Properties] > [EEM Applets]。

機能名	プラットフォームリリース	説明
EEM のメモリ トラッキング	9.4(1)	メモリ割り当てとメモリ使用量をログに記録し、メモリ ロギング ラップ イベントに応答する新しいデバッグ機能が追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced] > [Embedded Event Manager] > [Add Event Manager Applet] > [Add Event Manager Applet Event]

第 45 章

テストとトラブルシューティング

この章では、Cisco ASA のトラブルシューティング方法および基本接続のテスト方法について説明します。

イネーブル パスワードと Telnet パスワードの回復

ASA モデルでは、イネーブルパスワードまたは Telnet パスワードを忘れた場合に回復できます。 手順は、デバイス タイプによって異なります。CLI を使用してタスクを実行する必要があります。

（注） その他のプラットフォームでは、パスワードを忘れた場合に回復することはできません。工場出荷時のデフォルト設定に戻すことは可能で、パスワードをデフォルトにリセットできます。Firepower 4100/9300 の場合は、『FXOS configuration guide』を参照してください。Firepower 1000 および 2100 の場合は、『FXOS troubleshooting guide』を参照してください。

ASA 5500-X でのパスワードの回復

この手順は、ASA 5525-X、5545-X、5555-X で実行できます。

ASA のパスワードを回復するには、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMONモードに入るようにプロンプトが表示されたら、**Escape**キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

ステップ 5 スタートアップ コンフィギュレーションを無視するように ASA を設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

ASAによって現在のコンフィギュレーションのレジスタ値が表示され、それを変更するかどうかが尋ねられます。

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

ステップ 6 後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

ステップ 7 値を変更する場合は、プロンプトに対して **Y** を入力します。

ASA によって、新しい値の入力を求めるプロンプトが表示されます。

ステップ 8 「disable system configuration?」の値を除き、すべての設定についてデフォルト値を受け入れます。

ステップ 9 プロンプトに対して、**Y** を入力します。

ステップ 10 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップコンフィギュレーションの代わりにデフォルトコンフィギュレーションをロードします。

ステップ 11 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 12 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 13 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 14 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 15 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 16 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 17 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506-X、ASA 5508-X、ASA 5516-X でのパスワードの回復

ASA 5506-X、ASA 5508-X、ASA 5516-X のパスワードの回復には、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMONモードに入るようにプロンプトが表示されたら、**Escape**キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASAで現在のコンフィギュレーション レジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ..... auto-boot index 1 image in disks
```

ステップ 5 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 6 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 7 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 8 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 11 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 12 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASAv でのパスワードまたはイメージの回復

ASAv のパスワードまたはイメージを回復するには、次の手順を実行します。

手順

ステップ 1 実行コンフィギュレーションを ASAv のバックアップ ファイルにコピーします。

copy running-config *filename*

例：

```
ciscoasa# copy running-config backup.cfg
```

ステップ 2 ASAv を再始動します。

reload

ステップ 3 [GNU GRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしない**オプションで <**filename**> を選択し、Enter キーを押します。ファイル名は、ASAv のデフォルトのブート イメージのファイル名です。デフォルトのブート イメージは、**fallback** コマンドによって自動的にブートされることはありません。その後、選択したブート イメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
```

bootflash: /asa100123-20-smp-k8.bin with no configuration load

例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

ステップ 4 実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy *filename* **running-config**

例：

```
ciscoasa (config)# copy backup.cfg running-config
```

ステップ 5 パスワードのリセット。

enable password *password*

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ 6 新しい設定を保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ASA ハードウェアのパスワード回復の無効化

（注） ASAv または Firepower のモデルでパスワード回復をディセーブルにすることはできません。

権限のないユーザーがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

始める前に

ASA で、**no service password-recovery** コマンドを使用すると ROMMON モードに入って、コンフィギュレーションの変更を防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去

しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザーがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

service password-recovery コマンドは、コンフィギュレーション ファイルに通知用としてのみ表示されます。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。（パスワード回復の準備段階で）スタートアップ時にスタートアップ コンフィギュレーションを無視するよう ASA が設定されている場合にパスワード回復をディセーブルにすると、通常どおりスタートアップ コンフィギュレーションをロードするように ASA の設定が変更されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password- recovery** コマンドでスタンバイ装置に複製したときに、コンフィギュレーション レジスタに同じ変更が加えられます。

手順

パスワード回復をディセーブルにします。

no service password-recovery

例：

```
ciscoasa (config)# no service password-recovery
```

Packet Capture Wizard を使用したキャプチャの設定と実行

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは ACL を使用して、キャプチャされるトラフィックのタイプを、送信元と宛先のアドレスとポート、および 1 つ以上のインターフェイスで制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを 1 回実行します。キャプチャしたパケットは、PC に保存してパケット アナライザで分析できます。

（注） このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

手順

ステップ 1 **[Wizards]** > **[Packet Capture Wizard]** の順に選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。これらのタスクには、以下が含まれます。

- 入力インターフェイスの選択。
- 出力インターフェイスの選択。
- バッファ パラメータの設定。
- キャプチャの実行。
- （オプション）キャプチャ データの PC への保存。

ステップ 2 [Next] をクリックします。

クラスタ環境では、[Cluster Option] 画面が表示されます。ステップ 3 に進みます。

非クラスタ環境では、[Ingress Traffic Selector] 画面が表示されます。ステップ 4 に進みます。

ステップ 3 [Cluster Option] 画面で、キャプチャの実行対象として [This device only] または [The whole cluster] のいずれかのオプションを選択します。[Next] をクリックして [Ingress Selector] 画面を表示します。

ステップ 4 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。

クラスタリング環境では、クラスタ コントロール プレーン パケットのみをキャプチャするには、[CP-Cluster] チェックボックスをオンにします。

ステップ 5 ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 6 [Packet Match Criteria] 領域で、次のいずれかを実行します。

- パケットの照合に使用する ACL を指定するには、[Specify access-list] オプション ボタンをクリックし、[Select ACL] ドロップダウン リストから ACL を選択します。以前設定した ACL を現在のドロップダウン リストに追加するには、[Manage] をクリックして [ACL Manager] ペインを表示します。ACL を選択して [OK] をクリックします。
- [**Specify Packet Parameters**] オプション ボタンをクリックして、パケット パラメータを指定します。

a) [ICMP Capture] ドロップダウンリストで次のいずれかを実行します。

（注） [ICMP Capture] フィールドは、前のウィンドウでクラスタ オプションとして [The whole cluster] を選択した場合にのみ設定されます。

- ファイアウォールデバイスに入った時点で、通常のトラフィックと復号化されたトラフィックの両方を含む復号化された IPsec パケットをキャプチャするには、[include-decrypted] を選択します。
- クラスタ ユニット上の永続パケットをキャプチャするには、[persist] を選択します。

ステップ 7 以降の手順については、入力トラフィック セレクタ （1245 ページ）を参照してください。

ステップ 8 [Next] をクリックして、[Egress Traffic Selector] 画面を表示します。

ステップ 9 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。

クラスタリング環境でクラスタ コントロール プレーン パケットみをキャプチャするには、[CP-Cluster] チェックボックスをオンにします。

（注） [Egress Traffic Selector] のフィールドの詳細については出力トラフィック セレクタ （1246 ページ）を参照してください。

[Egress Traffic Selector] のフィールドの詳細については出力トラフィック セレクタ （1246 ページ）を参照してください。

ステップ 10 [Next] をクリックして [Buffers & Captures] 画面を表示します。続行するには、「バッファ」(34-8 ページ）を参照してください。

ステップ 11 最新のキャプチャを 10 秒ごとに自動的に取得するように、[Capture Parameters] 領域で [Get capture every 10 seconds] チェックボックスをオンにします。デフォルトでは、このキャプチャは循環バッファを使用します。

ステップ 12 [Buffer Parameters] 領域で、バッファ サイズとパケット サイズを指定します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

a) パケット サイズを入力します。有効なサイズ範囲は 14 ～ 1522 バイトです。
b) バッファ サイズを入力します。有効なサイズ範囲は 1534 ～ 33554432 バイトです。
c) キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

（注） この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

ステップ 13 [Next] をクリックして、入力したクラスタ内の全装置のクラスタ オプション（クラスタを使用している場合）、トラフィック セレクタ、バッファ パラメータを表示する [Summary] 画面を表示します。続行するには、「サマリー」(34-8 ページ）を参照してください。

ステップ 14 [Next] をクリックして [Run Captures] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。以降の手順については、キャプチャの実行 （1247 ページ）を参照してください。クラスタリングを使用している場合は、ステップ 14 に進みます。

ステップ 15 残りのバッファ スペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。

ステップ 16 クラスタ環境では、[Run Captures] 画面で、次の手順の 1 つ以上を実行します。

- [Get Cluster Capture Summary] をクリックすると、クラスタ内の全装置のパケット キャプチャ情報のサマリーに続いて、各装置のパケット キャプチャ情報が表示されます。
- [Get Capture Buffer] をクリックすると、クラスタの各装置にどの程度バッファ スペースが残っているかが表示されます。[Capture Buffer from Device] ダイアログ ボックスが表示されます。
- [Clear Capture Buffer] をクリックすると、クラスタ内の特定の装置またはすべての装置の現在のコンテンツを削除し、さらにパケットをキャプチャするためのバッファ容量を確保します。

ステップ 17 [Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。続行するには、「キャプチャの保存」(34-9 ページ）を参照してください。

ステップ 18 [Save Ingress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。

ステップ 19 [Launch Network Sniffer Application] をクリックして、**[Tools]** > **[Preferences]** で指定したパケット分析アプリケーションを起動し、入力キャプチャを分析します。

ステップ 20 [Save Egress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。

ステップ 21 [Launch Network Sniffer Application] をクリックして、**[Tools]** > **[Preferences]** で指定したパケット分析アプリケーションを起動し、出力キャプチャを分析します。

ステップ 22 [Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

パケット キャプチャのガイドライン

コンテキスト モード

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
- 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。

- キャプチャを指定したインターフェイスに着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN 上の他のコンテキストへのトラフィックも含まれます。したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブ キャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

その他のガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP が *invalid-tcp-hdr-length* であるというドロップ理由でそのパケットをドロップする場合、そのパケットを受信したインターフェイス上の **show capture** コマンド出力は、そのパケットを表示しません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- パケットキャプチャには、システムを変更する、またはインスペクションのために接続に挿入されるパケット、NAT、TCPの正規化、パケットの内容を調整するその他の機能が含まれます。
- データパスに挿入された仮想パケットの寿命のトレースは、データパスでの物理パケットの処理を正確に反映していません。この違いは、ソフトウェアバージョン、構成、および挿入された仮想パケットのタイプによって異なります。違いが生じる原因となる可能性がある構成の設定を次に示します。
  - 同じホストに対して 2 つ以上の NAT ステートメントが存在する。
  - 接続の順方向と逆方向のフローでプロトコルが異なる（順方向のフローが UDP または TCP で、逆方向のフローが ICMP である場合など）。
  - ICMP エラーインスペクションが有効になっている。

入力トラフィック セレクタ

パケットキャプチャの入力インターフェイス、送信元と宛先のホストまたはネットワーク、およびプロトコルを設定するには、次の手順を実行します。

手順

ステップ 1 ドロップダウン リストから入力インターフェイス名を選択します。

ステップ 2 入力送信元ホストおよびネットワークを入力します。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 3 入力宛先ホストおよびネットワークを入力します。

ステップ 4 キャプチャするプロトコル タイプを指定します。指定できるプロトコルは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp です。

a) ICMP にのみ ICMP タイプを入力します。指定できるタイプは、all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。

b) TCP および UDP プロトコルだけの送信元および宛先ポートのサービスを指定します。指定できるオプションは次のとおりです。

- すべてのサービスを含めるには、[All Services] を選択します。
- サービス グループを含めるには、[Service Groups] を選択します。

  特定のサービスを含めるには、aol、bgp、chargen、cifx、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、または whois のいずれかを指定します。

ステップ 5 Cisco TrustSec サービスのパケット キャプチャをイネーブルにするには、[Security Group Tagging] 領域の [SGT number] チェックボックスをオンにして、セキュリティ グループ タグ番号を入力します。有効なセキュリティ グループ タグ番号は 2 ～ 65519 です。

出力トラフィック セレクタ

パケット キャプチャでの出力インターフェイス、送信元と宛先のホストとネットワーク、および送信元と宛先ポートのサービスを設定するには、次の手順を実行します。

手順

ステップ 1 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 2 ドロップダウン リストから出力インターフェイス名を選択します。

ステップ 3 出力送信元ホストおよびネットワークを入力します。

ステップ 4 出力宛先ホストおよびネットワークを入力します。

入力設定時に選択したプロトコル タイプがすでにリストされています。

Buffers

パケット キャプチャのパケット サイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定するには、次の手順を実行します。

手順

ステップ 1 キャプチャが保持できる最長のパケットを入力します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。

ステップ 2 パケットを保存するためにキャプチャが使用できるメモリの最大容量を入力します。

ステップ 3 パケットの保存には循環バッファを使用します。循環バッファのバッファ ストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。

要約

[Summary] 画面には、クラスタ オプション（クラスタリングを使用している場合）、トラフィック セレクタ、前のウィザード画面で選択したパケット キャプチャのためのバッファ パラメータが表示されます。

キャプチャの実行

キャプチャ セッションの開始および停止、キャプチャ バッファの表示、ネットワーク アナライザ アプリケーションの起動、パケット キャプチャの保存、およびバッファのクリアを行うには、次の手順を実行します。

手順

ステップ 1 [Start] をクリックして、選択したインターフェイス上でパケット キャプチャ セッションを開始します。

ステップ 2 [Stop] をクリックして、選択したインターフェイス上のパケット キャプチャ セッションを停止します。

ステップ 3 [Get Capture Buffer] をクリックして、インターフェイス上でキャプチャされたパケットのスナップショットを取得します。

ステップ 4 [Ingress] をクリックして、入力インターフェイスのキャプチャ バッファを表示します。

ステップ 5 [Egress] をクリックして、出力インターフェイスのキャプチャ バッファを表示します。

ステップ 6 [Clear Buffer on Device] をクリックして、デバイス上のバッファを消去します。

ステップ 7 [Launch Network Sniffer Application] をクリックして、**[Tools]** > **[Preferences]** で指定した、入力キャプチャまたは出力キャプチャを分析するためのパケット分析アプリケーションを起動します。

ステップ 8 [Save Captures] をクリックして、入力キャプチャおよび出力キャプチャを ASCII または PCAP 形式で保存します。

キャプチャの保存

パケットをさらに分析するために、入力および出力パケット キャプチャを ASCII または PCAP ファイル形式で保存するには、次の手順を実行します。

手順

ステップ 1 キャプチャ バッファを ASCII 形式で保存するには、[ASCII] をクリックします。

ステップ 2 キャプチャ バッファを PCAP 形式で保存するには、[PCAP] をクリックします。

ステップ 3 入力パケット キャプチャを保存するファイルを指定するには、[Save ingress capture] をクリックします。

ステップ 4 出力パケット キャプチャを保存するファイルを指定するには、[Save egress capture] をクリックします。

ASAv の vCPU 使用量

ASAv の vCPU 使用率では、データ パス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

vSphere で報告される vCPU の使用率には、この ASAv の使用率に加えて、次のものが含まれます。

- ASAv アイドル時間
- ASAv VM に使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASAv のレポート：40%

- DP：35%
- 外部プロセス：5%
- vSphere のレポート：95%
- ASA（ASAv レポートとして）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASAv のためのオーバーヘッドとして、ESXi サーバーが追加のコンピューティング リソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート（%USER、%IDLE、%SYS など）の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバーのシェル（ホストへの接続に SSH を使用してシェルにアクセスします）では、esxtop を使用できます。Esxtop は Linux の **top** コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細
- 各 VM のステートごとの vCPU 使用率
- メモリ（実行中に「M」と入力）とネットワーク（実行中に「N」と入力）に加えて、統計情報と RX ドロップ数

ASAv のグラフと vCenter のグラフ

ASAv と vCenter の間で CPU 使用率の数字に違いがあります。

- vCenter のグラフの数値は常に ASAv の数値よりも大きくなります。
- vCenter ではこの値は「%CPU usage」と呼ばれ、ASAv ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。

- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

使用率を MHz で比較すると、vCenter と ASAv の両方の数値は一致します。vCenter グラフから、MHz % CPU 使用率は 60/(2499 x 1 vCPU) = 2.4 と求められます。

設定のテスト

ここでは、シングル モード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイス上のホストから他のインターフェイス上のホストに ping できるようにする方法について説明します。

基本接続のテスト：アドレス向けの ping の実行

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。次のトピックでは、このコマンドの詳細とそれを使って実行可能なテストについて説明します。

ping で実行可能なテスト

デバイスを ping すると、そのデバイスにパケットが送信され、デバイスが応答を返します。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping を使用して、次のテストを実行できます。

- 2 つのインターフェイスのループバック テスト：同じ ASA で一方のインターフェイスからもう一方のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- ASA の ping：別の ASA のインターフェイスを ping し、そのインターフェイスがアップしていて応答することを確認できます。

- ASA 経由の ping：ASA の反対側のデバイスを ping することによって、中間 ASA 経由で ping することができます。パケットは、それぞれの方向に移動するときに、2 つの中間 ASA のインターフェイスを通過します。このアクションは、中間ユニットのインターフェイス、動作、および応答時間の基本テストになります。
- ネットワーク デバイスの疑わしい動作をテストするための ping：ASA インターフェイスから、正常に機能していないと思われるネットワーク デバイスに ping することができます。インターフェイスが正しく設定されているにもかかわらずエコーが受信されない場合は、デバイスに問題があると考えられます。
- 中間通信をテストするための ping：ASA インターフェイスから、正常に機能することがわかっているネットワーク デバイスに ping することができます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ICMP ping と TCP ping の選択

ASA には、ICMP エコー要求パケットを送信して、エコー応答パケットを受信する従来の ping が付属しています。これは、標準ツールで、すべての仲介ネットワーク デバイスで ICMP トラフィックが許可される場合にうまく機能します。ICMP ping を使用して、IPv4/IPv6 アドレスまたはホスト名を ping することができます。

ただし、ICMP を禁止しているネットワークもあります。ご使用のネットワークがこれに該当する場合は、代わりに、TCP ping を使用してネットワーク接続をテストできます。TCP ping では、ping から TCP SYN パケットが送信され、応答で SYN-ACK が受信された段階でその ping が成功したと見なされます。また、TCP ping では、IPv4 アドレスまたはホスト名は ping できますが、IPv6 アドレスは ping できません。

正常な ICMP または TCP ping とは、使用されているアドレスが有効で特定のタイプのトラフィックに応答することを意味しているにすぎません。これは基本接続が機能していることを意味します。デバイス上で動作する他のポリシーで、特定のタイプのトラフィックがデバイスを通過できないようにすることができます。

ICMP の有効化

デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの ping を実行できます。リターン トラフィックを通過させるように ICMP インスペクションをイネーブルにすることだけが必要です。セキュリティの低いインターフェイスから高いインターフェイスに ping するには、トラフィックを許可する ACL を適用する必要があります。

ASA インターフェイスを ping する場合は、そのインターフェイスに適用された ICMP ルールによって、エコー要求パケットとエコー応答パケットが許可される必要があります。ICMP ルールは省略可能です。このルールを設定しなかった場合は、インターフェイスへのすべての ICMP トラフィックが許可されます。

この手順では、ASA インターフェイスの ICMP ping をイネーブルにするため、または、ASA 経由の ping 用に構成する必要のある ICMP コンフィギュレーションのすべてについて説明します。

手順

ステップ 1 ICMP ルールでエコー要求/エコー応答が許可されることを確認します。

ICMP ルールは、省略可能で、インターフェイスに直接送信される ICMP パケットに適用されます。ICMP ルールを適用しなかった場合は、すべての ICMP アクセスが許可されます。この場合は、アクションが不要です。

ただし、ICMP ルールを実装する場合は、エコー要求メッセージとエコー応答メッセージのアドレスを許可するルールが各インターフェイスに含まれていることを確認します。[Configuration] > [Device Management] > [Management Access] > [ICMP] ペインで ICMP ルールを設定します。

ステップ 2 アクセス ルールで ICMP が許可されることを確認します。

ASA 経由でホストを ping する場合は、アクセス ルールで ICMP トラフィックの送受信が許可される必要があります。アクセス ルールは、少なくとも、エコー要求/エコー応答 ICMP パケットを許可する必要があります。これらのルールはグローバル ルールとして追加することができます。

アクセス ルールを使用しない場合は、必要な他のタイプのトラフィックも許可する必要があります。これは、インターフェイスにアクセス ルールを適用すると、暗黙の deny が追加されるため、他のすべてのトラフィックが破棄されるためです。

[Configuration] > [Firewall] > [Access Rules] ペインでアクセス ルールを設定します。単にテスト目的でルールを追加する場合は、テストの終了後にそのルールを削除できます。

ステップ 3 ICMP インスペクションをイネーブルにします。

インターフェイスの ping とは対照的に、ASA 経由で ping する場合は、ICMP インスペクションが必要です。インスペクションを使用すれば、リターン トラフィック（つまり、エコー応答パケット）を ping を開始したホストに返すことができるうえ、パケットあたり 1 つの応答の存在が保証されるため、特定のタイプの攻撃を防止することができます。

ICMPインスペクションは、デフォルトのグローバルインスペクション ポリシーでイネーブルにできます。

a) **[Configuration] > [Firewall] > [Service Policy Rules]** の順に選択します。
b) **inspection_default** グローバル ルールを編集します。
c) [Rule Actions] > [Protocol Inspection] タブで、ICMP を選択します。
d) [OK] をクリックし、さらに [Apply] をクリックします。

ホストの ping

デバイスを ping するには、[Tools] > [Ping] を選択して、ping する宛先の IP アドレスまたはホスト名を入力し、[Ping] をクリックするだけです。TCP ping の場合は、[TCP] を選択して、宛先ポートも含めます。通常は、実行する必要のあるテストの範囲にします。

成功した ping の出力例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合は、失敗した試行が ? で示され、成功率が 100% 未満になります（すべて失敗した場合は 0% になります）。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ただし、pingの一部の側面を制御するパラメータを追加することもできます。以下に基本オプションを示します。

- ICMP ping：宛先ホストに接続するインターフェイスを選択できます。インターフェイスを選択しなかった場合は、ルーティングテーブルを使用して、適切なインターフェイスが決定されます。IPv4/IPv6 アドレスまたはホスト名を ping することができます。
- TCP ping：ping する宛先の TCP ポートを選択する必要もあります。たとえば、HTTP ポートを ping するには **www.example.com 80** とします。IPv4 アドレスまたはホスト名を ping することはできますが、IPv6 アドレスを ping することはできません。

  ping を送信する送信元アドレスおよびポートを指定するオプションもあります。この場合は、任意で、送信元から ping が送信されるインターフェイスを選択します（インターフェイスを選択しなかった場合は、ルーティング テーブルが使用されます）。

  最後に、ping を繰り返す回数（デフォルトは 5 回）または各試行のタイムアウト（デフォルトは 2 秒）を指定できます。

ASA 接続の体系的なテスト

ASA 接続のさらに体系的なテストを実行する場合は、次の一般的な手順を使用できます。

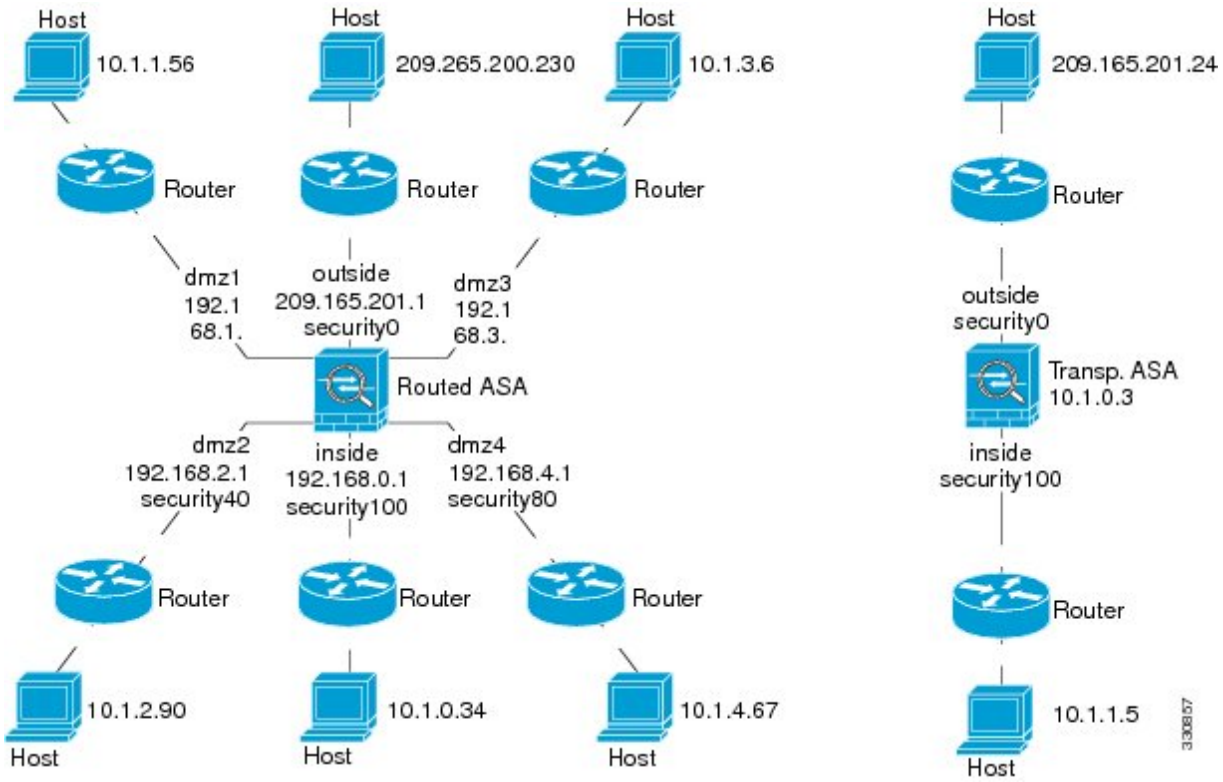
始める前に

手順で説明した syslog メッセージを確認する場合は、ロギングをイネーブルにします（**logging enable** コマンドまたは ASDM の [Configuration] > [Device Management] > [Logging] > [Logging Setup]）。

手順

ステップ 1 インターフェイス名、セキュリティ レベル、および IP アドレスを示すシングル モードの ASA またはセキュリティ コンテキストの図を作成します。図には、直接接続されたすべてのルータ、および ASA を ping するルータの反対側にあるホストも含める必要があります。

図 *76 : インターフェイス、ルータ、およびホストを含むネットワーク図*



ステップ 2 直接接続されたルータから各 ASA インターフェイスを ping します。トランスペアレント モードでは、BVI IP アドレスを ping します。このテストでは、ASA インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ASA インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（次の図を参照）。この場合は、パケットが ASA に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

図 *77 : ASA インターフェイスでの ping の失敗*

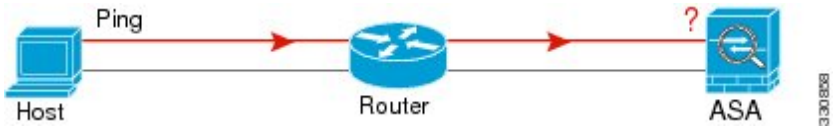
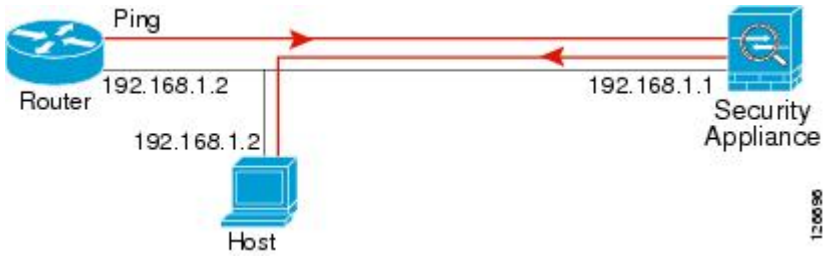


図 *78 : IP* アドレッシングの問題による *ping* の失敗



ping 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（次の図を参照）。

ステップ 3 リモート ホストから各 ASA インターフェイスを ping します。トランスペアレント モードでは、BVI IP アドレスを ping します。このテストでは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA にない場合、ping は失敗する可能性があります（次の図を参照）。この場合は、デバッグ メッセージはpingが成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 *79 : ASA* の戻りルート未設定による *ping* の失敗

ステップ 4 ASA インターフェイスから既知のネットワーク デバイスへの ping は正しく機能しています。

- pingを受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASAのインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイス ハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ステップ 5 ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

ping が成功すると、ルーテッド モードのアドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認する syslog メッセージが表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力してこの情報を表示することもできます。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます（305005 または 305006）。ping

が外部ホストから内部ホストへ送信され、スタティック変換が存在しない場合は、メッセージ 106010 が表示されます。

図 *80 : ASA* のアドレス変換の問題による *ping* の失敗

ホストまでのルートの追跡

IPアドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワーク パスに問題がないかどうかを確認できます。

手順

ステップ 1 トレース ルート上の ASA の表示 （1256 ページ）。

ステップ 2 パケット ルートの決定 （1257 ページ）を使用して無効にすることができます。

トレース ルート上の ASA の表示

デフォルトで、ASA はトレース ルート上にホップとして表示されません。これを表示するには、ASA を通過するパケットの存続可能時間を減らして、ICMP 到達不能メッセージのレート制限を増やす必要があります。

手順

ステップ 1 サービス ポリシーを使用して TTL を減らします。

a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。

b) ルールを追加または編集します。たとえば、TTL を減らすためのオプションを追加可能なルールがすでに存在する場合は、新しいルールを作成する必要はありません。

c) ルールをグローバルまたはインターフェイスに適用し、トラフィック照合を指定する [Rule Actions] ページまでウィザードを進めます。たとえば、グローバル match any ルールを作成できます。

d) [Rule Actions] ページで、[Connection Settings] タブをクリックして、[Decrement time to live for a connection] を選択します。

e) [OK] または [Finish] をクリックしてから、[Apply] をクリックします。

ステップ 2 ICMP 到達不能レート制限を増やします。

a) [Configuration] > [Device Management] > [Management Access] > [ICMP] を選択します。
b) ページの下部にある [IPv4 ICMP Unreachable Message Limits] > [Rate Limit] の値を増やします。たとえば、50 に増やします。
c) [適用（Apply）] をクリックします。

パケット ルートの決定

traceroute を使用すれば、パケットが宛先に到着するまでのルートを特定できます。traceroute は、無効なポート上の宛先に UDP パケットまたは ICMPv6 エコーを送信することで機能します。ポートが有効でないため、宛先への途中にあるルータは ICMP または ICMPv6 Time Exceeded Message で応答し、そのエラーを ASA に報告します。

traceroute は送信された各プローブの結果を表示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、出力記号の説明を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
U	宛先へのルートが存在しません。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。ICMPv6 では、アドレスは対象外です。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。ICMPv6 では、ポートが到達不能です。
!A	ICMP が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

手順

ステップ 1 **Tools** > **Traceroute** の順に選択します。
ステップ 2 ルートを追跡する宛先ホスト名または IP アドレスを入力します。ホスト名を使用するように DNS サーバーを設定します。
ステップ 3 （オプション）トレースの特性を設定します。デフォルトがほとんどのケースに適合します。

- [Timeout]：タイムアウトするまで応答を待機する時間。デフォルトは 3 秒です。

- [Port]：使用する UDP ポート。デフォルトは 33434 です。
- [Probe]：各 TTL レベルで送信するプローブの数。デフォルトは 3 です。
- [TTL]：プローブの最小および最大存続可能時間。デフォルトの最小値は 1 ですが、この値を増やして、既知のホップの表示を抑制することができます。デフォルトの最大値は30です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。
- [Specify source interface or IP address]：トレースの送信元として使用するインターフェイス。インターフェイスは、名前または IP アドレスで指定できます。IPv6 では、送信元インターフェイスを指定できません。送信元 IP アドレスだけを指定できます。IPv6 アドレスは、ASA インターフェイスで IPv6 を有効にしている場合にのみ有効です。トランスペアレント モードでは、管理アドレスを使用する必要があります。
- [Reverse Resolve]：DNS 名前解決が設定されている場合に検出されたホップの名前を出力に表示するかどうか。IP アドレスのみを表示するオプションを選択解除します。
- [Use ICMP]：UDP プローブ パケットの代わりに ICMP プローブ パケットを送信するかどうか。

ステップ 4 [Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

パケット トレーサを使用したポリシー設定のテスト

送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースは、ポリシー参照を実行してアクセス ルールや NAT などをテストし、パケットを許可するか、拒否するかを確認します。

このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。

手順

ステップ 1 **[Tools]** > **[Packet Tracer]** の順に選択します。

ステップ 2 パケット トレースの送信元**インターフェイス**を選択します。

ステップ 3 パケット トレースの**パケット タイプ**を指定します。指定できるプロトコル タイプは、ICMP、IP、TCP、UDP、および SCTP です。

ステップ 4 （オプション）。セキュリティ グループ タグの値がレイヤ 2 CMD ヘッダーに埋め込まれたパケットを追跡する（Trustsec）場合は、[SGT number] をオンにして、セキュリティ グループ タグの番号（0 ～ 65533）を入力します。

ステップ 5 （トランスペアレント モード）パケット トレーサが（後でサブインターフェイスにリダイレクトされる）親インターフェイスに入るようにするには、[VLAN ID] をオンにして、1 ～ 4096 の範囲の ID を入力します。VLAN ID は、入力インターフェイスがサブインターフェイスでない場合にのみ使用できます。

ステップ 6 （トランスペアレント モード）**宛先 MAC アドレス**を指定します。

ステップ 7 パケットの送信元と宛先を指定します。

Cisco TrustSec を使用する場合は、IPv4 または IPv6 アドレス、完全修飾ドメイン名（FQDN）、またはセキュリティ グループの名前あるいはタグを指定できます。送信元アドレスに対して、Domain\username 形式でユーザー名を指定することもできます。

ステップ 8 プロトコルの特性を指定します。

- [ICMP]：ICMP タイプ、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP]：送信元および宛先のポート番号を入力します。
- [Raw IP]：プロトコル番号(0 ～ 255）を入力します。

ステップ 9 クラスタ ユニット全体でパケットをデバッグするには、パケット トレーサを使用します。[Cluster Capture] ドロップダウンリストから、次の項目を選択します。

a) **decrypted**：VPN トンネルで復号化されたパケットを注入し、さらに、VPN トンネルを経由して到着するパケットをシミュレートします。
b) **persist**：クラスタ ユニット全体で追跡するパケットを注入します。
c) **bypass-checks**—Skips security checks like ACL, VPN filters, IPsec spoof, and uRPF.
d) **transmit**：シミュレートされたパケットが ASA から出られるようにします。

ステップ 10 [Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケット トレースの結果に関する詳細情報が表示されます。

パフォーマンスとシステム リソースのモニターリング

さまざまなシステム リソースをモニターすることによって、パフォーマンス上の問題またはその他の潜在的な問題を特定することができます。

パフォーマンスのモニターリング

ASA のパフォーマンス情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Connection Graphs]** > **[Perfmon]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストから最大 4 つのエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [AAA Perfmon]：認証、許可、およびアカウンティング要求に関する秒単位の要求数。
- [Inspection Perfmon]：HTTP、FTP、および TCP インスペクションに関する秒単位のパケット数。
- [Web Perfmon]：URL アクセス要求と URL サーバー要求に関する秒単位の要求数。
- [Connections Perfmon]：すべての接続、UDP 接続、TCP 接続、および TCP 代行受信に関する秒単位の接続数。
- [Xlate Perfmon]：秒単位の NAT xlate。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリ ブロックのモニターリング

空きメモリ ブロックと使用中のメモリ ブロックをグラフ形式または表形式で表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[System Resources Graphs]** > **[Blocks]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Blocks Used]：ASA で使用中のメモリ ブロックを表示します。
- [Blocks Free]：ASA の空きメモリ ブロックを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

CPU のモニターリング

CPU 使用率を表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[System Resources Graphs]** > **[CPU]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Selected Graphs] リストに [CPU Utilization] を追加します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間で表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリのモニターリング

メモリ使用量情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[System Resources Graphs]** > **[Memory]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Free Memory]：ASA の空きメモリを表示します。
- [Used Memory]：ASA の使用中のメモリを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

プロセス単位の CPU 使用率のモニターリング

CPU で実行されているプロセスをモニターできます。特定のプロセスで使用される CPU の使用率に関する情報を取得できます。CPU使用率の統計情報は降順で並べられ、使用率の最も高いプロセスが先頭に表示されます。また、プロセスごとのCPUに対する負荷に関する情報（記録時間の 5 秒前、1 分前、および 5 分前の情報）も含まれています。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。ASDM では、30 秒おきに更新されます。

プロセス単位の CPU 使用率を表示するには、**[Monitoring]** > **[Properties]** > **[Per-Process CPU Usage]** の順に選択します。

自動更新を停止して、情報を手動で更新し、ファイルに保存することができます。[Configure CPU Usage Colors] をクリックして、使用率に基づいて背景色と前景色を選択することによって、使用率の高いプロセスのスキャンを実行しやすくすることもできます。

接続のモニターリング

現在の接続を表形式で表示するには、ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [Connections] の順に選択します。各接続に関する情報には、プロトコル、送信元アドレスと宛先アドレスの特性、最後のパケットが送信または受信されてからのアイドル時間、および接続中のトラフィック量が含まれます。

テストおよびトラブルシューティングの履歴

機能名	プラットフォームリリース	説明
tracerouteの IPv6 サポート	9.7(1)	**traceroute** コマンドが変更され、IPv6 アドレスも受け入れられるようになりました。 次の画面が変更されました。**[Tools]** > **[Traceroute]**

機能名	プラットフォームリリース	説明
ブリッジグループメンバーインターフェイス用のパケットトレーサのサポート	9.7(1)	ブリッジグループメンバーインターフェイスにパケット トレーサを使用できるようになりました。 パケット トレーサの画面に [VLAN ID] および [Destination MAC Address] フィールドが追加されました。**[Tools]** > **[Packet Tracer]**
手動によるパケット キャプチャの開始と停止	9.7(1)	キャプチャを手動で停止および開始できるようになりました。 追加/変更された画面：**[Wizards]** > **[Packet Capture Wizard]** > **[Run Captures]** 追加/変更されたオプション：[Start] ボタン、[Stop] ボタン

機能名	プラットフォームリリース	説明
強化されたパケット トレーサおよびパケット キャプチャ機能	9.9(1)	

機能名	プラットフォームリリース	説明
		パケット トレーサは次の機能で強化されました。 • パケットがクラスタ ユニット間を通過するときにパケットを追跡します。 • シミュレートされたパケットが ASA から出られるようにします。 • シミュレートされたパケットのセキュリティ チェックをバイパスします。 • シミュレートされたパケットを IPsec/SSL で復号化されたパケットとして扱います。 パケット キャプチャは次の機能で強化されました。 • パケットを復号化した後にキャプチャします。 • トレースをキャプチャし、永続リストに保持します。 新規または変更された画面： **[Tools]** > **[Packet Tracer]** 次のオプションをサポートする [Cluster Capture] フィールドを追加しました：[decrypted]、[persist]、[bypass-checks]、[transmit] [All Sessions] ドロップダウン リストの下の [Filter By] ビューに 2 つの新しいオプションを追加しました：[Origin] および [Origin-ID] **[Monitoring]** > **[VPN]** > **[VPN**

機能名	プラットフォームリリース	説明
		Statistics] > **[Packet Tracer and Capture]** [Packet Capture Wizard] 画面に [ICMP Capture] フィールドを追加しました：**[Wizards]** > **[Packet Capture Wizard]** ICMP キャプチャをサポートする 2 つのオプション、**include-decrypted** および **persist** を追加しました。
ACL を使用せず IPv6 トラフィックを一致させるためのパケット キャプチャのサポート	9.10(1)	**capture** コマンドの **match** キーワードを使用する場合、**any** キーワードは IPv4 トラフィックのみ照合します。IPv4 または IPv6 トラフィックをキャプチャするために、**any4** と **any6** キーワードを指定できるようになりました。**any** キーワードでは、引き続き IPv4 トラフィックのみ照合されます。 新規/変更されたコマンド：**capture match** ASDM サポートはありません。
Forepower 9300/4100 の新しい **debug telemetry** コマンド	9.14(1)	**debug telemetry** コマンドを使用すると、テレメトリに関連するデバッグメッセージが表示されます。このデバッグは、テレメトリレポートの生成時にエラーの原因を特定するために役立ちます。 変更された画面はありません。

第 VIII 部

モニタリング

第 46 章

ログ

この章では、システムメッセージを記録して、トラブルシューティングに使用する方法について説明します。

ロギングの概要

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央syslogサーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslogサービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログ用の保護された長期ストレージを提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

ASA のシステムログにより、Secure Firewall ASA のモニタリングおよびトラブルシューティングに必要な情報が得られます。ロギング機能を使用して、次の操作を実行できます。

- ログに記録する syslog メッセージを指定する。
- syslog メッセージの重大度を無効化または変更する。
- 次のような syslog メッセージ送信先を 1 つ以上指定する。
  - 内部バッファ
  - 1 台以上の syslog サーバ
  - ASDM
  - SNMP 管理ステーション

- 指定の電子メール アドレス
- コンソール
- Telnet および SSH セッション。

- 重大度レベルやメッセージ クラスなどによる、グループ内での syslog メッセージを設定および管理する。
- syslog の生成にレート制限を適用するかどうかを指定する。
- 内部ログ バッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュ メモリに保存する）を指定する。
- 場所、重大度レベル、クラス、またはカスタム メッセージ リストにより、syslog メッセージをフィルタリングする。

マルチ コンテキスト モードでのロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの syslog メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

ASA は、各メッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の syslog サーバーに送信されるコンテキスト メッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。

syslog メッセージ分析

次に、さまざまな syslog メッセージを確認することで取得できる情報タイプの例を示します。

- ASA セキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA セキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA に対して発生している攻撃が表示されます。

- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザー認証とコマンドの使用により、セキュリティ ポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。
- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

syslog メッセージはパーセントの記号（%）で始まり、次のように構造化されています。

```
%ASA Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

ASA	ASA が生成するメッセージの syslog メッセージ ファシリティ コード。この値は常に ASA です。
レベル	1 ～ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザー名が含まれていることがあります。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。ASDM ログ ビューアで重大度を区別しやすくするために、重大度のそれぞれにカスタム カラーを割り当てることができます。syslog メッセージの色設定を行うには、[ツール（Tools）]>[設定（Preferences）]>[Syslog（Syslog）] タブを選択するか、またはログ ビューア自体のツールバーで [色の設定（Color Settings）] をクリックします。

表 *57 : Syslog* メッセージの重大度

レベル番号	重大度	説明
0	**emergencies**	システムが使用不可能な状態です。

レベル番号	重大度	説明
1	**alert**	すぐに措置する必要があります。
2	**critical**	深刻な状況です。
3	**error**	エラー状態です。
4	**warning**	警告状態です。
5	**Notification**（通告）	正常ですが、注意を必要とする状況です。
6	**informational**	情報メッセージです。
7	**debugging**	デバッグ メッセージです。 問題をデバッグするときに、このレベルで一時的にのみログに記録します。このログレベルでは、非常に多くのメッセージが生成される可能性があるため、システムパフォーマンスに影響を与える可能性があります。

（注） ASA は、重大度 0（緊急）の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、Secure Firewall ASA を設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージ クラス（機能エリアと同等）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するように Secure Firewall ASA を設定することもできます。

syslog メッセージ クラス

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージ クラスを指定するメッセージ リストを作成します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *58 : syslog* メッセージのクラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	ユーザ認証	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
citrix	Citrix クライアント	723
—	クラスタリング	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	セキュアなデスクトップ	724
cts	Cisco TrustSec	776

クラス	定義	Syslog メッセージ ID 番号
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレスの割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ボットネット トラフィック フィルタリング	338
—	ライセンシング	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用するための NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	Phone Proxy	337

クラス	定義	Syslog メッセージ ID 番号
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN および AnyConnect クライアント	716
—	NAT および PAT	305

ログ ビューアのメッセージのソート

すべての ASDM ログ ビューア（Real-Time Log Viewer、Log Buffer Viewer、および Latest ASDM Syslog Events Viewer）でメッセージをソートできます。複数のカラムでテーブルをソートするには、ソートの基準とする、最初のカラムのヘッダーをクリックし、**Ctrl** キーを押したまま、同時にソート順に含める他のカラムのヘッダーをクリックします。時間順にメッセージをソートするには、日付と時刻のカラムを両方選択します。どちらか一方だけを選択した場合は、（時刻に関係なく）日付のみまたは（日付に関係なく）時刻のみでメッセージがソートされます。

Real-Time Log Viewer および Latest ASDM Syslog Events Viewer でメッセージをソートすると、記録された新しいメッセージは通常の表示位置となる一番上ではなく、ソートされた順序で表示されます。つまり、メッセージはその他のメッセージの中に混ざって表示されます。

カスタム メッセージ リスト

カスタム メッセージ リストを作成して、送信する syslog メッセージとその出力先を柔軟に制御できます。カスタム syslog メッセージのリストで、次の条件のいずれかまたはすべてを使用して syslog メッセージのグループを指定します。

- 重大度
- メッセージ ID
- syslog メッセージ ID の範囲
- メッセージ クラス

たとえば、メッセージ リストを使用して次の操作を実行できます。

- 重大度が 1 および 2 の syslog メッセージを選択し、1 つ以上の電子メール アドレスに送信する。
- メッセージ クラス（「ha」など）に関連付けられたすべての syslog メッセージを選択し、内部バッファに保存する。

メッセージ リストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンドエントリで行う必要があります。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。メッセージリストの2つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

クラスタ

syslog メッセージは、クラスタリング環境でのアカウンティング、モニターリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイム スタンプおよびデバイス ID を含むヘッダー フィールドを制御で

きます。syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

（注） クラスタの装置から syslog メッセージをモニターするには、モニターする各装置に対して ASDM セッションを開く必要があります。

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

- IPv6 がサポートされます。Syslog は、TCP または UDP を使用して送信できます。
- syslog 送信用に設定されたインターフェイスが有効であること、IPv6 対応であること、および syslog サーバが指定インターフェイス経由で到達できることを確認します。
- Ipv6 を介したセキュア ロギングはサポートされていません。

その他のガイドライン

- syslog サーバでは、syslogd というサーバプログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。
- Secure Firewall ASA が生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、Secure Firewall ASA はメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数の syslog サーバーを指定するには、各 syslog サーバーの **[Syslog Server]** ペインで、個別のエントリを指定します。
- スタンドバイ デバイスでは、TCP 上での syslog の送信はサポートされません。
- トランスポートプロトコルとして TCP を使用する場合、メッセージが失われないように syslog サーバーへの接続が 4 つ開きます。syslog サーバーを使用して非常に多数のデバイスからメッセージを収集する場合、接続オーバーヘッドの合計がサーバーに対して大きすぎる場合は、代わりに UDP を使用します。
- 2 つの異なるリストまたはクラスを異なる syslog サーバーまたは同じ場所に割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。ただし、マルチ コンテキスト モードでは、コンテキストごとに 4 サーバーに制限されています。

- syslog サーバは、Secure Firewall ASA 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバーがクラッシュしないようにするため、syslog 313001、313004、および 313005 の生成を抑制します。
- syslog の UDP 接続の数は、ハードウェア プラットフォームの CPU の数と、設定する syslog サーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定する syslog サーバの数を乗算した値と同じになります。たとえば各 syslog サーバでは次のようになります。
  - Firepower 4110 では最大 22 の UDP syslog 接続が可能です。
  - Firepower 4120 では最大 46 の UDP syslog 接続が可能です。

  これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは2分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。
- アクセス リストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギング重大度がデバッグ（レベル7）のアクセス リストに対しては、アクセス リストのログは生成されません。**logging list** コマンドのロギング重大度のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセス リスト コンフィギュレーションのロギング重大度をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体も変更する必要があります。

  ロギング重大度がデバッグに変更されたため、アクセス リストのヒットが含まれていない **show running-config logging** コマンドの出力例を次に示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

次に、アクセス リスト ヒットを含む **show running-config logging** コマンドの出力例を示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

この場合、アクセス リスト コンフィギュレーションは変更せず、アクセス リスト ヒット数が次の例のように表示されます。

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
```

```
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- Secure Firewall ASA が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。
- syslog サーバーから受信したサーバー証明書には、[拡張キーの使用（Extended Key Usage）] フィールドに「ServAuth」が含まれている必要があります。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

ロギングの設定

ここでは、ロギングの設定方法について説明します。

ロギングの有効化

ロギングをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 ASDM で、次のいずれかを選択します。

- **[Home]** > **[Latest ASDM Syslog Messages]** > **[Enable Logging]**
- **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]**
- **[Monitoring]** > **[Real-Time Log Viewer]** > **[Enable Logging]**
- **[Monitoring]** > **[Log Buffer]** > **[Enable Logging]**

ステップ 2 [Enable logging] チェックボックスをオンにして、ロギングをオンにします。

出力先の設定

トラブルシューティングおよびパフォーマンスのモニターリング用に syslog メッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部 syslog サーバー、ASDM、SNMP 管理ステーション、コンソール ポート、指定した電子メール アドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

管理専用アクセスが有効になっているインターフェイスで syslog ロギングを設定した場合、データプレーン関連のログ（syslog ID 302015、302014、106023、および 304001）はドロップされて syslog サーバーに到達しません。これらの syslog メッセージがドロップされるのは、

データパス ルーティング テーブルに管理インターフェイスのルーティングがないためです。したがって、設定するインターフェイスで管理専用アクセスが無効になっていることを確認してください。

外部 syslog サーバーへの syslog メッセージの送信

外部syslogサーバーで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

外部 syslog サーバーに syslog メッセージを送信するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** を選択します。

ステップ 2 [Enable logging] チェックボックスをオンにして、ASA に対するロギングを有効にします。

ステップ 3 [Enable logging on the failover standby unit] チェックボックスをオンにして、スタンバイ ASA に対するロギングを有効にします（可能な場合）。

ステップ 4 [Send debug messages as syslogs] チェックボックスをオンにして、すべてのデバッグ トレース出力がシステム ログにリダイレクトされるようにします。このオプションがイネーブルになっている場合、syslogメッセージはコンソールには表示されません。そのため、デバッグメッセージを表示するには、コンソールでロギングをイネーブルにし、デバッグsyslogメッセージ番号および重大度レベルの宛先としてコンソールを設定する必要があります。使用するsyslogメッセージ番号は、[711001] です。この syslog メッセージに対するデフォルトの重大度レベルは、[Debugging] です。

ステップ 5 [Send syslogs in EMBLEM format] チェックボックスをオンにして、EMBLEM 形式をイネーブルにします。これにより、syslog サーバーを除くロギングの宛先すべてに対して EMBLEM 形式が使用されます。

ステップ 6 ロギング バッファがイネーブルの場合、syslog メッセージを保存する内部ログ バッファのサイズを指定します。バッファの空き容量がなくなると、FTPサーバーまたは内部フラッシュ メモリにログを保存していない限り、メッセージは上書きされます。デフォルトのバッファ サイズは 4096 バイトです。有効な範囲は 4096 ～ 1048576 です。

ステップ 7 バッファ内のデータが上書きされる前に、それらを FTP サーバーに保存する場合は、[Save Buffer To FTP Server] チェックボックスをオンします。バッファ内のデータが上書きされるようにする場合は、このチェックボックスをオフにします。

ステップ 8 [Configure FTP Settings] をクリックして、FTP サーバーを指定し、バッファ内のデータを保存する際に使用する FTP パラメータを設定します。

ステップ 9 [Save Buffer To Flash] チェックボックスをオンにして、上書きする前に内部フラッシュ メモリにバッファの内容を保存します。

（注） このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。

ステップ 10 [Configure Flash Usage] をクリックし、ロギングに使用する内部フラッシュ メモリの最大容量、および最低限維持すべき空き容量を KB 単位で指定します。このオプションをイネーブルにすると、メッセージが格納されるデバイス ディスク上に、「syslog」という名前のディレクトリが作成されます。

（注） このオプションは、単一ルーテッド モードまたはトランスペアレント モードでだけ使用できます。

ステップ 11 ASA で表示するシステムログのキューサイズを指定します。

FTP の設定

ログ バッファの内容の保存に使用する FTP サーバーのコンフィギュレーションを指定するには、次の手順を実行します。

手順

ステップ 1 [Enable FTP client] チェックボックスをオンにして、FTP クライアントのコンフィギュレーションをイネーブルにします。

ステップ 2 FTP サーバーの IP アドレスを指定します。

ステップ 3 保存されるログ バッファ コンテンツの格納先となる FTP サーバー上のディレクトリ パスを指定します。

ステップ 4 FTP サーバーにログインするためのユーザー名を指定します。

ステップ 5 FTP サーバーへログインするためのユーザー名に関連付けられたパスワードを指定します。

ステップ 6 パスワードを確認し、[OK] をクリックします。

ロギングに使用するフラッシュ メモリの設定

ログ バッファの内容を内部フラッシュ メモリに保存する場合の制限事項を指定するには、次の手順を実行します。

手順

ステップ 1 ロギングに使用できる内部フラッシュ メモリの最大容量を指定します（KB 単位）。

ステップ 2 維持する内部フラッシュ メモリの容量を指定します（KB 単位）。内部フラッシュメモリがこの制限値に近づくと、新しいログが保存されなくなります。

ステップ 3 [OK] をクリックして、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

セキュア ロギングの有効化

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Server]** の順に選択します。

ステップ 2 セキュア ロギングをイネーブルにする syslog サーバーを選択し、[Edit] をクリックします。

[Edit Syslog Server] ダイアログボックスが表示されます。

ステップ 3 [TCP] オプション ボタンをクリックします。

セキュア ロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。

ステップ 4 [Enable secure syslog with SSL/TLS] チェックボックスをオンにして、[OK] をクリックします。

ステップ 5 （任意） [Reference Identity] に、syslog サーバーから受信した証明書に対する RFC 6125 参照 ID チェックをイネーブルにする参照 ID オブジェクトを名前で指定します。

参照 ID オブジェクトについて詳しくは、参照 ID の設定 （803 ページ）を参照してください。

syslog サーバーに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバーへの EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Server]** の順に選択します。

IPv6 を介した syslog の送信がサポートされています。

ステップ 2 [Add] をクリックして、新しい syslog サーバを追加します。

[Add Syslog Server] ダイアログボックスが表示されます。

（注） 1 つのセキュリティ コンテキストに対して設定できる syslog サーバーの数は最大で 4 です（合計で 16 まで）。

ステップ 3 syslog サーバーがビジー状態の場合、ASA でキューに入れることができるメッセージ数を指定します。値がゼロの場合は、キューに入れられるメッセージ数が無制限になります。

ステップ 4 [Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにして、syslog サーバーがダウンしている場合にすべてのトラフィックを許可するように設定します。

ASA では、TCP 接続された syslog サーバーに syslog メッセージを送信するように設定されている場合、syslog サーバーに障害が発生すると、セキュリティ保護のために ASA を経由する新しい接続をブロックします。syslog サーバーが動作していない場合でも新しい接続を許可するには、このチェックボックスをオンにします。

UDP を指定すると、ASA は、syslog サーバーが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

（注） TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** を選択します。

ステップ 2 [Send syslogs in EMBLEM format] チェックボックスをオンにします。

syslog サーバーの設定の追加または編集

syslog サーバー設定を追加または編集するには、次の手順を実行します。

手順

ステップ 1 syslogサーバーとの通信に使用するインターフェイスを、ドロップダウンリストから選択します。

ステップ 2 syslog サーバーとの通信に使用する IP アドレスを入力します。

syslog サーバーが ASA または ASASM との通信に使用するプロトコル（TCP または UDP）を選択します。UDP または TCP のいずれかを使用して syslog サーバーにデータを送信するように ASA および ASASM を設定することができます。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

警告 TCP を指定すると、ASA は syslog サーバーの障害を検出したときに、セキュリティ上の理由で ASA を経由する新しい接続をブロックします。syslog サーバーに障害が発生しても新しい接続を許可するには、syslog サーバーに送信する EMBLEM 形式の syslog メッセージの生成 （1282 ページ）のステップ 4 を参照してください。

ステップ 3 syslog サーバーにおいて、ASA または ASASM との通信に使用されるポート番号を入力します。

ステップ 4 [Log messages in Cisco EMBLEM format (UDP only)] チェックボックスをオンにして、シスコの EMBLEM 形式でメッセージをログに記録するかどうかを指定します（プロトコルとして UDP が選択されている場合に限る）。

ステップ 5 [Enable secure logging using SSL/TLS (TCP only)] チェックボックスをオンにして、syslog サーバーへの接続が SSL/TLS over TCP の使用により保護され、syslog メッセージの内容が暗号化されるよう指定します。

ステップ 6 [OK] をクリックして設定を完了します。

内部ログ バッファへの syslog メッセージの送信

一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定する必要があります。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

syslog メッセージを内部ログ バッファに送信するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択して、内部ログ バッファに送信する syslog メッセージを指定します。

- **[Home]** > **[Latest ASDM Syslog Messages]** > **[Configure ASDM Syslog Filters]**
- **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Filters]**

ステップ 2 **[Monitoring]** > **[Logging]** > **[Log Buffer]** > **[View]** の順に選択します。次に [Log Buffer] ペインで **[File]** > **[Clear Internal Log Buffer]** の順に選択して、内部ログ バッファを空にします。

ステップ 3 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** の順に選択して、内部ログ バッファのサイズを変更します。デフォルトのバッファ サイズは 4 KB です。

ASA は、新しいメッセージを引き続き内部ログバッファに保存し、いっぱいになったログバッファの内容を内部フラッシュ メモリに保存します。バッファの内容を別の場所に保存するとき、ASA は、次のタイムスタンプ形式を使用する名前でログ ファイルを作成します。

LOG-YYYY-MM-DD-HHMMSS.TXT

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

ステップ 4 別の場所に新しいメッセージを保存するには、次のオプションから 1 つを選択します。

- 内部フラッシュ メモリに新しいメッセージを送信するには、[Flash] チェックボックスをオンにして、[Configure Flash Usage] をクリックします。[Configure Logging Flash Usage] ダイアログボックスが表示されます。
  1. ロギングに使用するフラッシュ メモリの最大容量を KB で指定します。
  2. ロギングをフラッシュ メモリに保持する最小空き領域量を KB で指定します。

3. [OK] をクリックして、このダイアログボックスを閉じます。

- FTP サーバーに新しいメッセージを送信するには、[FTP Server] チェックボックスをオンにし、[Configure FTP Settings] をクリックします。[Configure FTP Settings] ダイアログボックスが表示されます。

  1. [Enable FTP Client] チェックボックスをオンにします。
  2. 表示されたフィールドに、FTP サーバー IP アドレス、パス、ユーザー名、パスワードを入力します。
  3. パスワードを確認し、[OK] をクリックしてこのダイアログボックスを閉じます。

内部ログ バッファのフラッシュへの保存

内部ログ バッファをフラッシュ メモリに保存するには、次の手順を実行します。

手順

ステップ 1 **[File]** > **[Save Internal Log Buffer to Flash]** の順に選択します。

[Enter Log File Name] ダイアログボックスが表示されます。

ステップ 2 最初のオプションを選択し、LOG-YYYY-MM-DD-hhmmss.txt 形式のデフォルト ファイル名でログ バッファを保存します。

ステップ 3 2 番目のオプションを選択し、そのログ バッファのファイル名を指定します。

ステップ 4 ログ バッファのファイル名を入力して [OK] をクリックします。

ログの記録で使用可能な内部フラッシュ メモリの容量の変更

ログの記録で使用可能な内部フラッシュ メモリの容量を変更するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** を選択します。

ステップ 2 [Enable Logging] チェックボックスをオンにします。

ステップ 3 [Logging to Internal Buffer] 領域の [Save Buffer to Flash] チェックボックスをオンにします。

ステップ 4 [Configure Flash Usage] をクリックします。

[Configure Logging Flash Usage] ダイアログボックスが表示されます。

ステップ 5 ログインに使用できるフラッシュ メモリの最大容量を KB で入力します。

デフォルトでは、ASAは、内部フラッシュメモリの最大1MBをログデータに使用できます。ASA でログデータを保存するために必要な内部フラッシュメモリの最小空き容量は 3 MB です。内部フラッシュメモリに保存されているログファイルにより、内部フラッシュメモリの空き容量が設定された最小限の容量を下回ってしまう場合、ASAは最も古いログファイルを削除し、新しいログファイルの保存後も最小限の容量が確保されるようにします。削除するファイルがない場合、または古いファイルをすべて削除しても空きメモリの容量が最小限の容量を下回っている場合、ASA はその新しいログファイルを保存できません。

ステップ 6 フラッシュ メモリにロギングするために維持する空き領域の最小容量を KB で入力します。

ステップ 7 [OK] をクリックして、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

ASDM Java Console による記録されたエントリの参照とコピー

ASDM Java コンソールを使用して、ASDM エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。

ASDM Java Console にアクセスするには、次の手順を実行します。

手順

ステップ 1 **[Tools]** > **[ASDM Java Console]** の順に選択します。

ステップ 2 コンソールで **m** と入力して、仮想マシンのメモリ統計情報を表示します。

ステップ 3 コンソールで **g** と入力して、ガベージ コレクションを実行します。

ステップ 4 Windows タスク マネージャを開き、**asdm_launcher.exe** ファイルをダブルクリックして、メモリ使用量を監視します。

（注） メモリ割り当ての最大値は 256 MB です。

電子メール アドレスへの syslog メッセージの送信

syslog メッセージを電子メール アドレスに送信するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[E-mail Setup]** を選択します。

ステップ 2 電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メール アドレスを指定します。

ステップ 3 [追加（Add）] をクリックして、指定した syslog メッセージの受信者の新しい電子メール アドレスを入力します。

ステップ 4 その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウンリストから選択します。宛先の電子メール アドレスに対して適用される syslog メッセージの重大度フィルタに

より、指定された重大度レベル以上のメッセージが送信されます。[Logging Filters] ペインで指定されたグローバル フィルタも、各電子メール受信者に適用されます。

ステップ 5 [Edit] をクリックして、この受信者へ送信する syslog メッセージの現在の重大度を変更します。

ステップ 6 [OK] をクリックして、[Add E-mail Recipient] ダイアログボックスを閉じます。

電子メール受信者の追加または編集

電子メールの受信者および重大度を追加または編集するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[E-mail Setup]** を選択します。

ステップ 2 [Add] または [Edit] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを表示します。

ステップ 3 宛先の電子メール アドレスを入力し、ドロップダウン リストから syslog 重大度を選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）

  （注） 重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

（注） 宛先電子メール アドレスへのメッセージをフィルタリングする場合は、[Add/Edit E-Mail Recipient] ダイアログボックスで指定した重大度と、[Logging Filters] ペインですべての電子メール受信者に対して設定したグローバル フィルタの重大度のうち、上位にある方が使用されます。

ステップ 4 [OK] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを閉じます。

追加または修正されたエントリが [E-mail Recipients] ペインに表示されます。

ステップ 5 [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

リモート SMTP サーバーの設定

特定のイベントに対する電子メール アラートおよび通知の送信先となるリモート SMTP サーバーを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Logging]** > **[SMTP]** の順に選択します。

ステップ 2 プライマリ SMTP サーバーの IP アドレスを入力します。

ステップ 3 （任意）スタンバイ SMTP サーバーの IP アドレスを入力し、[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

コンソール ポートへの syslog メッセージの送信

syslog メッセージをコンソール ポートに送信するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- **[Home]** > **[Latest ASDM Syslog Messages]** > **[Configure ASDM Syslog Filters]**
- **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Filters]**

ステップ 2 [Logging Destination] カラムでコンソールを選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3 すべてのイベント クラスまたは特定のイベント クラスのいずれかから syslog を選択して、コンソール ポートに送信する syslog メッセージを指定します。

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- **[Home]** > **[Latest ASDM Syslog Messages]** > **[Configure ASDM Syslog Filters]**
- **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Filters]**

ステップ 2 [Logging Destination] カラムの [Telnet and SSH Sessions] を選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3 すべてのイベント クラスまたは特定のイベント クラスのいずれかから syslog を選択して、Telnet または SSH セッションに送信する syslog メッセージを指定します。

ステップ 4 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** の順に選択して、現在のセッションのロギングだけをイネーブルにします。

ステップ 5 [Enable logging] チェックボックスをオンにし、[Apply] をクリックします。

syslog メッセージの設定

syslog メッセージの設定

syslog メッセージを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Setup]** の順に選択します。

ステップ 2 ファイル メッセージのベースとして使用する syslog サーバーのシステム ログ機能を選択します。デフォルトは LOCAL(4)20 です。これは、ほとんどの UNIX システムで必要となるコードです。ただし、ネットワーク デバイス間では 8 つのファシリティが共用されているため、システム ログではこの値を変更しなければならない場合があります。

ステップ 3 [Include timestamp in syslogs] チェックボックスをオンにして、送信される各 syslog メッセージに日付と時刻を追加します。

[Timestamp Format] ドロップダウンを使用して、レガシー（mm: dd: yyyy hh: mm: ss）または RFC 5424（yyyy: Dd: mmTHH: Mm: ssz）形式を選択します。

ステップ 4 ログイン試行が失敗した場合に無効なユーザー名を syslog メッセージに表示する場合は、[Hide username if its validity cannot be determined] チェックボックスをオフにします。デフォルト設定では、ユーザー名が無効な場合、または有効かどうか不明な場合、ユーザー名は非表示です。たとえば、ユーザーが誤ってユーザー名の代わりにパスワードを入力した場合、結果として生成される syslog メッセージで「ユーザー名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザー名を表示することもできます。

ステップ 5 [Syslog ID] テーブルに表示する情報を選択します。使用可能なオプションは、次のとおりです。

- [Syslog ID] テーブルにすべての syslog メッセージ ID を表示するように指定するには、[Show all syslog IDs] を選択します。
- [Syslog ID] テーブルに明示的にディセーブルにした syslog メッセージ ID だけを表示するように指定するには、[Show disabled syslog IDs] を選択します。
- [Syslog ID] テーブルにデフォルト値から変更された重大度を含む syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs with changed logging] を選択します。

- [Syslog ID] テーブルに重大度が変更された syslog メッセージ ID と、明示的にディセーブルにされた syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs that are disabled or with a changed logging level] を選択します。

ステップ 6 [Syslog ID Setup] テーブルには、その設定内容に基づいて、syslog メッセージのリストが表示されます。変更する個々のメッセージ ID またはメッセージ ID の範囲を選択します。選択したメッセージ ID は、ディセーブルにすることも、その重大度レベルを変更することもできます。リストから複数のメッセージ ID を選択する場合は、その範囲の先頭にあたる ID を選択し、Shift キーを押しながらその範囲の最後にあたる ID をクリックします。

ステップ 7 syslog メッセージにデバイス ID が含まれるよう設定する場合は、[Advanced] をクリックします。

syslog ID 設定の編集

syslog メッセージの設定を変更するには、次の手順を実行します。

（注） [Syslog ID(s)] フィールドは表示専用です。この領域に表示される値は、[Syslog Setup] ペインにある [Syslog ID] テーブルで選択されたエントリにより決まります。

手順

ステップ 1 [Disable Message(s)] チェックボックスをオンにして、[Syslog ID(s)] リストに ID が表示されている syslog メッセージをディセーブルにします。

ステップ 2 [Syslog ID(s)] リストに表示される syslog メッセージ ID に送信するメッセージの重大度のロギング レベルを選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）

  （注） 重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3 [OK] をクリックして [Edit Syslog ID Settings] ダイアログボックスを閉じます。

非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

ステップ 1 [Enable syslog device ID] チェックボックスをオンにして、非 EMBLEM 形式の syslog メッセージすべてにデバイス ID が含まれるように指定します。

ステップ 2 次のいずれかのオプションを選択して、どのようなデバイス ID を使用するかを指定します。

- ASA のホスト名
- インターフェイス IP アドレス

  選択した IP アドレスに対応するインターフェイス名を、ドロップダウン リストから選択します。

  クラスタリングを使用する場合は、[In an ASA cluster, always use control's IP address for the selected interface] チェックボックスをオンにします。
- 文字列

  英数字のユーザー定義文字列を入力します。
- ASA クラスタ名

ステップ 3 [OK] をクリックして、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

syslog メッセージに日付と時刻を含める

syslog メッセージに日付と時刻を含めるには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Setup]** の順に選択します。

ステップ 2 [Syslog ID Setup] 領域で [Include timestamp in syslogs] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックして変更内容を保存します。

syslog メッセージの無効化

指定した syslog メッセージをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Setup]** の順に選択します。

ステップ 2 テーブルからディセーブルにする syslog を選択して、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3 [Disable messages] チェックボックスをオンにし、[OK] をクリックします。

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Setup]** の順に選択します。

ステップ 2 重大度を変更する syslog をテーブルから選択して、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3 適切な重大度を [Logging Level] ドロップダウン リストから選択し、[OK] をクリックします。

スタンバイ装置の syslog メッセージのブロック

スタンバイ装置で特定の syslog メッセージが生成されないようにするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Settings]** の順に選択します。

ステップ 2 テーブルの syslog ID を選択し、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3 スタンバイ装置で syslog メッセージが生成されないようにするには、[Disable messages on standby unit] チェックボックスをオンにします。

ステップ 4 [OK] をクリックして、このダイアログボックスを閉じます。

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Setup]** > **[Advanced]** > **[Advanced Syslog Configuration]** の順に選択します。

ステップ 2 [Enable syslog device ID] チェックボックスをオンにします。

ステップ 3 [Device ID] 領域で、[Hostname]、[Interface IP Address] または [String] オプション ボタンをクリックします。

- [Interface IP Address] オプションを選択した場合は、ドロップダウン リストで正しいインターフェイスが選択されていることを確認します。
- [String] オプションを選択した場合は、[User-Defined ID] フィールドにデバイス ID を入力します。文字列の長さは、最大で 16 文字です。

（注） イネーブルにすると、EMBLEM 形式の syslog メッセージや SNMP トラップにデバイス ID は表示されません。

ステップ 4 [OK] をクリックして、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

カスタム イベント リストの作成

イベント リストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（SNMP サーバーなど）に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Event Lists]** の順に選択します。

ステップ 2 [Add] をクリックして、[Add Event List] ダイアログボックスを表示します。

ステップ 3 イベント リストの名前を入力します。スペースは使用できません。

ステップ 4 [Add] をクリックして、[Add Class and SeverityFilter] ダイアログボックスを表示します。

ステップ 5 ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 6 ドロップダウン リストから重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

（注） 重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 7 [OK] をクリックして、[Add Event List] ダイアログボックスを閉じます。

ステップ 8 [Add] をクリックして、[Add Syslog Message ID Filter] ダイアログボックスを表示します。

ステップ 9 フィルタに含める syslog メッセージ ID または syslog メッセージ ID の範囲（101001 ～ 199012 など）を入力します。

ステップ 10 [OK] をクリックして、[Add Event List] ダイアログボックスを閉じます。

目的のイベントがリストに表示されます。

ロギング フィルタの設定

ロギングの宛先へのメッセージ フィルタの適用

ロギングの宛先にメッセージ フィルタを適用するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Filters]** を選択します。

ステップ 2 フィルタを適用するロギングの宛先の名前を選択します。選択できるロギングの宛先は次のとおりです。

- ASDM
- コンソール ポート
- 電子メール
- 内部バッファ
- SNMP サーバー
- Syslog サーバー

- Telnet または SSH セッション

このほか、2 番目のカラム [Syslogs From All Event Classes] と 3 番目のカラム [Syslogs From Specific Event Classes] でも選択操作を行います。2 番目のカラムでは、ロギングの宛先へのメッセージをフィルタリングする場合に使用する重大度やイベントクラスが表示されるほか、すべてのイベントクラスに対してロギングをディセーブルにするかを選択することもできます。3 番目のカラムには、選択したロギングの宛先へのメッセージをフィルタリングする場合に使用するイベント クラスが表示されます。

ステップ 3 [Edit] をクリックして、[Edit Logging Filters] ダイアログボックスを表示します。フィルタを適用、編集、またはディセーブルにする手順については、ロギング フィルタの適用 （1295 ページ）を参照してください。

ロギング フィルタの適用

フィルタを適用するには、次の手順を実行します。

手順

ステップ 1 重大度レベルに基づいて syslog メッセージのフィルタリングを行う場合は、[Filter on severity] オプションを選択します。

ステップ 2 イベント リストに基づいて syslog メッセージのフィルタリングを行う場合は、[Use event list] オプションを選択します。

ステップ 3 選択した宛先に対するロギングをすべてディセーブルにする場合は、[Disable logging from all event classes] オプションを選択します。

ステップ 4 [New] をクリックして、新しいイベント リストを追加します。イベント リストを新たに追加する手順については、カスタム イベント リストの作成 （1293 ページ）を参照してください。

ステップ 5 ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 6 ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

  （注） 重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）

- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 7 [Add] をクリックして、イベント クラスおよび重大度レベルを追加し、[OK] をクリックします。

ダイアログボックスの上部には、フィルタに対して選択したロギングの宛先が表示されます。

syslog メッセージ ID フィルタの追加または編集

syslog メッセージ ID フィルタを作成または編集する手順については、syslog ID 設定の編集（1290 ページ）を参照してください。

メッセージ クラスと重大度フィルタの追加または編集

メッセージのフィルタリングに使用するメッセージクラスおよび重大度レベルを追加または編集するには、次の手順を実行します。

手順

ステップ 1 ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 2 ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

  （注） 重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3 選択が終了したら、[OK] をクリックします。

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべてのsyslogメッセージを指定した出力先に送信するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Filters]** を選択します。

ステップ 2 指定した出力先の設定をオーバーライドするには、変更する出力先を選択してから [Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3 [Syslogs from All Event Classes] または [Syslogs from Specific Event Classes] 領域のいずれかで設定を変更し、[OK] をクリックしてこのダイアログボックスを閉じます。

たとえば、重大度 7 のメッセージが内部ログバッファに送信されるように指定し、重大度 3 の haクラスのメッセージが内部ログバッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。

1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに異なるフィルタリング オプションを選択します。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートを制限するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Rate Limit]** を選択します。

ステップ 2 レート制限を割り当てるロギング レベル（メッセージの重大度）を選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）
- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）

- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3 送信されるメッセージの数が [No of Messages] フィールドに表示されます。また、選択したロギング レベルで送信できるメッセージ数を制限する際の基準となる時間間隔（秒単位）が [Interval (Seconds)] フィールドに表示されます。テーブルからロギング レベルを選択し、[Edit] をクリックして [Edit Rate Limit for Syslog Logging Level] ダイアログボックスを表示します。

ステップ 4 以降の手順については、個々の syslog メッセージに対するレート制限の割り当てまたは変更（1298 ページ）を参照してください。

個々の syslog メッセージに対するレート制限の割り当てまたは変更

個々のsyslogメッセージにレート制限を割り当てる、またはメッセージごとにレート制限を変更するには、次の手順を実行します。

手順

ステップ 1 特定の syslog メッセージにレート制限を割り当てる場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 2 以降の手順については、syslogメッセージに対するレート制限の追加または編集（1298ページ）を参照してください。

ステップ 3 特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 4 以降の手順については、syslog重大度に対するレート制限の編集（1299ページ）を参照してください。

syslog メッセージに対するレート制限の追加または編集

特定のsyslogメッセージに対するレート制限を追加または変更するには、次の手順を実行します。

手順

ステップ 1 特定の syslog メッセージに対するレート制限を追加する場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 2 レートを制限する syslog メッセージの ID を入力します。

ステップ 3 指定した時間内に送信できるメッセージの最大数を入力します。

ステップ 4 指定したメッセージのレートを制限する際の基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

（注） メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

syslog 重大度に対するレート制限の編集

指定した syslog 重大度のレート制限を変更するには、次の手順を実行します。

手順

ステップ 1 指定した重大度で送信可能なメッセージの最大数を指定します。

ステップ 2 指定した重大度のメッセージに対するレートを制限する基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

選択したメッセージ重大度が表示されます。

（注） メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

ログのモニターリング

ロギング ステータスの監視については、次のコマンドを参照してください。

- **[Monitoring] > [Logging] > [Log Buffer] > [View]**

  このペインでは、ログ バッファを表示できます。

- **[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]**

  このペインでは、リアルタイムのログを表示できます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

ログ ビューアを使用した syslog メッセージのフィルタリング

Real-Time Log Viewer および Log Buffer Viewer の任意のカラムに対応する 1 つ以上の値に基づいて、syslog メッセージをフィルタリングできます。

ログ ビューアのいずれかを使用して syslog メッセージをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- **[Monitoring]** > **[Logging]** > **[Real-Time Log Viewer]** > **[View]**
- **[Monitoring]** > **[Logging]** > **[Log Buffer]** > **[View]**

ステップ 2 [Real-Time Log Viewer] または [Log Buffer Viewer] ダイアログボックスのいずれかで、ツールバーの [Build Filter] をクリックします。

ステップ 3 [Build Filter] ダイアログボックスで、syslog メッセージに適用するフィルタリング基準を指定します。

a) [Date and Time] 領域で、リアルタイム、特定時刻、時間範囲の 3 つのオプションから 1 つを選択します。特定時刻を選択した場合は、数値を入力してドロップダウンリストから時または分を選択し、時刻を指定します。時間範囲を選択した場合、[Start Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。ドロップダウンリストから開始日と開始時刻を選択し、[OK] をクリックします。[End Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。ドロップダウンリストから終了日と終了時刻を選択し、[OK] をクリックします。

b) [Severity] フィールドに有効な重大度を入力します。または、[Severity] フィールドの右側で [Edit] アイコンをクリックします。フィルタリングする重大度をリストでクリックします。重大度 1 ～ 7 を含めるには、[All] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Severity] フィールドの右側にある [Info] アイコンをクリックします。

c) [Syslog ID] フィールドに有効な syslog ID を入力します。または、[Syslog ID] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Syslog ID] フィールドの右側にある [Info] アイコンをクリックします。

d) [Source IP Address] フィールドに有効な送信元 IP アドレスを入力するか、または [Source IP Address] フィールドの右側で [Edit] アイコンをクリックします。単一の IP アドレスまたは IP アドレスの特定の範囲を選択し、[Add] をクリックします。特定の IP アドレスまたは IP アドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにして、[OK] をクリックし、[Build Filter] ダイアログボックスにこれらの設定を表示します。使用する正しい入力形式に関する詳細な情報については、[Source IP Address] フィールドの右側にある [Info] アイコンをクリックします。

e) [Source Port] フィールドに有効な送信元ポートを入力するか、または [Source Port] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Source Port] フィールドの右側にある [Info] アイコンをクリックします。

f) [Destination IP Address] フィールドに有効な宛先 IP アドレスを入力するか、または [Destination IP Address] フィールドの右側で [Edit] アイコンをクリックします。単一の IP アドレスまた

はIPアドレスの特定の範囲を選択し、[Add]をクリックします。特定のIPアドレスまたはIPアドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Destination IP Address] フィールドの右側にある [Info] アイコンをクリックします。

g) [Destination Port] フィールドに有効な宛先ポートを入力するか、または [Destination Port] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式に関する詳細な情報については、[Destination Port] フィールドの右側にある [Info] アイコンをクリックします。

h) [Description] フィールドにフィルタリング テキストを入力します。このテキストには、正規表現を含む、1 つ以上の文字からなる任意の文字列を指定できます。ただし、セミコロンは有効な文字ではありません。また、この設定では大文字と小文字が区別されます。複数のエントリを指定する場合は、カンマで区切ります。

i) [OK] をクリックして、指定したフィルタリング設定をログ ビューアの [Filter By] ドロップダウン リストに追加します。フィルタ文字列は特定の形式に従います。FILTER:プレフィックスは、[Filter By] ドロップダウン リストに表示されるすべてのカスタム フィルタを示します。このフィールドにはランダムなテキストを入力することもできます。

次の表に、使用される形式の例を示します。

Build Filter の例	フィルタ文字列形式
Source IP = 192.168.1.1 または 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 ～ 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
725001 ～ 725003 の範囲外の syslog ID	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

ステップ 4 [Filter By] ドロップダウン リストの設定の 1 つを選択し、ツールバーの [Filter] をクリックして、syslog メッセージをフィルタリングします。この設定は、これ以降のすべての syslog メッセージにも適用されます。すべてのフィルタをクリアするには、ツールバーにある [Show All] をクリックします。

（注） [Build Filter] ダイアログボックスを使用して指定したフィルタは保存できません。これらのフィルタは、そのフィルタが作成された ASDM セッションのみで有効です。

フィルタリング設定の編集

[Build Filter] ダイアログボックスを使用して作成したフィルタリング設定を編集するには、次の手順を実行します。

手順

次のいずれかのオプションを選択します。

- [Filter By] ドロップダウン リストで変更を入力して、フィルタを直接修正します。
- [Filter By] ドロップダウン リストでフィルタを選択し、[Build Filter] をクリックして [Build Filter] ダイアログボックスを表示します。[Clear Filter] をクリックして、現在のフィルタ設定を削除し、新しい値を入力します。それ以外の場合は、表示された設定を変更して [OK] をクリックします。

  （注） これらのフィルタリング設定は、[Build Filter] ダイアログボックスで定義されたフィルタのみに適用されます。

- ツールバーの [Show All] をクリックすると、フィルタリングが停止し、すべての syslog メッセージが表示されます。

ログ ビューアを使用した特定のコマンドの発行

いずれかのログ ビューアを使用して、**ping**、**traceroute**、**whois**、および **dns lookup** コマンドを発行できます。

これらのコマンドのいずれかを実行するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのオプションを選択します。

- **[Monitoring]** > **[Logging]** > **[Real-Time Log Viewer]** > **[View]**
- **[Monitoring]** > **[Logging]** > **[Log Buffer]** > **[View]**

ステップ 2 [Real-Time Log Viewer] または [Log Buffer] ペインから [Tools] をクリックし、実行するコマンドを選択します。または、表示された特定の syslog メッセージを右クリックしてコンテキスト メニューを表示し、実行するコマンドを選択します。

[Entering command] ダイアログボックスが表示され、選択したコマンドが自動的にドロップダウン リストに表示されます。

ステップ 3 選択した syslog メッセージの送信元 IP アドレスまたは宛先 IP アドレスのいずれかを [Address] フィールドに入力し、[Go] をクリックします。

指定した領域にコマンド出力が表示されます。

ステップ 4 [Clear] をクリックして出力を削除し、実行する別のコマンドをドロップダウン リストから選択します。必要に応じてステップ 3 を繰り返します。完了したら [Close] をクリックします。

ロギングの履歴

表 *59 :* ロギングの履歴

機能名	プラットフォームリリース	説明
Logging	7.0(1)	さまざまな出力先を経由して ASA ネットワーク ロギング情報を提供します。ログ ファイルを表示して保存するオプションも含まれています。 次の画面が導入されました。[Configuration] > [Device Management] > [Logging] > [Logging Setup]。
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Rate Limit]。
ロギング リスト	7.2(1)	さまざまな基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために他のコマンドで使用されるロギング リストを作成します。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Event Lists]。

機能名	プラットフォームリリース	説明
セキュア ロギング	8.0(2)	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Syslog Server]。
ロギング クラス	8.0(4)、8.1(1)	ロギング メッセージの ipaa イベント クラスに対するサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Filters]。
ロギング クラスと保存されたロギング バッファ	8.2(1)	ロギング メッセージの dap イベント クラスに対するサポートが追加されました。 保存されたロギング バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアする追加サポート。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Setup]。
パスワードの暗号化	8.3(1)	パスワードの暗号化に対するサポートが追加されました。
ログ ビューア	8.3(1)	送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。

機能名	プラットフォームリリース	説明
拡張ロギングと接続ブロック	8.3(2)	TCP を使用するように syslog サーバーを設定すると、syslog サーバーを使用できない場合、ASA はサーバーが再び使用可能になるまで syslog メッセージを生成する新しい接続をブロックします（たとえば、VPN、ファイアウォール、カットスループロキシ接続）。この機能は、ASA のロギング キューがいっぱいのときにも新しい接続をブロックするように拡張されました。接続は、ロギング キューがクリアされると再開されます。 この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも接続を許可することを推奨します。接続を許可するには、[Configuration] > [Device Management] > [Logging] > [Syslog Servers] ペインで [Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにします。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。 変更された ASDM 画面はありません。

機能名	プラットフォームリリース	説明
syslog メッセージのフィルタリングとソート	8.4(1)	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージ フィルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、『ASDM 構成ガイド』を参照してください。 この機能は、すべての ASA バージョンと相互運用性があります。 次の画面が変更されました。 [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]。 [Monitoring] > [Logging] > [Log Buffer Viewer] > [View]。
クラスタ	9.0(1)	ASA 5580 および 5585-X のクラスタリング環境での syslog メッセージ生成のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration]。
スタンバイ装置の syslog のブロック	9.4(1)	フェールオーバー コンフィギュレーションのスタンバイ装置で特定の syslog メッセージの生成をブロックするためのサポートを追加しました。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Syslog Setup]。

機能名	プラットフォームリリース	説明
syslog サーバーのセキュアな接続のための参照 ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 検証は、syslog サーバーサーバーへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のページが変更されました。[ASDM Configuration] > [Remote Access VPN] > [Advanced] および [Configuration] > [Device Management] > [Logging] > [Syslog Servers -> Add or Edit]
syslog サーバーでの IPv6 アドレスのサポート	9.7(1)	TCP と UDP 経由で syslog を記録、送信、受信するために、syslog サーバーを IPv6 アドレスで設定できるようになりました。 次の画面が変更されました。**[Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add Syslog Server]**

第 47 章

SNMP

この章では、Simple Network Management Protocol（SNMP）に Cisco ASA をモニターさせるための設定方法について説明します。

SNMP の概要

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコル スイートの一部です。Secure Firewall ASAは SNMP バージョン 1、2c、および3を使用したネットワーク監視に対するサポートを提供し、3つのバージョンの同時使用をサポートします。ASA のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワーク デバイスをモニターできます。ASAは GET 要求の発行を通じて SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように ASA を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIBは定義の集合であり、ASAは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

ASA には SNMP エージェントが含まれています。このエージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。ASA エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *60 : SNMP* の用語

用語	説明
エージェント	ASAで稼働する SNMP サーバー。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニターすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIBは、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMPイベントのモニターやASAなどのデバイスの管理用に設定されている、PCまたはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニターおよび表示される情報の源をユーザーに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバーと SNMP エージェント間でデータをクリアテキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザーベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスを

コントロールします。ASA は、SNMP グループとユーザーの作成、およびセキュアな SNMP 通信の転送の認証と暗号化を有効にするために必要なホストの作成もサポートします。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティ モデルにまとめられます。セキュリティ モデルはユーザーとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuthPriv：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- AuthNoPriv：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- AuthPriv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザーは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザー

SNMPユーザーは、指定されたユーザー名、ユーザーが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5、SHA-1、および SHA-256 HMAC です。暗号化アルゴリズムのオプションは DES、3DES、および AES（128、192、および 256 バージョンで使用可能）です。ユーザーを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザーはグループのセキュリティ モデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザーだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザー名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA で一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザー クレデンシャルが ASA のクレデンシャルと一致するように設定してください。

ASA と Cisco IOS ソフトウェアの実装の相違点

ASA での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装とは次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカルエンジン ID は、ASA が起動されたとき、またはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザーとグループを作成する必要があります。
- 正しい順序でユーザー、グループ、およびホストを削除する必要があります。
- snmp-server host コマンドを使用すると、着信 SNMP トラフィックを許可する ASA ルールが作成されます。

SNMP syslog メッセージ

SNMP では、212*nnn* という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、ASA または ASASM から、SNMP 要求、SNMP トラップ、SNMP チャネルのステータスを、指定のインターフェイスの指定のホストに表示します。

syslog メッセージの詳細については、syslog メッセージガイドを参照してください。

（注） SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

この項では、SNMP を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバーとクラスタリングのガイドライン

- クラスタリングまたはフェールオーバーで SNMPv3 を使用する場合、最初のクラスタ形成後に新しいクラスタユニットを追加するか、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットに複製されません。ユーザを新しいユニットに強制的に複製するには、SNMPv3 ユーザを制御またはアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます（SNMPv3 ユーザおよびグループは、クラスタデータユニットで設定コマンドを入力できないというルールの例外です）。制御ユニットまたはアクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してデータユニットまたはスタンバイユニットに直接入力することにより、各ユーザを再設定します。

IPv6 ガイドライン（すべての ASA モデル）

SNMP を IPv6 転送上で設定できるため、IPv6 ホストは SNMP クエリを実行でき、IPv6 ソフトウェアを実行するデバイスから SNMP 通知を受信できます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。

（注） ユーザリストの 1 人のユーザまたはユーザグループをネットワークオブジェクトに関連付けるためのコマンド **snmp-server host-group** は、IPv6 をサポートしていません。

Firepower 2100 の IPv6 ガイドライン

Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティングシステムを実行し、アプライアンスモード（デフォルト）とプラットフォームモードの両方をサポートします。アプライアンスまたはプラットフォーム モードへの Firepower 2100 の設定 （52 ページ）を参照してください。

プラットフォームモードでは、FXOS で IPv6 管理 IP アドレスを設定する必要があります。次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
```

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

その他のガイドライン

- アプライアンスモードで動作しているシステムでは、電源トラップは発行されません。
- プラットフォームモードの Firepower 2100 では、EtherChannel のメンバーインターフェイスをポーリングできず、メンバーインターフェイスのトラップは生成されません。この機能は、FXOS で直接 SNMP を有効にした場合にサポートされます。アプライアンスモードは影響を受けません。
- プラットフォームモードの Firepower 2100 では、個々のポートメンバーの ASA トラップはサポートされません。『Cisco Firepower 2100 FXOS MIB Reference Guide』を参照してください。
- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。
- サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。次に、外部インターフェイスをポーリングして、SNMP が設定されている内部インターフェイスから情報を取得します。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。
- ENTITY-MIB は Firepower 9300 では使用できません。代わりに、CISCO-FIREPOWER-EQUIPMENT-MIB および CISCO-FIREPOWER-SM-MIB を使用します。
- 一部のデバイスでは、**snmpwalk** の出力に表示されるインターフェイスの順序（ifDescr）が再起動後に変わることが確認されています。ASA では、アルゴリズムを使用して SNMP が照会する ifIndex テーブルを決定します。ASA の起動時、ASA による設定の読み取りでロードされる順序でインターフェイスが ifIndex テーブルに追加されます。ASA に新しいインターフェイスが追加されると、ifIndex テーブルのインターフェイスのリストに追加されていきます。インターフェイスの追加、削除、または名前変更により、再起動時にインターフェイスの順序が変わることがあります。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。

- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。
- 結果として SNMP 機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザー、ホストの順に行う必要があります。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザーが削除されていることを確認する必要があります。
- ユーザーを削除する前に、そのユーザー名に関連付けられているホストが設定されていないことを確認する必要があります。
- 特定のセキュリティ モデルを使用して特定のグループに属するようにユーザーが設定されている場合にそのグループのセキュリティ レベルを変更する場合は、次の順に操作を実行する必要があります。
  - そのグループからユーザを削除します。
  - グループのセキュリティ レベルを変更します。
  - 新しいグループに属するユーザーを追加します。
- MIB オブジェクトのサブセットへのユーザー アクセスを制限するためのカスタム ビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- connection-limit-reached トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザー コンテキストで設定された SNMP サーバー ホストが少なくとも 1 つ必要です。
- NMS が正常にオブジェクトを要求できない場合、または ASA からの着信トラップを適切に処理していない場合は、パケット キャプチャの実行が問題を判別する最も有効な方法となります。[Wizards] > [Packet Capture Wizard] を選択して、画面に表示される指示に従います。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザーを関連付けることができます。
- ネットワーク オブジェクトは、別の **host-group** コマンドと重複して指定することができます。異なるネットワーク オブジェクトの共通のホストに対しては、最後のホスト グループに指定した値が適用されます。

- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホスト グループで指定されている値を使用してホストが再設定されます。
- ホストで取得される値は、コマンドの実行に使用するように指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- ASA では、コンテキストごとに SNMP サーバーのトラップ ホスト数の制限がありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。

SNMP の設定

ここでは、SNMP の設定方法について説明します。

手順

ステップ 1 ASA から要求を受信するように SNMP 管理ステーションを設定します。

ステップ 2 SNMP トラップを設定します。

ステップ 3 SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。

SNMP 管理ステーションの設定

SNMP 管理ステーションを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。デフォルトでは、SNMP サーバーはイネーブルになっています。

ステップ 2 [SNMP Management Stations] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 3 SNMP ホストが存在するインターフェイスを選択します。

ステップ 4 SNMP ホストの IP アドレスを入力します。

ステップ 5 SNMP ホストの UDP ポートを入力します。デフォルトのポート 162 をそのまま使用することもできます。

ステップ 6 SNMP ホストのコミュニティ ストリングを追加します。管理ステーションに対してコミュニティ ストリングが指定されていない場合は、[SNMP Management Stations] ペインの [Community String (default)] フィールドに設定されている値が使用されます。

ステップ 7 SNMP ホストで使用される SNMP のバージョンを選択します。

ステップ 8 前の手順で SNMP バージョン 3 を選択した場合は、設定済みユーザーの名前を選択します。

ステップ 9 [Poll] チェックボックスまたは [Trap] チェックボックスのいずれかをオンにして、NMS との通信に使用する方式を指定します。

ステップ 10 [OK] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

NMS が設定され、その変更内容が実行コンフィギュレーションに保存されます。SNMP バージョン 3 の NMS ツールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

SNMP トラップの設定

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [Configure Traps] をクリックします。

[SNMP Trap Configuration] ダイアログボックスが表示されます。

ステップ 3 [SNMPサーバトラップ構成（SNMP Server Traps Configuration）] チェックボックスをオンにします。

デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。トラップ タイプを指定しない場合、デフォルトで **syslog** トラップに設定されます。デフォルトの SNMP トラップは、**syslog** トラップとともにイネーブルの状態を続けます。デフォルトでは他のトラップはすべてディセーブルです。トラップをディセーブルにするには、該当するチェックボックスをオフにします。

トラップは、次のカテゴリに分類されます。

a) [標準SNMPトラップ（Standard SNMP Traps）]、該当するものをすべてチェックします。

[クリティカルCPU温度（Critical CPU temperature）]、[シャーシ温度（Chassis temperature）]、[アクセラレータCPU温度（Accelerator CPU temperature）]、および[シャーシファンの障害（Chassis Fan Failure）] から選択します。

（注）　デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。

b) [環境トラップ（Environment Traps）]、該当するものをすべてチェックします。

[認証（Authentication）]、[リンクアップ（Link up）]、[リンクダウン（Link down）]、[コールドスタート（Cold start）]、および [ウォームスタート（Warm start）] から選択します。

c) [Ikev2トラップ（Ikev2 Traps）]、該当するものをすべてチェックします。

[開始（Start）] および [停止（Stop）] から選択します。

d) [エンティティMIB通知（Entity MIB Notifications）]。

現場交換可能ユニットに関する通知を受信するには、この項目をオンにします。

e) [IPSecトラップ（IPSec Traps）]、該当するものをすべてチェックします。

[開始（Start）] および [停止（Stop）] から選択します。

f) [リモートアクセストラップ（Remote Access Traps）]。

確立されたセッション数が設定されたしきい値を超えたときに通知を受信するには、この項目をオンにします。

g) [リソーストラップ（Resource Traps）]、該当するものをすべてチェックします。

[接続制限に達しました（Connection limit reached）]、[メモリのしきい値に達しました（Memory threshold reached）]、および [インターフェイスのしきい値に達しました（Interface threshold reached）] から選択します。

h) [NATトラップ（NAT Traps）]。

マッピングスペースが使用できないために IP パケットが NAT によって破棄されたときに通知を受信するには、この項目をオンにします。

i) [Syslog]。

確立されたセッション数が設定されたしきい値を超えたときに通知を受信するには、[syslogトラップを有効にする（Enable syslog traps）] をオンにします。

syslog トラップの重大度レベルを設定するには、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [ロギングフィルタ（Logging Filters）]** の順に選択します

j) [CPU使用率トラップ（CPU Utilization Traps）]。

CPU 使用率が、設定された [モニタリング間隔（Monitoring interval）] に対して設定された [CPU使用率しきい値（CPU Utilization threshold）] を超えた場合に通知を受信するには、[CPU上昇しきい値に達しました（CPU rising threshold reached）] をオンにします。

k) [SNMPインターフェイスしきい値（SNMP interface threshold）]。

インターフェイスの帯域幅使用率が、設定された [SNMPインターフェイスしきい値（SNMP interface threshold）] を超えた場合に通知を受信するには、[しきい値と間隔の設定（Configure threshold and interval）] をオンにします。

有効なしきい値の範囲は 30～99 % です。デフォルト値は 70 % です。

l) [SNMPメモリしきい値（SNMP Memory threshold）]。

CPU 使用率が、[SNMPメモリしきい値（SNMP memory threshold）] に設定されたしきい値を超えた場合に通知を受信するには、[メモリしきい値の設定（Configure memory threshold）] をオンにします。

使用されたシステムコンテキストのメモリが総システムメモリの80%に達すると、メモリしきい値トラップが管理コンテキストから生成されます。他のすべてのユーザーコンテキストでは、このトラップは使用メモリが特定のコンテキストの総システム メモリの 80 % に到達した場合に生成されます。

m) [フェールオーバートラップ（Failover Traps）]。

フェールオーバーの SNMP syslog トラップを受信するには、[フェールオーバー関連のトラップを有効にする（Enable Failover related traps）] をオンにします。

n) [クラスタトラップ（Cluster Traps）]。

クラスタメンバーの SNMP syslog トラップを受信するには、[クラスタ関連のトラップを有効にする（Enable cluster related traps）] をオンにします。

o) [ピアフラップトラップ（Peer-Flap Traps）]。

クラスタピア MAC アドレスフラッピングの SNMP syslog トラップを受信するには、[bgp/ospfピアフラップ関連のトラップを有効にする（Enable bgp/ospf peer-flap related traps）] をオンにします。

ステップ 4 [OK] をクリックして、[SNMP Trap Configuration] ダイアログボックスを閉じます。

ステップ 5 [Apply] をクリックします。

SNMP トラップが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 SNMP バージョン 1 または 2c を使用する場合は、[Community String (default)] フィールドにデフォルトのコミュニティ ストリングを入力します。要求を ASA に送信するときに SNMP NMS

で使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP NMS と管理対象のネットワーク ノード間の共有秘密です。ASA では、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは、大文字と小文字が区別される、最大 32 文字の英数字です。スペースは使用できません。デフォルトは public です。SNMP バージョン 2c では、NMS ごとに、別々のコミュニティ ストリングを設定できます。コミュニティ ストリングがどの NMS にも設定されていない場合、ここで設定した値がデフォルトとして使用されます。

（注） コミュニティストリングでは特殊文字（!、@、#、$、%、^、&、*、\）を使用しないでください。一般に、オペレーティングシステムで使用される関数用に予約されている特殊文字を使用すると、予期しない結果が生じる可能性があります。たとえば、バックスラッシュ（\）はエスケープ文字と解釈されるため、コミュニティストリングでは使用できません。

ステップ 3 ASA システム管理者の名前を入力します。テキストは、大文字と小文字が区別される、最大 127 文字の英数字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 4 SNMP で管理している ASA の場所を入力します。テキストは、大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 5 NMS からの SNMP 要求をリッスンする ASA ポートの番号を入力します。デフォルトのポート番号 161 をそのまま使用することもできます。

ステップ 6 （オプション）[Enable Global-Shared pool in the walk] チェックボックスをオンにして、SNMP ウォーク操作によって空きメモリと使用済みメモリの統計情報を照会します。

重要 ASA がメモリ情報を照会すると、CPU は他のプロセスに開放される前に SNMP プロセスによって長時間にわたり保持されることがあります。これにより、SNMP 関連の CPU ホグ状態になり、パケットがドロップされることがあります。

ステップ 7 [SNMP Host Access List] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 8 トラップの送信元となるインターフェイスの名前をドロップダウン リストから選択します。

ステップ 9 ASA に接続できる NMS または SNMP マネージャの IP アドレスを入力します。

ステップ 10 UDP のポート番号を入力します。デフォルトは 162 です。

ステップ 11 使用する SNMP のバージョンをドロップダウン リストから選択します。バージョン 1 または 2c を選択した場合は、コミュニティ ストリングを入力する必要があります。バージョン 3 を選択した場合は、ドロップダウン リストからユーザー名を選択する必要があります。

バージョンは、トラップと要求（ポーリング）に使用される SNMP のバージョンを指定します。サーバとの通信は、選択したバージョンのみを使用して許可されます。

ステップ 12 要求の送信（ポーリング）だけに NMS を制限する場合は、[Server Poll/Trap Specification] 領域の [Poll] チェックボックスをオンにします。トラップの受信だけに NMS を制限する場合は、

[Trap] チェックボックスをオンにします。両方のチェックボックスをオンにすると、SNMP ホストの両方の機能が実行されます。

ステップ 13 [OK] をクリックして、[Add SNMP Host Access Entry] ダイアログボックスを閉じます。

新しいホストが [SNMP Host Access List] ペインに表示されます。

ステップ 14 **Apply** をクリックします。

SNMP バージョン 1、2c、または 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで **[Add]** > **[SNMP User]** の順にクリックして、設定済みのユーザーまたは新規ユーザーをグループに追加します。グループ内に残る最後のユーザーを削除すると、そのグループは ASDM により削除されます。

（注） ユーザーが作成された後は、そのユーザーが属するグループは変更できません。

[Add SNMP User Entry] ダイアログボックスが表示されます。

ステップ 3 SNMP ユーザーが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザーには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザーには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザーには、認証も暗号化も設定されません。

（注） グループ名は変更できません。

ステップ 4 ユーザー セキュリティ モデル（USM）グループを使用する場合は、[USM Model]]タブをクリックします。

ステップ 5 [Add] をクリックします。

[Add SNMP USM Entry] ダイアログボックスが表示されます。

ステップ 6 グループ名を入力します。

ステップ 7 ドロップダウン リストからセキュリティ レベルを選択します。設定済みの USM グループをセキュリティ レベルとして SNMPv3 ユーザーに割り当てることができます。

ステップ 8 設定済みユーザーまたは新規ユーザーの名前を入力します。ユーザー名は、選択した SNMP サーバー グループ内で一意であることが必要です。

ステップ 9 [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 10 [MD5]、[SHA1]、[SHA256] のいずれかのオプションボタンをクリックして、使用する認証のタイプを指定します。

ステップ 11 認証に使用するパスワードを入力します。

ステップ 12 [DES]、[3DES]、[AES] の中からいずれかのオプションボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13 AES 暗号化を選択した場合は、使用する AES 暗号化のレベルとして、128、192、256 のいずれかを選択します。

ステップ 14 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 15 [OK] をクリックすると、グループが作成され（指定したユーザーがそのグループに属する最初のユーザーである場合）、[Group Name] ドロップダウン リストにそのグループが表示されます。またそのグループ内にユーザーが作成されます。

[Add SNMP User Entry] ダイアログボックスが閉じます。

ステップ 16 [Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

ユーザーのグループの設定

指定したユーザーのグループからなる SNMP ユーザー リストを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで **[Add]** > **[SNMP User Group]** の順にクリックし、設定済みのユーザー グループまたは新規ユーザー グループを追加します。グループ内に残る最後のユーザーを削除すると、そのグループは ASDM により削除されます。

[Add SNMP User Group] ダイアログボックスが表示されます。

ステップ 3 ユーザー グループ名を入力します。

ステップ 4 既存のユーザーまたはユーザー グループを選択する場合は、[Existing User/User Group] オプション ボタンをクリックします。

ステップ 5 新規ユーザーを作成する場合は、[Create new user] オプション ボタンをクリックします。

ステップ 6 SNMP ユーザーが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザーには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザーには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザーには、認証も暗号化も設定されません。

ステップ 7 設定済みユーザーまたは新規ユーザーの名前を入力します。ユーザー名は、選択した SNMP サーバー グループ内で一意であることが必要です。

ステップ 8 [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 9 [MD5]、[SHA1]、または [SHA256] のいずれかのオプションボタンをクリックして、使用する認証のタイプを指定します。

ステップ 10 認証に使用するパスワードを入力します。

ステップ 11 認証に使用するパスワードを確認のためにもう一度入力します。

ステップ 12 [DES]、[3DES]、[AES] の中からいずれかのオプションボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 14 暗号化に使用するパスワードを確認のためにもう一度入力します。

ステップ 15 [Members in Group] ペインの指定したユーザー グループに新規ユーザーを追加するには、[Add] をクリックします。[Members in Group] ペインから既存のユーザーを削除するには、[Remove] をクリックします。

ステップ 16 [OK] をクリックすると、指定したユーザー グループに新規ユーザーが作成されます。

[Add SNMP User Group] ダイアログボックスが閉じます。

ステップ 17 [Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP モニターリング

次の SNMP モニターリング用のコマンドを参照してください。**[Tools] > [Command Line Interface]** を使用して次のコマンドを入力できます。

- **show running-config snmp-server** [**default**]

  すべての SNMP サーバーのコンフィギュレーション情報を表示します。

- **show running-config snmp-server group**

  SNMP グループのコンフィギュレーション設定を表示します。

- **show running-config snmp-server host**

リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。

- **show running-config snmp-server host-group**

  SNMP ホスト グループのコンフィギュレーションを表示します。

- **show running-config snmp-server user**

  SNMP ユーザーベースのコンフィギュレーション設定を表示します。

- **show running-config snmp-server user-list**

  SNMP ユーザー リストのコンフィギュレーションを表示します。

- **show snmp-server engineid**

  設定されている SNMP エンジンの ID を表示します。

- **show snmp-server group**

  設定されている SNMP グループの名前を表示します。コミュニティ ストリングがすでに設定されている場合、デフォルトでは2つの別のグループが出力に表示されます。この動作は通常のものです。

- **show snmp-server statistics**

  SNMPサーバーの設定済み特性を表示します。すべてのSNMPカウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

- **show snmp-server user**

  ユーザーの設定済み特性を表示します。

SNMP の履歴

表 *61 : SNMP* の履歴

機能名	バージョン	説明
SNMP バージョン 1 および 2c	7.0(1)	クリアテキストのコミュニティストリングを使用したSNMPサーバーと SNMP エージェント間のデータ送信によって、ASA ネットワークのモニターリングおよびイベント情報を提供します。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。

機能名	バージョン	説明
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザー、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。
SNMP トラップと MIB	8.4(1)	追加のキーワードとして、**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart** をサポートします。 entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。 追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。 さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
IF-MIB ifAlias OID のサポート	8.2(5) / 8.4(2)	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。

機能名	バージョン	説明
ASA サービス モジュール（ASASM）	8.5(1)	ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。 8.5(1) のサポートされていない MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • ENTITY-SENSOR-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • DISMAN-EXPRESSION-MIB（expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます）。 8.5(1) のサポートされていないトラップ： • ceSensorExtThresholdNotification（CISCO-ENTITY-SENSOR-EXT-MIB）。このトラップは、電源障害、ファン障害および高 CPU 温度のイベントだけに使用されます。 • InterfacesBandwidthUtilization。
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure, entity power-supply-temperature** をサポートします。 次のコマンドが変更されました。**snmp-server enable traps**。
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB が有効になりました。 • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。

機能名	バージョン	説明
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、**show xlate count** コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホスト グループ、ユーザー リスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザーを関連付けることができます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。
SNMP の MIB および OID	9.2(1)	ASA は、cpmCPUTotal5minRev OID をサポートするようになりました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASAv が追加されました。 新しい ASAv プラットフォームをサポートするよう、CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 VPN 共有ライセンスの使用状況をモニターするための新しい SNMP MIB が追加されました。
SNMP の MIB および OID	9.3(1)	ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB（OID 1.3.6.1.4.1.9.9.392）のサポートが追加されました。

機能名	バージョン	説明
SNMP の MIB およびトラップ	9.3(2)	ASA 5506-X をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP] > [Configure Traps] > [SNMP Trap Configuration]。
SNMP の MIB およびトラップ	9.4(1)	SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506W-X、ASA 5506H-X、ASA 5508-X、および ASA 5516-X が追加されました。
コンテキストごとに無制限の SNMP サーバー トラップ ホスト	9.4(1)	ASA は、コンテキストごとに無制限の SNMP サーバー トラップ ホストをサポートします。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 変更された ASDM 画面はありません。
ISA 3000 のサポートが追加されました。	9.4(1.225)	ISA 3000 製品ファミリーで SNMP がサポートされました。このプラットフォームに新しい OID が追加されました。**snmp-server enable traps entity** コマンドが変更され、新しい変数 *l1-bypass-status* が追加されました。これにより、ハードウェアのバイパス状態の変更が可能になりました。 変更された ASDM 画面はありません。

機能名	バージョン	説明
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	9.6(1)	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニターリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。
Precision Time Protocol（PTP）の E2E トランスペアレント クロック モード MIB のサポート	9.7(1)	E2E トランスペアレント クロック モードに対応する MIB がサポートされます。 （注） SNMP の bulkget、getnext、walk 機能のみがサポートされています。
SNMP over IPv6	9.9(2)	ASA は、IPv6 経由での SNMP サーバーとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.10(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 変更された ASDM 画面はありません。
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.12(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**

機能名	バージョン	説明
SNMPv3 認証	9.14(1)	ユーザー認証に SHA-256 HMAC を使用できるようになりました。 新規/変更された画面：**[構成（Configuration）]>[デバイス管理（Device Management）] > [管理アクセス（Management Access）] > [SNMP]**
9.14(1) 以降のフェールオーバーペアの場合、ASA は SNMP クライアントエンジンデータをピアと共有しません。	9.14(1)	ASA は、SNMP クライアントのエンジンデータをピアと共有しなくなりました。
サイト間 VPN 経由の SNMP ポーリング	9.14(2)	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。

第 48 章

Cisco Success Network とテレメトリデータ

この章では、Cisco Success Network についてと、Cisco Success Network を ASA で有効にする方法について説明します。また、Security Service Engine（SSE）クラウドに送信されるテレメトリデータポイントも示します。

Cisco Success Network について

Cisco Success Network は、ASA の使用率情報と統計情報をストリーミングする Security Service Exchange（SSE）クラウドとのセキュアな接続を確立するユーザーが有効なクラウドサービスです。テレメトリをストリーミングすることによって、ASA使用率とその他の詳細を構造化形式（JSON）でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- 製品に利用可能な、追加のテクニカルサポートサービスとモニターリングについて通知します。
- シスコ製品の改善に役立ちます。

デフォルトでは、Cisco Success Network は、（ブレードレベルで）ASA デバイスをホストする Firepower 9300/4100 プラットフォームで有効になっています。ただし、テレメトリデータを送信するには、シャーシレベルでFXOS の設定を有効にするか（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』を参照）、シャーシマネージャで Cisco Success Network を有効にする必要があります（『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide』を参照）。

ASAデバイスで収集されるテレメトリデータには、CPU、メモリ、ディスク、または帯域幅、ライセンスの使用状況、設定されている機能リスト、クラスタ/フェールオーバー情報などが含まれます。「Cisco Success Network - テレメトリデータ （1334 ページ）」を参照してください。

サポートされるプラットフォームと必要な設定

- ASA バージョン 9.13.1 以降を実行している FP9300/4100 プラットフォームでサポートされます。
- クラウドに接続するには、FXOS バージョン2.7.1 以降が必要です。
- FXOS の SSE コネクタは、SSE クラウドに接続されている必要があります。この接続は、スマートライセンスバックエンドでスマートライセンスを有効にして登録することによって確立されます。FXOS の SSE コネクタは、スマートライセンスを登録することによって、SSE クラウドに自動的に登録されます。
- Cisco Success Network の設定は、シャーシマネージャで有効にする必要があります。
- テレメトリ設定は、ASA で有効にする必要があります。

ASA テレメトリデータが SSE クラウドに到達する仕組み

Cisco Success Network は、ASA 9.13(1) の Firepower 9300/4100 プラットフォームでデフォルトでサポートされています。FXOS サービスマネージャは、Firepower プラットフォームで実行されている ASA アプリケーションにテレメトリ要求を毎日送信します。ASA エンジンは、設定および接続ステータスに基づいて、スタンドアロンモードまたはクラスタモードのいずれかでテレメトリデータを FXOS に送信します。つまり、テレメトリのサポートが ASA で有効になっていて、SSE コネクタのステータスが接続済みの場合、テレメトリスレッドは、システムやプラットフォーム、またはデバイス API、ライセンス API、CPU API、メモリ API、ディスク API、Smart Call Home 機能の API などさまざまなソースから必要な情報を取得します。ただし、テレメトリのサポートが ASA で無効になっているか、または SSE コネクタのステータスが切断である場合、ASA は、テレメトリの設定ステータスを示す応答を FXOS（appAgent）に送信し、テレメトリデータは送信しません。

FXOS では、1 つの SSE コネクタインスタンスのみが実行されます。これが SSE クラウドに登録されると、1 つのデバイスと見なされ、SSE インフラでは FXOS に 1 つのデバイス ID が割り当てられます。SSE コネクタを介して送信されるテレメトリレポートは、同じデバイス ID で分類されます。したがって、FXOS は、各 ASA からのテレメトリレポートを 1 つのレポートに集約します。スマート ライセンス アカウント情報などのその他の内容が、レポートに追加されます。その後、FXOS は、最終的なレポートを SSE クラウドに送信します。テレメトリデータは、SSE データ交換（DEX）に保存され、シスコの IT チームで使用できるようになります。

Cisco Success Networkの有効化または無効化

始める前に

- FXOS でスマートライセンスを有効にして登録します。
- シャーシレベルで FXOS のテレメトリサポートを有効にするか（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』』を参照）、シャーシマネージャで Cisco Success Network

を有効にします（『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide』を参照）。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Telemetry]** を選択します。

[Enable Cisco Success Network] チェックボックスはデフォルトで選択されています。

ステップ 2 [Enable Cisco Success network] チェックボックスをオンにして、Cisco Success Network を有効にします。

ステップ 3 Cisco Success Network を無効にするには、[Enable Cisco Success Network] チェックボックスをオフにします。

ステップ 4 [Apply] をクリックします。

次のタスク

- テレメトリの設定とアクティビティのログまたはテレメトリデータを表示できます。「ASA テレメトリデータの表示 （1333 ページ）」を参照してください
- テレメトリデータおよびデータフィールドのサンプルを表示するには、次を参照してください。Cisco Success Network - テレメトリデータ （1334 ページ）

ASA テレメトリデータの表示

始める前に

- ASA でテレメトリサービスを有効にします。「Cisco Success Networkの有効化または無効化 （1332 ページ）」を参照してください

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Telemetry]** を選択します。

ステップ 2 [Telemetry] で、該当するオプションをクリックします。

- [History]：テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示します。
- [Sample]：即時に生成されたテレメトリデータを JSON 形式で表示します。
- [Last-report]：FXOS に送信された最新のテレメトリデータを JSON 形式で表示します。

ステップ 3 レポートを更新するには、[Refresh] をクリックします。

Cisco Success Network - テレメトリデータ

Cisco Success Network は、デフォルトでは Firepower 9300/4100 プラットフォームでサポートされています。FXOS サービスマネージャは、Firepower プラットフォームで実行されている ASA エンジンにテレメトリ要求を毎日送信します。ASA エンジンは、要求を受信すると、接続ステータスに基づいて、スタンドアロンモードまたはクラスタモードのいずれかでテレメトリデータを FXOS に送信します。次の表に、テレメトリデータポイント、その説明、およびサンプル値を示します。

表 *62 : Device Info*

データ ポイント	説明	値の例
Device Model	デバイス モデル	Cisco Adaptive Security Appliance
シリアル番号	デバイスのシリアル番号	FCH183771EZ
System Time	システムの動作期間	11658000
プラットフォーム	ハードウェア	FPR9K-SM-24
構成モード	展開タイプ	Native
セキュリティ コンテキスト モード	単一/複数	シングル

表 *63 :* バージョン情報

データ ポイント	説明	値の例
バージョングローバル変数	ASA のバージョン	9.13.1.5
デバイスマネージャのバージョン	デバイスマネージャのバージョン	7.10.1

表 *64 :* ライセンス情報

データ ポイント	説明	値の例
スマートライセンスのグローバル変数	有効化されているライセンス	regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION、1.0_555507e9-85f8-4e41-96de-860b59f10bbe

表 *65 :* プラットフォームに関する情報

データ ポイント	説明	値の例
CPU	過去 5 分間の CPU 使用率	fiveSecondsPercentage：0.2000000、 oneMinutePercentage：0、 fiveMinutesPercentage：0
メモリ	メモリ使用量	freeMemoryInBytes：225854966384、 usedMemoryInBytes：17798281616、 totalMemoryInBytes：243653248000
ディスク	ディスク使用量	freeGB：21.237285、 usedGB：0.238805、 totalGB：21.476090
Bandwidth	帯域幅の使用方法	receivedPktsPerSec：3、 receivedBytesPerSec：212、 transmittedPktsPerSec：3、 transmittedBytesPerSec：399

表 *66 :* 機能情報

データ ポイント	説明	値の例
機能リスト	有効な機能リスト	name：cluster status：enabled

表 *67 :* クラスタ情報

データ ポイント	説明	値の例
クラスタ情報	クラスタ情報	clusterGroupName：ssp-cluster interfaceMode：spanned unitName：unit-3-3 unitState：SLAVE otherMembers： items： memberName：unit-2-1 memberState：MASTER memberSerialNum：FCH183771BA

表 *68 :* フェールオーバー情報

データ ポイント	説明	値の例
フェールオーバー	フェールオーバー情報	myRole：Primary、 peerRole：Secondary、 myState：active、 peerState：standby、 peerSerialNum：FCH183770EZ

表 *69 :* ログイン情報

データ ポイント	説明	値の例
ログイン	ログイン履歴	loginTimes：2 times in last 2 days、 lastSuccessfulLogin：12:25:36 PDT Mar 11 2019

ASA テレメトリデータの例

次に、JSON 形式で ASA から送信されるテレメトリデータの例を示します。サービスマネージャは、この入力を受信すると、すべての ASA のデータを集約し、SSE コネクタに送信する前に必要なヘッダー/フィールドを追加します。ヘッダー/フィールドには、“version”、“metadata”、“payload”（“recordedAt”、“recordType”、 “recordVersion” 、および ASA テレメトリ

データの "smartLicenseProductInstanceIdentifier"、"smartLicenseVirtualAccountName" などを含む）があります。


```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
    "deviceInfo": {
        "deviceModel": "Cisco Adaptive Security Appliance",
        "serialNumber": "AANNNXXX",
        "systemUptime": 285,
        "udiProductIdentifier": "FPR9K-SM-36",
        "deploymentType": "Native",
        "securityContextMode": "Single"
    },
    "versions": {
        "items": [
            {
                "type": "asa_version",
                "version": "201.4(1)82"
            },
            {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
            }
        ]
    },
    "licenseActivated": {
        "items": [
            {
                "type": "Strong encryption",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",

                "count": 1
            },
            {
```

```
                "type": "Carrier",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "count": 1
            }
        ]
    },
    "CPUUsage": {
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0,
        "fiveMinutesPercentage": 0
    },
    "memoryUsage": {
        "freeMemoryInBytes": 99545662064,
        "usedMemoryInBytes": 20545378704,
        "totalMemoryInBytes": 120091040768
    },
    "diskUsage": {
        "freeGB": 21.237027,
        "usedGB": 0.239063,
        "totalGB": 21.476090
    },
    "bandwidthUsage": {
        "receivedPktsPerSec": 3,
        "receivedBytesPerSec": 268,
        "transmittedPktsPerSec": 4,
        "transmittedBytesPerSec": 461
    },
    "featureStatus": {
        "items": [
            {
                "name": "call-home",
                "status": "enabled"
            },
            {
                "name": "cluster",
                "status": "enabled"
            },
            {
                "name": "firewall_user_authentication",
                "status": "enabled"
            },
            {
                "name": "inspection-dns",
                "status": "enabled"
            },
            {
                "name": "inspection-esmtp",
                "status": "enabled"
            },
            {
                "name": "inspection-ftp",
                "status": "enabled"
            },
            {
                "name": "inspection-netbios",
                "status": "enabled"
            },
            {
                "name": "inspection-rsh",
                "status": "enabled"
            },
            {
                "name": "inspection-sip",
```

```
                "status": "enabled"
            },
            {
                "name": "inspection-sqlnet",
                "status": "enabled"
            },
            {
                "name": "inspection-sunrpc",
                "status": "enabled"
            },
            {
                "name": "inspection-tftp",
                "status": "enabled"
            },
            {
                "name": "inspection-xdmcp",
                "status": "enabled"
            },
            {
                "name": "logging-console",
                "status": "informational"
            },
            {
                "name": "management-mode",
                "status": "normal"
            },
            {
                "name": "sctp-engine",
                "status": "enabled"
            },
            {
                "name": "threat_detection_basic_threat",
                "status": "enabled"
            },
            {
                "name": "threat_detection_stat_access_list",
                "status": "enabled"
            },
            {
                "name": "webvpn-activex-relay",
                "status": "enabled"
            },
            {
                "name": "webvpn-dtls",
                "status": "enabled"
            }
        ]
    },
    "clusterInfo": {
        "clusterGroupName": "ssp-cluster",
        "interfaceMode": "spanned",
        "unitName": "unit-3-3",
        "unitState": "SLAVE",
        "otherMembers": {
            "items": [
                {
                    "memberName": "unit-2-1",
                    "memberState": "MASTER",
                    "memberSerialNum": "FCH183771BA"
                },
                {
                    "memberName": "unit-2-3",
                    "memberState": "SLAVE",
                    "memberSerialNum": "FLM1949C6JR"
```

```
                    },
                    {
                        "memberName": "unit-2-2",
                        "memberState": "SLAVE",
                        "memberSerialNum": "xxxxxxxx"
                    },
                    {
                        "memberName": "unit-3-2",
                        "memberState": "SLAVE",
                        "memberSerialNum": "xxxxxxxx"
                    },
                    {
                        "memberName": "unit-3-1",
                        "memberState": "SLAVE",
                        "memberSerialNum": "xxxxxxxx"
                    }
                ]
            }
        },
        "loginHistory": {
            "loginTimes": "1 times in last 1 days",
            "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
        }
    }
```

第 49 章

Cisco ISA 3000 のアラーム

この章では、ISA 3000 のアラーム システムの概要を示し、アラームを設定およびモニターする方法についても説明します。

アラームについて

さまざまな条件でアラームを発行するように ISA 3000 を設定できます。いずれかの条件が設定と一致しない場合、アラームがトリガーされます。これにより、LED、Syslog メッセージ、SNMP トラップによって、またアラーム出力インターフェイスに接続された外部デバイスを通じて、アラートがレポートされます。デフォルトでは、トリガーされたアラームにより Syslog メッセージだけが発行されます。

次のものをモニタするようにアラーム システムを設定できます。

- 電源
- プライマリおよびセカンダリ温度センサー。
- アラーム入力インターフェイス。

ISA 3000 には内部センサーに加えて 2 つのアラーム入力インターフェイスと 1 つのアラーム出力インターフェイスがあります。アラーム入力インターフェイスにはドアセンサーなどの外部センサーを接続できます。アラーム出力インターフェイスにはブザーやライトなどの外部アラーム デバイスを接続できます。

アラーム出力インターフェイスはリレーメカニズムです。アラーム条件に応じて、リレーが活性化または非活性化されます。リレーが活性化されると、インターフェイスに接続されているすべてのデバイスがアクティブになります。リレーが非活性化されると、接続されているすべてのデバイスが非アクティブ状態になります。リレーは、アラームがトリガーされているかぎり、活性化状態のままになります。

外部センサーとアラーム リレーの接続については、『Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide』を参照してください。

アラーム入力インターフェイス

アラーム入力インターフェイス（または接点）は外部センサー（ドアが開いているかどうかを検出するセンサーなど）に接続できます。

各アラーム入力インターフェイスには対応する LED があります。これらの LED は各アラーム入力のアラーム ステータスを示します。アラーム入力ごとにトリガーと重大度を設定できます。LED に加えて、出力リレーのトリガー（外部アラームをアクティブにするため）、Syslog メッセージの送信、および SNMP トラップの送信を行うように接点を設定できます。

次の表に、アラーム入力のアラーム状態に応じた LED のステータスを示します。また、アラーム入力に対する出力リレー、Syslog メッセージ、および SNMP トラップの応答を有効にしている場合のそれらの動作も示します。

Alarm Status	LED	出力リレー	Syslog	SNMP トラップ
アラームが設定されていない	オフ	—	—	—
アラームがトリガーされていない	グリーンに点灯	—	—	—
アラームがアクティブになる	マイナー アラーム：赤色で点灯 メジャー アラーム：赤色で点滅	リレーの電源が入る	syslog が生成される	SNMP トラップが送信される
アラーム終了	グリーンに点灯	リレーの電源がオフになる	syslog が生成される	—

アラーム出力インターフェイス

アラーム出力インターフェイスにはブザーやライトなどの外部アラームを接続できます。

アラーム出力インターフェイスはリレーとして機能します。また、このインターフェイスには、入力インターフェイスに接続された外部センサーや、デュアル電源センサー、温度センサーなどの内部センサーのアラーム ステータスを示す、対応する LED があります。出力リレーをアクティブにする必要があるアラームがある場合は、それを設定します。

次の表に、アラーム状態に応じた LED と出力リレーのステータスを示します。また、アラームに対する Syslog メッセージおよび SNMP トラップの応答を有効にしている場合のそれらの動作も示します。

Alarm Status	LED	出力リレー	Syslog	SNMP トラップ
アラームが設定されていない	オフ	—	—	—
アラームがトリガーされていない	グリーンに点灯	—	—	—
アラームがアクティブになる	レッド（点灯）	リレーの電源が入る	syslog が生成される	SNMP トラップが送信される
アラーム終了	グリーンに点灯	リレーの電源がオフになる	syslog が生成される	—

アラームのデフォルト

次の表に、アラーム入力インターフェイス（コンタクト）、冗長電源、および温度のデフォルト設定を示します。

	アラーム	Trigger	重大度	SNMP トラップ	出力リレー	syslog メッセージ
アラーム コンタクト 1	イネーブル	クローズ状態	Minor	ディセーブル	ディセーブル	有効
アラーム コンタクト 2	イネーブル	クローズ状態	Minor	ディセーブル	ディセーブル	有効
冗長電源（有効な場合）	[有効（Enabled）]	—	—	ディセーブル	ディセーブル	有効
温度	プライマリ温度アラームで有効（高温/低温のデフォルトしきい値はそれぞれ 92°C および -40°C）。 セカンダリ アラームでは無効。	—	—	プライマリ温度アラームについて有効	プライマリ温度アラームについて有効	プライマリ温度アラームについて有効

アラームの設定

ISA 3000 に対してアラームを設定するには、次の手順を実行します。

手順

ステップ 1 必要なアラーム コンタクト ペインで、アラーム、監視、およびロギングを設定します。

a) **[Configuration]** > **[Device Management]** > **[Alarm Port]** > **[Alarm Contact]** を選択します。
b) [major] または [minor] オプション ボタンをクリックして、重大度を指定します。重大度のアラームを無効にするには、[none] をクリックします。
c) [open] または [close] オプション ボタンをクリックして、トリガーを指定します。

デフォルトは close です。open を指定すると、通常は閉じているコンタクトが開かれた場合、または電流の流れが止まった時点で、アラームがトリガーされます。closed を指定すると、通常は開いているコンタクトが閉じられた場合、または電流の流れが開始された時点で、アラームがトリガーされます。

たとえば、ドア センサーがアラーム入力に接続されている場合、通常のオープン状態では、コンタクトを通過する電流はありません。ドアが開くと、コンタクトを電流が流れ、アラームが活性化されます。

d) （オプション）[Description] フィールドに説明を入力します。説明には最大 80 文字の英数字を使用でき、syslog メッセージに含められます。
e) [Enable relay] チェックボックスをオンにします。
f) syslog を有効化するには、[Enable system logger] チェックボックスをオンにします。
g) SNMP トラップを有効にするには、[Enable notification sent to server] チェック ボックスをオンにします。
h) [Apply] をクリックします。

ステップ 2 冗長電源のアラーム、監視、およびロギングを設定します。

電源アラームが動作するためには、冗長電源を有効にする必要があります。

冗長電源を有効にするには、**[Configuration]** > **[Device Management]** > **[Power Supply]** を選択します。[Enable Redundant Power Supply] チェック ボックスをオンにし、[Apply] をクリックします。

a) **[Configuration]** > **[Device Management]** > **[Alarm Port]** を選択します。
b) [Redundant Power Supply] タブをクリックします。
c) SNMP トラップを有効にするには、[Enable notification sent to server] チェック ボックスをオンにします。
d) [Enable relay] チェックボックスをオンにします。
e) syslog を有効化するには、[Enable system logger] チェックボックスをオンにします。
f) [Apply] をクリックします。

ステップ 3 温度のアラーム、監視、およびロギングを設定します。

a) **[Configuration]** > **[Device Management]** > **[Alarm Port]** を選択します。
b) [Temperature] タブをクリックします。
c) SNMP トラップを有効にするには、[Enable notification sent to server] チェック ボックスをオンにします。
d) [Enable relay] チェックボックスをオンにします。
e) syslog を有効化するには、[Enable system logger] チェックボックスをオンにします。
f) 必要なアラーム ペインのうち、[High Threshold] フィールドと [Low Threshold] フィールドに、それぞれ高い方のしきい値と低い方のしきい値を入力します。

   プライマリ温度アラームの有効な値の範囲は、–40 ℃ から 92 ℃ までです。セカンダリ温度アラームの有効な値の範囲は、–35 ℃ から 85 ℃ までです。セカンダリ アラームの高い方の温度しきい値が設定されている場合、セカンダリ アラームのみ有効になります。プライマリ アラームは無効にできません。プライマリ アラームのしきい値が指定されていない場合、高い方のしきい値と低い方のしきい値は、それぞれデフォルト値の 92 ℃ および -40 ℃ に戻ります。

g) [Apply] をクリックします。

アラームのモニターリング

アラームをモニターするには、次のペインを参照してください。

手順

- **[Monitoring]** > **[Properties]** > **[Alarm]** > **[Alarm Settings]** の順に選択します。

  このペインには、すべてのグローバル アラーム設定が表示されます。

- **[Monitoring]** > **[Properties]** > **[Alarm]** > **[Alarm Contact]** の順に選択します。

  このペインには、すべての外部アラーム設定が表示されます。

- **[Monitoring]** > **[Properties]** > **[Alarm]** > **[Facility Alarm Status]** の順に選択します。

  このペインには、指定した重大度に基づくすべてのアラームと、以下の情報が表示されます。

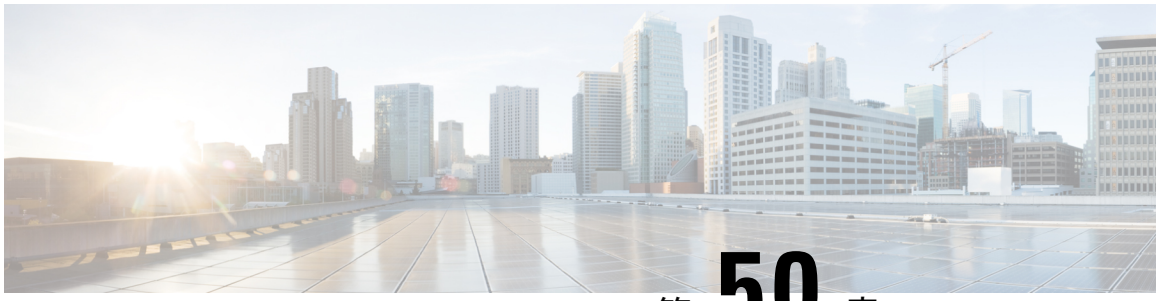
カラム	説明
ソース（Source）	アラームがトリガーされたデバイス。通常は、デバイスで設定されているホスト名です。
Severity	重大度が高い（major）か、低い（minor）か
説明	トリガーされたアラームのタイプ。たとえば、温度、外部連絡先、冗長電源など。

カラム	説明
Relay	電源が入っている（energized）か、入っていない（de-energized）か
時刻	トリガーされたアラームのタイムスタンプ

アラームの履歴

機能名	プラットフォームリリース	説明
ISA 3000 のアラーム ポートのサポート	9.7(1)	

機能名	プラットフォームリリース	説明
		ISA 3000 では、2 つのアラーム入力ピンと 1 つのアラーム出力ピン、およびアラームのステータスを通知する LED をサポートするようになりました。外部センサーは、アラーム入力に接続できます。外部ハードウェアリレーは、アラーム出力ピンに接続できます。外部アラームの説明を設定できます。また、外部アラームと内部アラームの重大度とトリガーも指定できます。すべてのアラームは、リレー、モニターリング、およびロギングに設定できます。 次のコマンドが導入されました。**alarm contact description**、**alarm contact severity**、**alarm contact trigger**、**alarm facility input-alarm**、**alarm facility power-supply rps**、**alarm facility temperature**、**alarm facility temperature high**、**alarm facility temperature low**、**clear configure alarm**、**clear facility-alarm output**、**show alarm settings**、**show environment alarm-contact**。 次の画面が導入されました。 **[Configuration]** > **[Device Management]** > **[Alarm Port]** > **[Alarm Contact]** **[Configuration]** > **[Device Management]** > **[Alarm Port]** > **[Redundant Power Supply]** **[Configuration]** > **[Device Management]** > **[Alarm Port]** > **[Temperature]** **[Monitoring]** > **[Properties]** > **[Alarm]** > **[Alarm Settings]** **[Monitoring]** > **[Properties]** > **[Alarm]** > **[Alarm Contact]** **[Monitoring]** > **[Properties]** > **[Alarm]** > **[Facility Alarm Status]**



第 50 章

Anonymous Reporting および Smart Call Home

この章では、Anonymous Reporting および Smart Call Home サービスを設定する方法について説明します。

Anonymous Reporting について

Anonymous Reporting をイネーブルにして、Cisco ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。この機能をイネーブルにした場合、お客様のアイデンティティは匿名のままとなり、識別情報は送信されません。

Anonymous Reporting をイネーブルにすると、トラスト ポイントが作成され、証明書がインストールされます。CA 証明書は、ASA でメッセージを安全に送信できるように、Smart Call Home Web サーバー上のサーバー証明書を検証して、HTTPS セッションを形成するために必要です。ソフトウェアに事前定義済みの証明書が、シスコによってインポートされます。Anonymous Reporting をイネーブルにする場合は、ハードコードされたトラスト ポイント名の _SmartCallHome_ServerCA で証明書が ASA にインストールされます。Anonymous Reporting をイネーブルにすると、このトラスト ポイントが作成され、適切な証明書がインストールされて、このアクションに関するメッセージが表示されます。これで、証明書が設定の中に存在するようになります。

Anonymous Reporting をイネーブルにしたときに、適切な証明書がすでに設定に存在する場合、トラスト ポイントは作成されず、証明書はインストールされません。

（注） Anonymous Reporting をイネーブルにすると、指定されたデータをシスコまたはシスコの代わりに運用するベンダー（米国以外の国を含む）に転送することに同意することになります。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いに関する詳細については、次の URL にあるシスコのプライバシー声明を参照してください。
http://www.cisco.com/web/siteassets/legal/privacy.html

ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行する CA の証明書を含むトラストポイントを自動生成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層を変更する必要はありません。また、手動介入なしに ASA が証明書階層を更新できるよう、トラストプールの証明書を自動的にインポートすることもできます。

ASA 9.14（2.14）をアップグレードすると、トラストポイントの設定が CallHome_ServerCA から CallHome_ServerCA2 に自動的に変更されます。

DNS 要件

ASA が Cisco Smart Call Home サーバーに到達してシスコにメッセージを送信できるように DNS サーバーを正しく設定する必要があります。ASA をプライベート ネットワークに配置し、パブリック ネットワークにはアクセスできないようにすることが可能なため、シスコでは DNS 設定を検証し、必要な場合には次の手順を実行して、ユーザーの代わりにこれを設定します。

1. 設定されているすべての DNS サーバーに対して DNS ルックアップを実行します。
2. 最もセキュリティレベルの高いインターフェイスで DHCPINFORM メッセージを送信して、DHCP サーバーから DNS サーバーを取得します。
3. ルックアップにシスコの DNS サーバーを使用します。
4. tools.cisco.com に対してランダムに静的 IP アドレスを使用します。

これらの作業は、現在の設定を変更せずに実行されます。（たとえば、DHCP から学習された DNS サーバーは設定には追加されません）。

設定されている DNS サーバーがなく、ASA が Cisco Smart Call Home サーバーに到達できない場合は、各 Smart Call Home メッセージに対して、重大度「warning」の syslog メッセージが生成されます。これは、DNS を適切に設定するようお願いするためです。

syslog メッセージについては、syslog メッセージガイドを参照してください。

Smart Call Home の概要

完全に設定が終わると、Smart Call Home は設置場所での問題を検出し、多くの場合はそのような問題があることにユーザーが気付く前に、シスコにレポートを返すか、別のユーザー定義のチャネル（ユーザー宛の電子メールまたはユーザーに直接など）を使用してレポートを返します。シスコでは、これらの問題の重大度に応じて次のサービスを提供することにより、システ

ムコンフィギュレーションの問題、製品ライフサイクル終了通知の発表、セキュリティ勧告問題などに対応します。

- 継続的モニターリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別する。
- サービス要求が開かれ、すべての診断データが添付された Smart Call Home 通知を使用して、潜在的な問題をユーザーに認識させる。
- Cisco TAC の専門家に自動的に直接アクセスすることにより、重大な問題を迅速に解決する。
- トラブルシューティングに必要な時間を短縮することにより、スタッフリソースを効率よく使用する。
- Cisco TAC へのサービス リクエストを自動的に生成し（サービス契約がある場合）、適切なサポート チームに提出する。問題解決の時間を短縮する、詳細な診断情報を提供します。

Smart Call Home ポータルを使用すると必要な情報に迅速にアクセスできるため、以下の事項が実現されます。

- すべての Smart Call Home メッセージ、診断、および推奨事項を一箇所で確認する。
- サービス リクエスト ステータスを確認する。
- すべての Smart Call Home 対応デバイスに関する最新のインベントリ情報およびコンフィギュレーション情報を表示する。

Anonymous Reporting および Smart Call Home のガイドライン

この項では、Anonymous Reporting と Smart Call Home を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

Anonymous Reporting のガイドライン

- DNS が設定されていること。
- Anonymous Reporting のメッセージを最初の試行で送信できなかった場合、ASA はメッセージをドロップする前にさらに 2 回試行します。
- Anonymous Reporting は、既存の設定を変更せずに、他の Smart Call Home 設定と共存させることができます。たとえば、Anonymous Reporting をイネーブルにする前に Smart Call Home がディセーブルになっている場合、Anonymous Reporting をイネーブルにした後でも、ディセーブルのままです。

- Anonymous Reporting をイネーブルにしている場合、トラスト ポイントを削除することはできません。また、Anonymous Reporting をディセーブルにした場合、トラスト ポイントはそのまま残ります。Anonymous Reporting がディセーブルの場合は、トラスト ポイントを削除できますが、Anonymous Reporting をディセーブルにしてもトラスト ポイントは削除されません。
- マルチ コンテキスト モード設定を使用している場合は、**dns**、**interface**、**trustpoint** コマンドは管理コンテキストにあり、**call-home** コマンドはシステム コンテキストにあります。
- CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。このトラストプール自動更新機能は、マルチ コンテキストの導入ではサポートされません。

Smart Call Home のガイドライン

- マルチ コンテキスト モードでは、subscribe-to-alert-group snapshot periodic コマンドは、システム コンフィギュレーションから情報を取得するコマンドと、ユーザ コンテキストから情報を取得するコマンドの 2 つのコマンドに分割されます。
- Smart Call Home のバックエンド サーバーは、XML 書式のメッセージのみ受け取ることができます。
- Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次のイベントに対してのみ送信されます。
  - ユニットがクラスタに参加したとき
  - ユニットがクラスタから脱退したとき
  - クラスタユニットがクラスタ制御ユニットになったとき
  - クラスタのセカンダリ ユニットが故障したとき

  送信される各メッセージには次の情報が含まれています。
  - アクティブ クラスタのメンバ数
  - クラスタ制御ユニットでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

Anonymous Reporting および Smart Call Home の設定

Anonymous Reporting は Smart Call Home サービスの一部であり、これを使用すると、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに匿名で送信できます。一方、Smart Call Home サービスは、システム ヘルスのサポートをカスタマイズする機能です。Cisco TAC

がお客様のデバイスをモニタして、問題があるときにケースを開くことができるようになります。多くの場合は、お客様がその問題に気付く前に発見できます。

両方のサービスをシステム上で同時に設定できますが、Smart Call Home サービスを設定すれば、Anonymous Reporting と同じ機能に加えて、カスタマイズされたサービスも使用できるようになります。

Anonymous Reporting の設定

Anonymous Reporting を設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Smart Call Home] の順に選択します。

ステップ 2 [Enable Anonymous Reporting] チェックボックスをオンにします。

ステップ 3 [Test Connection] をクリックして、システムでメッセージを送信できることを確認します。

ASDM は成功メッセージまたはエラー メッセージを返して、テスト結果を通知します。

ステップ 4 [Apply] をクリックして設定を保存し、Anonymous Reporting をイネーブルにします。

Smart Call Home の設定

Smart Call Home サービス、システム セットアップ、およびアラート サブスクリプション プロファイルを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Smart Call Home]** の順に選択します。

ステップ 2 [Enable Registered Smart Call Home] チェックボックスをオンにして、Smart Call Home をイネーブルにし、ASA を Cisco TAC に登録します。

ステップ 3 [Advanced System Setup] をダブルクリックします。この領域は、3 個のペインで構成されています。各ペインは、タイトル行をダブルクリックすると展開または縮小できます。

a) [Mail Servers] ペインで、Smart Call Home メッセージを電子メールのサブスクライバに配信する際に通過するメール サーバーを設定できます。

b) ASA の [Contact Information] ペインで、Smart Call Home メッセージに表示される担当者の個人情報を入力できます。このペインには、次の情報が含まれます。

- 連絡先担当者の名前。
- 連絡先の電話番号。
- 連絡先担当者の住所。

- 連絡先の電子メール アドレス。
- Smart Call Home 電子メールの「from」電子メール アドレス。
- Smart Call Home 電子メールの「reply-to」電子メール アドレス。
- カスタマー ID。
- サイト ID。
- 連絡先 ID。

c) [Alert Control] ペインで、アラートの制御パラメータを調整できます。このペインには、[Alert Group Status] ペインが含まれ、ここには次のアラート グループのステータス（イネーブルまたはディセーブル）がリストされます。

- 診断アラート グループ。
- コンフィギュレーション アラート グループ。
- 環境アラート グループ。
- インベントリ アラート グループ。
- スナップショット アラート グループ。
- syslog アラート グループ。
- テレメトリ アラート グループ。
- 脅威アラート グループ。
- 1 分間に処理される Smart Call Home メッセージの最大数。
- Smart Call Home 電子メールの「from」電子メール アドレス。

ステップ 4 [Alert Subscription Profiles] をダブルクリックします。指定した各サブスクリプション プロファイルによって、サブスクライバおよび対象とするアラート グループが特定されます。

a) [Add] または [Edit] をクリックして、**サブスクリプション プロファイル エディタ**を表示します。ここでは、新規サブスクリプションプロファイルを作成したり、既存のサブスクリプション プロファイルを編集したりできます。
b) [Delete] をクリックして、選択したプロファイルを削除します。
c) [Active] チェックボックスをオンにして、選択されたサブスクリプション プロファイルの Smart Call Home メッセージをサブスクライバに送信します。

ステップ 5 [Add] または [Edit] をクリックして、[Add Alert Subscription Profile] ダイアログボックスまたは [Edit Alert Subscription Profile] ダイアログ ボックスを表示します。

a) [Name] フィールドは読み取り専用であり、編集できません。
b) [Enable this subscription profile] チェックボックスをオンにして、この特定のプロファイルをイネーブルまたはディセーブルにします。

c) [Alert Delivery Method] 領域で、[HTTP] または [Email] オプション ボタンのいずれかをクリックします。

d) [Subscribers] フィールドに電子メール アドレスまたは Web アドレスを入力します。

e) [Reference Identity] に、syslog サーバーから受信した証明書に対する RFC 6125 参照 ID チェックをイネーブルにする参照 ID オブジェクトを名前で指定します。

参照 ID オブジェクトについて詳しくは、参照 ID の設定 （803 ページ）を参照してください。

ステップ 6 [Alert Dispatch] 領域では、管理者が、サブスクライバに送信する Smart Call Home 情報の種類と送信の条件を指定できます。時間ベースとイベントベースの 2 種類のアラートがあり、アラートのトリガー方法に応じて選択します。コンフィギュレーション、インベントリ、スナップショット、およびテレメトリの各アラート グループは時間ベースです。診断、環境、Syslog、および脅威の各アラート グループはイベントベースです。

ステップ 7 [Message Parameters] 領域では、優先されるメッセージ形式や最大メッセージ サイズなど、サブスクライバに送信されるメッセージを制御するパラメータを調整できます。

ステップ 8 時間ベースのアラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Add Configuration Alert Dispatch Condition] または [Edit Configuration Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b) [Basic] または [Detailed] オプション ボタンをクリックして、サブスクライバに必要な情報のレベルを指定します。

c) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 9 イベントベースの診断、環境、および脅威アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Diagnostic Alert Dispatch Condition] または [Edit Diagnostic Alert Dispatch Condition] ダイアログボックスを表示します。

ステップ 10 [Event Severity] ドロップダウン リストで、サブスクライバへのアラートのディスパッチをトリガーするイベントの重大度を指定し、[OK] をクリックします。

ステップ 11 時間ベースのインベントリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Inventory Alert Dispatch Condition] または [Edit Inventory Alert Dispatch Condition] ダイアログボックスを表示します。

ステップ 12 [Alert Dispatch Frequency] ドロップダウン リストで、サブスクライバにアラートをディスパッチする頻度を指定し、[OK] をクリックします。

ステップ 13 時間ベースのスナップショット アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Snapshot Alert Dispatch Condition] または [Edit Snapshot Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。
- 間隔サブスクリプションの場合、サブスクライバに情報を送信する頻度を分単位で指定します。この要件は、スナップショット アラート グループにのみ適用されます。

b) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 14 イベントベースの syslog アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Syslog Alert Dispatch Condition] または [Edit Syslog Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Specify the event severity which triggers the dispatch of alert to subscribers] チェックボックスをオンにして、ドロップダウン リストからイベントの重大度を選択します。
b) [Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers] チェックボックスをオンにします。
c) 画面の指示に従って、サブスクライバへのアラートのディスパッチをトリガーする syslog メッセージ ID を指定します。
d) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 15 イベントベースのテレメトリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Telemetry Alert Dispatch Condition] または [Edit Telemetry Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。

- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 16 [Test] をクリックして、設定したアラートが正しく動作しているかどうかを判別します。

trustpool 証明書の自動インポートの設定

スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層の変更を調整する必要はありません。CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。この機能はマルチ コンテキスト展開ではサポートされません。

trustpool の証明書バンドルを自動的にインポートするには、ASA がバンドルのダウンロードとインポートに使用する URL を指定する必要があります。次のコマンドを入力すると、デフォルトの Cisco URL とデフォルトの時間（22 時間）を使用して、毎日一定の間隔でインポートが実行されます。

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

また、次のコマンドを使用して、カスタム URL による自動インポートをイネーブルにできます。

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

オフピーク時またはその他の都合のよい時間帯に柔軟にダウンロードを設定できるようにするには、次のコマンドを入力して、カスタム時間によるインポートをイネーブルにします。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

カスタム URL とカスタム時間の両方による自動インポートを設定するには、次のコマンドを使用する必要があります。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

Anonymous Reporting および Smart Call Home のモニターリング

Anonymous Reporting および Smart Call Home サービスのモニターリングについては、次のコマンドを参照してください。**[Tools] > [Command Line Interface]**を使用してこのコマンドを入力できます。

- **show call-home detail**

このコマンドは、現在の Smart Call Home の詳細設定を表示します。

- **show call-home mail-server status**

  このコマンドは、現在のメール サーバーのステータスを表示します。

- **show call-home profile** {profile name | **all**}

  このコマンドは、Smart Call Home プロファイルのコンフィギュレーションを表示します。

- **show call-home registered-module status** [**all**]

  このコマンドは、登録されているモジュールのステータスを表示します。

- **show call-home statistics**

  このコマンドは、Call Home の詳細ステータスを表示します。

- **show call-home**

  このコマンドは、現在の Smart Call Home のコンフィギュレーションを表示します。

- **show running-config call-home**

  このコマンドは、現在の Smart Call Home の実行コンフィギュレーションを表示します。

- **show smart-call-home alert-group**

  このコマンドは、Smart Call Home アラート グループの現在のステータスを表示します。

- **show running-config all**

  このコマンドは、Anonymous Reporting ユーザー プロファイルに関する詳細を表示します。

Anonymous Reporting および Smart Call Home の履歴

表 *70 : Anonymous Reporting* および *Smart Call Home* の履歴

機能名	プラットフォームリリース	説明
Smart Call Home	8.2(2)	Smart Call Home サービスは、ASA に関するプロアクティブ診断およびリアルタイム アラートを提供し、ネットワークの可用性と運用効率を向上させます。 次の画面が導入されました。 [Configuration] > [Device Management] > [Smart Call Home]。

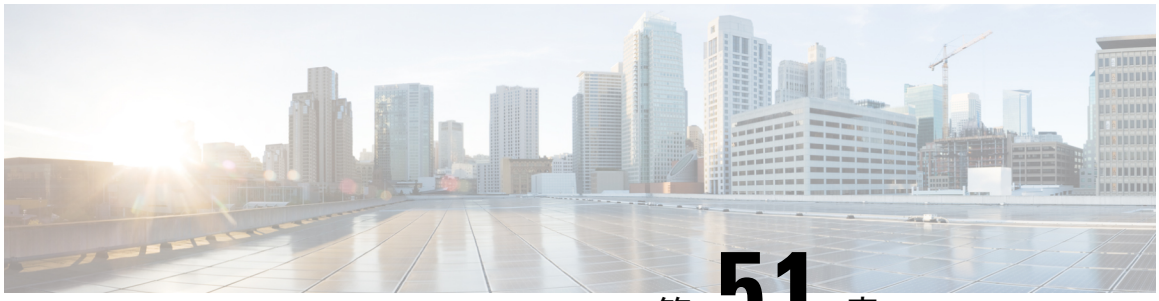
機能名	プラットフォームリリース	説明
Anonymous Reporting	9.0(1)	Anonymous Reporting をイネーブルにして、ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。 次の画面が変更されました。[Configuration] > [Device Monitoring] > [Smart Call Home]。
Smart Call Home	9.1(2)	テレメトリ アラート グループ レポートのための **show local-host** コマンドは、**show local-host | include interface** コマンドに変更になりました。
Smart Call Home	9.1(3)	Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタイベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対してのみ送信されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタユニットがクラスタ制御ユニットになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ制御ユニットでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

機能名	プラットフォームリリース	説明
セキュアな Smart Call Home サーバー接続のリファレンス ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 検証は、Smart Call Home サーバーへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のページが変更されました。[Configuration] > [Device Management] > [Smart Call Home]。

第 IX 部

参照先

- アドレス、プロトコル、およびポート （1363 ページ）



第 51 章

アドレス、プロトコル、およびポート

この章では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。

IPv4 アドレスとサブネット マスク

この項では、Cisco ASA で IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビット フィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワーク プレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワーク プレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワーク プレフィックスとホスト番号の間の境界を決定します。

クラス

IP ホスト アドレスは、Class A、Class B、Class C の 3 つの異なるアドレス クラスに分かれています。各クラスは、32 ビット アドレス内の異なるポイントで、ネットワーク プレフィックスとホスト番号の間の境界を決定します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）は、最初のオクテットのみをネットワーク プレフィックスとして使用します。

- Class B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス（192.0.0.xxx ～ 223.255.255.xxx）は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホスト アドレス、Class B アドレスには 65,534 個のホストがあるので、サブネットマスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、インターネット割り当て番号局（IANA）が推奨するプライベート IP アドレスを使用できます（RFC 1918 を参照）。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクを使用すると、単一の Class A、B、または C ネットワークを複数のネットワークに変換できます。サブネット マスクを使用して、ホスト番号からネットワーク プレフィックスにビットを追加する拡張ネットワーク プレフィックスを作成することができます。たとえば、Class C ネットワーク プレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワーク プレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネット マスクを容易に理解できます。サブネット マスク内のビットには、インターネット アドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

例 1：Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワーク プレフィックスの一部として使用するには、サブネット マスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネット マスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

例 2：3 番目のオクテットの一部だけを拡張ネットワーク プレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネット マスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワーク プレフィックスに使用されます。

サブネット マスクは、ドット付き 10 進数マスクまたは /ビット（「スラッシュ ビット」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリ オクテットを 10 進数の 255.255.255.0 に変換します。/ビット マスクの場合は、1s: /24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワーク プレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 です。

サブネットマスクの決定

必要なホストの数に基づいてサブネットマスクを決定するには、次の表を参照してください。

（注） 単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

表 *71* : ホスト、ビット、ドット区切りの *10* 進数マスク

ホスト	/ビット マスク	ドット付き 10 進数マスク
16,777,216	/8	255.0.0.0 Class A ネットワーク
65,536	/16	255.255.0.0 Class B ネットワーク
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C ネットワーク
128	/25	255.255.255.128
64	/26	255.255.255.192

ホスト	/ビット マスク	ドット付き 10 進数マスク
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

サブネットマスクに使用するアドレスの決定

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネット マスクで使用するネットワーク アドレスを判別する方法について説明します。

クラス C 規模ネットワーク アドレス

2 ～ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホスト アドレスの数の倍数になります。例として、次の表に 8 個のホストを持つサブネット（/29）、192.168.0.x を示します。

（注） サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

表 *72:* クラス *C* 規模ネットワーク アドレス

マスク /29（255.255.255.248）でのサブネット	アドレス範囲
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31
—	—
192.168.0.248	192.168.0.248 ～ 192.168.0.255

クラス B 規模ネットワーク アドレス

254 ～ 65,534 のホストを持つネットワークのサブネット マスクで使用するネットワーク アドレスを判別するには、可能な拡張ネットワーク プレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.*x*.0 のようなアドレスをサブネット化

することができます。ここで、最初の2つのオクテットは拡張ネットワーク プレフィックスで使用されるため固定されています。4 番目のオクテットは、すべてのビットがホスト番号に使用されるため、0 です。

3 番目のオクテットの値を判別するには、次の手順を実行します。

1. 65,536（3 番目と 4 番目のオクテットを使用するアドレスの合計）を必要なホスト アドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

   たとえば、65,536 を 4096 のホストで割ると、16 になります。したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

2. 256（3 番目のオクテットの値の数）をサブネットの数で割って、3 番目のオクテット値の倍数を判別します。

   この例では、256/16 = 16 です。

   3 番目のオクテットは、0 から始まる 16 の倍数になります。

次の表に、ネットワーク 10.1 の 16 個のサブネットを示します。

（注） サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

表 *73:* ネットワークのサブネット

マスク /20（255.255.240.0）でのサブネット	アドレス範囲
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
—	—
10.1.240.0	10.1.240.0 ～ 10.1.255.255

IPv6 アドレス

IPv6は、IPv4後の次世代インターネットプロトコルです。これにより、アドレス空間の拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フローラベル機能、および認証とプライバシーの機能が提供されます。IPv6についてはRFC2460で説明されています。IPv6 アドレッシング アーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 のアドレス形式とアーキテクチャについて説明します。

IPv6 アドレスの形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

（注） IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

アドレスの個々のフィールドに先行ゼロを入れる必要はありませんが、各フィールドに 1 個以上の桁が含まれている必要があります。したがって、例のアドレス 2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～ 6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン（::）を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。次の表に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

表 *74 : IPv6* アドレスの圧縮例

Address Type	標準形式	圧縮形式
ユニキャスト	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

（注） ゼロのフィールドが連続することを表す 2 つのコロン（::）は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、y はアドレスの 32 ビット IPv4 部分（IPv6 アドレスの残りの 2 つの 16 ビッ

ト部分を占める）の 10 進数値を表します。たとえば、IPv4 アドレス 192.168.1.1 は、IPv6 アドレス 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 として表すことができます。

IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト**：ユニキャストアドレスは、単一インターフェイスの識別子です。ユニキャストアドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1 つのインターフェイスに複数のユニキャスト アドレスが割り当てられている場合もあります。
- **マルチキャスト**：マルチキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト**：エニーキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスと違い、エニーキャストアドレスに送信されたパケットは、ルーティングプロトコルの距離測定によって判別された「最も近い」インターフェイスにだけ送信されます。

（注） IPv6 にはブロードキャスト アドレスはありません。マルチキャスト アドレスにブロードキャスト機能があります。

ユニキャスト アドレス

この項では、IPv6ユニキャストアドレスについて説明します。ユニキャストアドレスは、ネットワーク ノード上のインターフェイスを識別します。

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般的な形式では、グローバル ルーティング プレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバル ルーティングプレフィックスは、別の IPv6 アドレス タイプによって予約されていない任意のプレフィックスです。

バイナリ 000 で始まるものを除くすべてのグローバル ユニキャスト アドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。

バイナリ 000 で始まるグローバル ユニキャスト アドレスには、アドレスのインターフェイス ID部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります。

サイトローカル アドレス

サイトローカルアドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルで一意のプレフィックスを使用せずにサイト全体をアドレッシングするこ

とができます。サイトローカルアドレスでは、プレフィックス FEC0::/10、54 ビット サブネット ID、64 ビット インターフェイス ID（Modified EUI-64 形式）の順に並んでいます。

サイトローカル ルータは、サイト外の送信元または宛先にサイトローカル アドレスを持つパケットを転送しません。したがって、サイトローカル アドレスは、プライベート アドレスと見なされます。

リンクローカル アドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカル アドレスが必要です。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

リンクローカル アドレスは、Modified EUI-64 形式でリンクローカル プレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。リンクローカルアドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカルアドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカルアドレスを持つパケットを送信しません。したがって、リンクローカル アドレスは、プライベート アドレスと見なされます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、IPv4 互換 IPv6 アドレスです。IPv6 移行メカニズムには、IPv4 ルーティング インフラストラクチャ上で IPv6 パケットを動的にトンネリングさせるためのホストおよびルータの技術が実装されています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャスト アドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。この y.y.y.y は IPv4 ユニキャスト アドレスになります。

（注） 「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャスト アドレスである必要があります。

2 つ目のタイプの IPv6 アドレスは、IPv4 アドレスが埋め込まれたもので、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレス タイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャスト アドレスです。

未指定アドレス

未指定アドレス 0:0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（注） IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ループバック アドレス

ループバック アドレス 0:0:0:0:0:0:0:1 は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレス（127.0.0.1）と同じように機能します。

（注） IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

インターフェイス識別子

IPv6 ユニキャスト アドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネットプレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイス リンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ 000 で始まるものを除くすべてのユニキャストアドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル/ローカル ビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 FFFE を挿入することによって、48 ビット MAC アドレスから作成されます。

たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

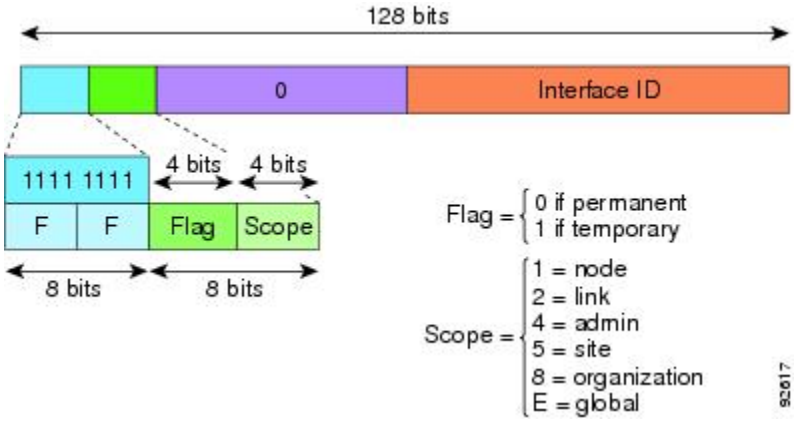
マルチキャスト アドレス

IPv6 マルチキャスト アドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。1 つのインターフェイスが任意の数のマルチキャスト グループに属すことができます。

IPv6 マルチキャスト アドレスのプレフィックスは FF00::/8（1111 1111）です。オクテットとそれに続くプレフィックスは、マルチキャストアドレスのタイプとスコープを定義します。永続的に割り当てられた（周知の）マルチキャストアドレスには、0 に等しいフラグ パラメータがあり、一時的な（過渡）マルチキャスト アドレスには 1 に等しいフラグ パラメータがあります。ノード、リンク、サイト、組織のスコープ、またはグローバル スコープを持つマルチ

キャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、または E です。たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。次の図に、IPv6 マルチキャスト アドレスの形式を示します。

図 *81 : IPv6* マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに参加する必要があります。

- All Nodes マルチキャスト アドレス：
  - FF01::（インターフェイスローカル）
  - FF02::（リンクローカル）
- ノード FF02:0:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャスト アドレスおよびエニーキャスト アドレスの送信要求ノード アドレス。ここで、XX:XXXX は低次 24 ビットのユニキャスト アドレスまたはエニーキャスト アドレスです。

注 送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャスト グループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャスト アドレスは、IPv6 パケットで送信元アドレスとして使用できません。

（注） IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャスト アドレスです。エニーキャスト アドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティング プロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられます。エニーキャスト アドレスは、複数のインターフェイスに割り当てられたユニキャスト アドレスにすぎません。インターフェイスは、アドレスをエニーキャストアドレスとして認識するように設定されている必要があります。

エニーキャスト アドレスには次の制限が適用されます。

- エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。
- エニーキャスト アドレスは、IPv6 ホストに割り当てることはできません。IPv6 ルータにだけ割り当てるこができます。

（注） ASA では、エニーキャスト アドレスをサポートされていません。

必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカル アドレス
- ループバック アドレス
- All-Nodes マルチキャスト アドレス
- 各ユニキャスト アドレスまたはエニーキャスト アドレスの送信要求ノード マルチキャスト アドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホスト アドレス
- このルータがルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャスト アドレス
- All-Routers マルチキャスト アドレス

IPv6 アドレス プレフィックス

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを特定します。次の表に、各 IPv6 アドレス タイプのプレフィックスを示します。

表 *75 : IPv6* アドレス タイプのプレフィックス

Address Type	バイナリ プレフィックス	IPv6 表記
未指定	000...0（128 ビット）	::/128
ループバック	000...1（128 ビット）	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカル（ユニキャスト）	1111111010	FE80::/10
サイトローカル（ユニキャスト）	1111111111	FEC0::/10
グローバル（ユニキャスト）	その他すべてのアドレス。	
エニーキャスト	ユニキャスト アドレス空間から取得。	

プロトコルとアプリケーション

次の表に、プロトコルのリテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。

表 *76 :* プロトコルのリテラル値

リテラル	値	説明
ah	51	IPv6 の認証ヘッダー（RFC 1826）。
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。
esp	50	IPv6 の暗号ペイロード（RFC 1827）。
gre	47	総称ルーティング カプセル化。

リテラル	値	説明
icmp	1	インターネット制御メッセージ プロトコル（RPC 792）。
icmp6	58	IPv6 のインターネット制御メッセージ プロトコル（RFC 2463）。
igmp	2	インターネット グループ管理プロトコル（RFC 1112）。
igrp	9	Interior Gateway Routing Protocol。
ip	0	インターネット プロトコル。
ipinip	4	IP-in-IP カプセル化。
ipsec	50	IP セキュリティ。ipsec プロトコル リテラルを入力すると、esp プロトコル リテラルを入力した場合と同じ結果が得られます。
nos	94	ネットワーク オペレーティング システム（Novell の NetWare）。
ospf	89	OSPF ルーティング プロトコル（RFC 1247）。
pcp	108	ペイロード圧縮プロトコル。
pim	103	プロトコル独立型マルチキャスト。
pptp	47	ポイントツーポイント トンネリング プロトコル。pptp プロトコル リテラルを入力すると、gre プロトコル リテラルを入力した場合と同じ結果が得られます。
snp	109	Sitara Networks Protocol。
tcp	6	伝送制御プロトコル（RFC 793）。
udp	17	ユーザー データグラム プロトコル（RFC 768）。

IANA の Web サイトでオンラインでプロトコル番号を確認できます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートおよび UDP ポート

次の表に、リテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。次の警告を参照してください。

- ASA は、SQL*Net 用にポート 1521 を使用します。これは、Oracle が SQL*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- ASA は、ポート 1645 と 1646 で RADIUS をリッスンしています。RADIUS サーバーが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリッスンするように ASA を設定できます。

- DNSアクセスにポートを割り当てるには、**dns**ではなく**domain**リテラル値を使用します。**dns** を使用した場合、ASA では、**dnsix** リテラル値を使用すると見なされます。

IANA の Web サイトでオンラインでポート番号を確認できます。

http://www.iana.org/assignments/port-numbers

表 77 : ポートのリテラル値

リテラル	TCP または UDP	値	説明
aol	TCP	5190	America Online
bgp	TCP	179	ボーダー ゲートウェイ プロトコル（RFC 1163）
biff	UDP	512	新しいメールの受信をユーザーに通知するために、メール システムが使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
bootps	UDP	67	ブートストラップ プロトコル サーバー
chargen	TCP	19	キャラクタ ジェネレータ
cifs	TCP、UDP	3020	Common Internet File System
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	cmd は自動認証機能がある点を除いて、exec と同様。
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time（日時）（RFC 867）
discard	TCP、UDP	9	廃棄
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
domain	TCP、UDP	53	DNS
echo	TCP、UDP	7	Echo
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	ファイル転送プロトコル（コンソールポート）

リテラル	TCP または UDP	値	説明
ftp-data	TCP	20	ファイル転送プロトコル（データ ポート）
gopher	TCP	70	Gopher
h323	TCP	1720	H.323 発呼信号
hostname	TCP	101	NIC ホスト ネーム サーバー
http	TCP、UDP	80	World Wide Web HTTP
https	TCP	443	HTTP over SSL
ident	TCP	113	ID 認証サービス
imap4	TCP	143	Internet Message Access Protocol バージョン 4
irc	TCP	194	インターネット リレー チャット プロトコル
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	[TCP]	389	Lightweight Directory Access Protocol。
ldaps	TCP	636	ライトウェイトディレクトリ アクセス プロトコル（SSL）
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	ライン プリンタ デーモン（プリンタ スプーラー）
mobile-ip	UDP	434	モバイル IP-Agent
nameserver	UDP	42	ホスト ネーム サーバー
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス

リテラル	TCP または UDP	値	説明
nfs	TCP、UDP	2049	ネットワーク ファイル システム（Sun Microsystems）
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	ネットワーク タイム プロトコル
pcanywhere-data	TCP	5631	pcAnywhere データ
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pim-auto-rp	TCP、UDP	496	Protocol Independent Multicast、逆パス フラッド、デンス モード
pop2	TCP	109	Post Office Protocol（POP）Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	リモート認証ダイヤルイン ユーザー サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザー サービス（アカウンティング）
rip	UDP	520	ルーティング情報プロトコル
rsh	TCP	514	リモート シェル
rtsp	TCP	554	Real Time Streaming Protocol
secureid-udp	UDP	5510	SecureID over UDP
sip	TCP、UDP	5060	Session Initiation Protocol
smtp	TCP	25	シンプル メール転送プロトコル
snmp	UDP	161	簡易ネットワーク管理プロトコル
snmptrap	UDP	162	簡易ネットワーク管理プロトコル（トラップ）
sqlnet	TCP	1521	構造化照会言語ネットワーク
ssh	TCP	22	セキュア シェル
sunrpc	TCP、UDP	111	Sun Remote Procedure Call
syslog	UDP	514	システム ログ

リテラル	TCP または UDP	値	説明
tacacs	TCP、UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP、UDP	517	Talk
Telnet	TCP	23	Telnet（RFC 854）
tftp	UDP	69	『Trivial File Transfer Protocol』
time	UDP	37	時刻
uucp	TCP	540	UNIX 間コピー プログラム
vxlan	UDP	4789	Virtual eXtensible Local Area Network（VXLAN）
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP、UDP	80	ワールドワイド ウェブ
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートとプロトコル

次の表に、ASA に向かうトラフィックを処理するために ASA が開くプロトコル、TCP ポート、および UDP ポートを示します。この表に記載されている機能とサービスをイネーブルにしない限り、ASA は、TCP または UDP ポートでローカル プロトコルを開きません。ASA がデフォルトのリスニング プロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルト ポート以外のポートを設定できます。

表 *78*：機能とサービスによって開かれるプロトコルとポート

機能またはサービス	プロトコル	Port Number	注
DHCP	UDP	67、68	—
フェールオーバー制御	105	該当なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	該当なし	—

機能またはサービス	プロトコル	Port Number	注
IGMP	2	該当なし	プロトコルは宛先 IP アドレス 224.0.0.1 でだけ開かれます
ISAKMP/IKE	UDP	500	設定可能。
IPsec（ESP）	50	該当なし	—
IPsec over UDP（NAT-T）	UDP	4500	—
IPsec over TCP（CTCP）	TCP	—	デフォルト ポートは使用されません。IPsec over TCP の設定時にポート番号を指定する必要があります。
NTP	UDP	123	—
OSPF	89	該当なし	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でだけ開かれます
PIM	103	該当なし	プロトコルは宛先 IP アドレス 224.0.0.13 でだけ開かれます
RIP	UDP	520	—
RIPv2	UDP	520	ポートは宛先 IP アドレス 224.0.0.9 でだけ開かれます
SNMP	UDP	161	設定可能。
SSH	TCP	22	—
ステートフルアップデート	8（ノンセキュア）9（セキュア）	該当なし	—
Telnet	TCP	23	—
VPN ロードバランシング	UDP	9023	設定可能。
VPN 個別ユーザー認証プロキシ	UDP	1645、1646	ポートは VPN トンネルでだけアクセスできます。

ICMP タイプ

次の表に、ASA のコマンドで入力できる ICMP タイプの番号と名前を示します。

表 *79 : ICMP* タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect