Cisco Secure Firewall Device Manager バージョン 7.4 コンフィギュレーション ガイド

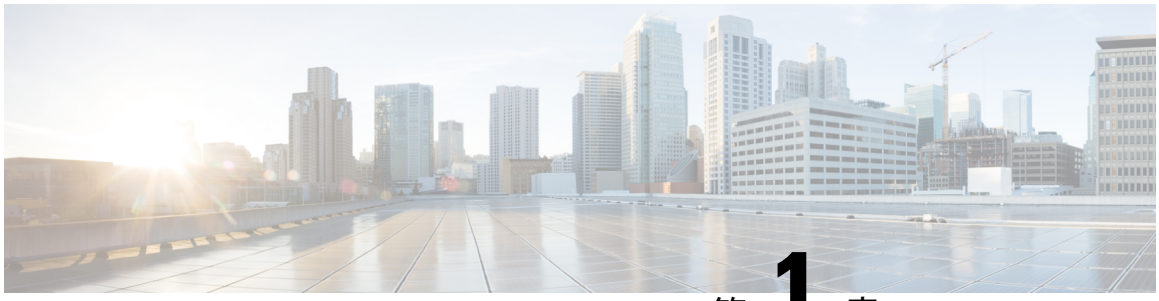
初版：2023 年 12 月 5 日

最終更新：2024 年 5 月 24 日

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



第 1 章

使用する前に

次のトピックでは、Secure Firewall Threat Defense（旧称 Firepower Threat Defense）の設定を開始する方法について説明します。

このガイドの対象読者

このマニュアルでは、脅威に対する防御デバイスに組み込まれたSecure Firewall Device Manager（旧称 Firepower Device Manager）の Web ベース設定インターフェイスを使用して 脅威に対する防御 を設定する方法について説明します。

Device Manager では、小規模または中規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの 脅威に対する防御 デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または 脅威に対する防御 で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Device Manager の代わりに Secure Firewall Management Center（旧称 Firepower Management Center）を使用してデバイスを設定します。

Device Manager /Threat Defense バージョン 7.4.1 の新機能

リリース日：2023 年 12 月 13 日

次の表に、Device Manager を使用して構成した場合に 脅威に対する防御 7.4.1 で使用可能な新規機能を示します。

機能	説明
プラットフォーム機能	
Firepower 1010E のサポートが再開されています。。	バージョン 7.2.3 で導入され、バージョン 7.3 で一時的に廃止された Firepower 1010E のサポートが再開されています。
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	Cisco Secure Firewall 3130 および 3140 向けに次のネットワークモジュールが導入されました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド
VPN 機能	
Cisco Secure Firewall 3100 向け VTI ループバック インターフェイスの IPSec フローのオフロード。	**アップグレードの影響。 条件を満たす接続のオフロードが開始されます。** Cisco Secure Firewall 3100 では、VTI ループバック インターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされるようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。この機能はアップグレードにより自動的に有効になります。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
インターフェイス機能	

機能	説明
マージされた管理インターフェイスと診断インターフェイス。	**アップグレードの影響。アップグレード後にインターフェイスをマージします。** 7.4 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。 マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。 新規/変更された画面： • **[Devices]** > **[Interfaces]** > **[Management]** インターフェイス • （インターフェイスに移動）**[System Settings]** > **[Management Interface]** • **[Devices]** > **[Interfaces]** > **[Merge Interface action needed]** > **[Management Interface Merge]** 新規/変更されたコマンド： **show management-interface convergence**
Azure と GCP 上の 3 つのインターフェイスを使用して Threat Defense Virtual を展開します。	Azure と GCP で（4 つではなく）3 つのインターフェイスを使用して Threat Defense Virtual を展開できるようになりました。そのためには、診断インターフェイスを削除します。 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 に対するインラインセット。	Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 デバイスでインラインセットを設定できます。[インターフェイス（Interface）] ページに [インラインセット（inline sets）] タブを追加しました。

機能	説明
ライセンシング機能	
ライセンス名の変更およびキャリアライセンスのサポート。	ライセンス名が次のように変更されました。 • Threat は IPS に変更 • Malware は Malware Defense に変更 • Base は Essentials に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更 さらに、キャリアライセンスを適用できるようになりました。これにより、GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定できます。これらの機能を設定するには、FlexConfig を使用します。
管理およびトラブルシューティングの機能	
デフォルトの NTP サーバーが更新されました。	**アップグレードの影響。システムは新しいリソースに接続します。** デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。別の NTP サーバーを使用するには、[デバイス（Device）] を選択し、[システム設定（System Settings）] パネルで [タイムサービス（Time Services）] をクリックします。
HTTPS 管理ユーザーアクセス用の SAML サーバー。	HTTPS 管理アクセスに外部認証を提供するように SAML サーバーを設定できます。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバーを使用する場合は、ログインに共通アクセスカード（CAC）を使用できます。 SAML アイデンティティ ソース オブジェクトの設定を更新し、該当オブジェクトを受け入れるように**[システム設定（System Settings）] > [管理アクセス（Management Access）]** ページを更新しました。

機能	説明
Threat Defense 高可用性ペアの設定の不一致を検出します。	CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。 新規/変更された CLI コマンド：**show failover config-sync error**、**show failover config-sync stats** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Cisco Secure Firewall 3100 でドロップされたパケットをキャプチャします。	MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100 は、これらのドロップされたパケットをキャプチャできるようになりました。 新規/変更された CLI コマンド：**capture** コマンドの [**drop** { **disable** | **mac-filter** }]。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
FXOS アップグレードに含まれるファームウェアのアップグレード。	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 以降への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド

機能	説明
Firepower 1000/2100 および Firepower 4100/9300 のデータプレーン障害後の迅速な回復。	Firepower 1000/2100 または Firepower 4100/9300 のデータプレーンプロセスがクラッシュすると、デバイスを再起動する代わりにプロセスがリロードされます。データプレーンをリロードすると、Snort を含む他のプロセスも再起動します。ブートアップ中にデータプレーンがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードループが回避されます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。 新規/変更された ASA CLI コマンド：**data-plane quick-reload**、**show data-plane quick-reload status** 新規/変更された Threat Defense CLI コマンド：**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 参照：Cisco Secure Firewall Threat Defense コマンドリファレンスおよびCisco Secure Firewall ASA シリーズ コマンド リファレンス

システムへのログイン

脅威に対する防御 デバイスには、次の 2 つのインターフェイスがあります。

Device Manager Web インターフェイス

Device Manager は Web ブラウザで実行されます。このインターフェイスを使用して、システムを設定、管理、モニターできます。

コマンドライン インターフェイス（CLI、コンソール）

CLI はトラブルシューティングに使用します。Device Manager の代わりに初期設定に使用することもできます。

次に、これらのインターフェイスにログインし、ユーザーアカウントを管理する方法を説明します。

ユーザー ロールで表示および実行可能な対象の制御

ユーザー名はロールに割り当てられ、Device Manager で何を実行できるか、また何を表示できるかがユーザーロールによって決まります。ローカルに定義される [管理者（admin）] ユーザ

にはすべての権限がありますが、別のアカウントを使用してログインすると権限が少なくなります。

Device Manager ウィンドウの右上隅にユーザー名と権限レベルが表示されます。

権限は次のとおりです。

- [管理者（Administrator）]：すべての機能を表示および使用できます。
- [読み取り/書き込みユーザー（Read-Write User）]：読み取り専用ユーザーが実行できることをすべて実行できます。また、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、他の Device Manager ユーザーセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- [読み取り専用ユーザ（Read-Only User）]：ダッシュボードおよび設定を表示できますが、変更することはできません。変更しようとすると、権限がないことを示すエラーメッセージが表示されます。
- [暗号管理者（Cryptographic Admin）]：証明書、復号ポリシー、秘密キーなどの暗号化関連機能を設定できます。他の機能への読み取り専用アクセス。
- [監査管理者（Audit Admin）]：ユーザーのログイン履歴と監査ログを表示し、監査関連のアクションを実行できます。設定機能への読み取り専用アクセス。

これらの権限は、CLI ユーザーが利用できる権限とは関連していません。

Device Manager へのログイン

Device Manager を使用して、システムの設定、管理、モニターを行います。ブラウザで設定可能な機能を、コマンドラインインターフェイス（CLI）で設定することはできません。セキュリティ ポリシーを実装するには、Web インターフェイスを使用する必要があります。

Firefox、Chrome、Safari、Edge ブラウザの最新バージョンを使用します。

（注） 誤ったパスワードを入力し、3 回連続してログインに失敗した場合、アカウントは 5 分間ロックされます。再度ログインを試みる前に待機する必要があります。

始める前に

最初は、**admin** ユーザー名を使用してのみ Device Manager にログインできます。ただし、Device Manager および Threat Defense ユーザーアクセスの管理（999 ページ）に説明されているように、外部 AAA サーバに定義されている追加ユーザの認証は設定できます。

アクティブなログインは一度に5つまで可能です。これには、デバイスマネージャにログインしているユーザーと、有効期限の切れていないAPIトークンなどのアクティブなAPIセッションが含まれます。この制限を超えると、最も古いセッション（デバイスマネージャログインまたはAPIトークン）が期限切れになり、新しいセッションが許可されます。これらの制限は、SSHセッションには適用されません。

手順

ステップ1 ブラウザを使用して、システムのホームページ（https://ftd.example.com など）を開きます。

次のいずれかのアドレス使用できます。設定済みのものであれば、IPv4 アドレス、IPv6 アドレス、または DNS 名を使用できます。

- 管理アドレス。（ほとんどのプラットフォームの）デフォルトでは、管理インターフェイスはDHCPクライアントであるため、IPアドレスはDHCPサーバーによって異なります。
- HTTPS アクセス用に開いたデータ インターフェイスのアドレス。（ほとんどのプラットフォームの）デフォルトでは、「内部」インターフェイスで HTTPS アクセスが許可されているため、デフォルトの内部アドレス 192.168.95.1 に接続できます。使用モデルの内部 IP アドレスの詳細については、初期設定前のデフォルト設定 （28 ページ）を参照してください。

  HTTPSデータポートを変更した場合は、URLにカスタムポートを含める必要があります。たとえば、ポートを 4443 に変更した場合は、https://ftd.example.com:4443 のようなURLにします。

ヒント ブラウザがサーバー証明書を認識するように設定されていない場合、信頼できない証明書に関する警告が表示されます。証明書を例外として受け入れるか、または信頼できるルート証明書ストアの証明書を受け入れます。

ステップ2 （ローカルユーザーおよびRADIUSのみ）デバイスに定義されているユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

事前定義されたユーザであるユーザ名 **admin** を使用できます。デフォルトのadminパスワードはAdmin123です。AWSでは、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]**>**[ユーザーデータ（User Data）]**）していなければ、デフォルトの管理者パスワードは AWS のインスタンス ID です。

セッションは非アクティブの状態が 30 分間続くと期限切れになり、再度ログインするように求められます。ページの右上にある[ユーザー（user）]アイコンのドロップダウンリストから[ログアウト（Log Out）] を選択するとログアウトできます。

ステップ3 （SAML サーバーのみ）[ログイン（Login）] ボタンの横にある [シングルサインオン（SSO）（Single-Sign On (SSO)）] リンクをクリックします。

これにより、ログイン用の SAML サーバーに移動します。ログイン情報を入力しないでください。リンクをクリックするだけです。ローカルのログイン情報を入力して[ログイン（Login）]をクリックすると、ローカルデータベースを使用してログインします。

SAML サーバーのログインページで、通常どおりにログインします。ログインに共通アクセスカード（CAC）を使用する場合は、リンクをクリックして証明書を使用してサインインします。デバイスマネージャは、CAC 認証を直接処理しません。

CLI（コマンドライン インターフェイス）へのログイン

コマンドライン インターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。

CLI にログインするには、次のいずれかを実行します。

- デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC を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、デバイスのハードウェア ガイドを参照してください。

（注） Firepower および Secure Firewall デバイスモデルでは、コンソールポートの CLI は Secure Firewall eXtensible オペレーティングシステム（FXOS）です。一部のデバイスモデルでは、**connect ftd** コマンドを使用して 脅威に対する防御 CLI にアクセスできます。Firepower 4100/9300 の場合は、「アプリケーションのコンソールへの接続 （230ページ）」を参照してください。FXOS CLIはシャーシ レベルのトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには 脅威に対する防御 CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

- Threat Defense Virtual の場合は、仮想コンソールを開きます。
- SSH クライアントを使用して、管理 IP アドレスに接続します。 SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます（管理アクセス リストの設定 （924 ページ）を参照）。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。**admin** ユーザ名または別の CLI ユーザアカウントを使用してログインします。デフォルトの admin パスワードは Admin123 です。AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザーデータ（User Data）]**）していなければ、 Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。

ヒント

- ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法の情報については、『Cisco Firepower Threat Defense コマンド リファレンス』（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。
- **configure user add** コマンドを使用して、CLI にログインできるローカルユーザアカウントを作成できます。ただし、これらのユーザは CLI のみにログインできます。Device Manager Web インターフェイスにはログインできません。
- 外部サーバで SSH アクセス用のユーザアカウントを作成できます。SSH アクセス用の外部認証の設定については、Threat Defense CLI（SSH）ユーザー用の外部認証（AAA）設定（1001 ページ）を参照してください。

パスワードの変更

パスワードは定期的に変更する必要があります。次の手順では、Device Manager にログインしているときにパスワードを変更する方法について説明します。

（注） CLI にログインしている場合は、**configure password** コマンドを使用してパスワードを変更できます。別の CLI ユーザーのパスワードを変更するには、**configure user password** *username* コマンドを使用します。

始める前に

この手順は、ローカルユーザにのみ適用されます。ユーザアカウントが外部 AAA サーバで定義されている場合、そのサーバでパスワードを変更する必要があります。

手順

ステップ 1 メニューの右上にある [ユーザー（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

ステップ 2 [パスワード（Password）] タブをクリックします。

ステップ 3 現在のパスワードを入力します。

ステップ 4 新しいパスワードを入力して確認します。

[生成（Generate）] をクリックすると、ランダムな 16 文字のパスワードが生成されます。[パスワードの表示（Show Password）]（）ボタンをクリックして、マスクされていないパス

ワードを表示します。次に、[クリップボードにコピー（Copy To Clipboard）] リンクをクリックして、[確認（Confirm）] フィールドにパスワードを貼り付けます。

このページには、パスワードの最小要件が含まれています。これらの最小要件は変更できません。パスワードは次のとおりです。

- 8 ～ 128 文字である
- 小文字と大文字がそれぞれ 1 文字以上含まれている
- 数字が 1 桁以上含まれている
- 特殊文字が 1 文字以上含まれている
- 同じ文字の繰り返しが含まれていない

ステップ 5 [変更（Change）] をクリックします。

ユーザー プロファイルの設定

ユーザー インターフェイスの設定を行い、パスワードを変更できます。

手順

ステップ 1 メニューの右上にある [ユーザー（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

ステップ 2 [プロファイル（Profile）] タブで次の設定を行い、[保存（Save）] をクリックします。

- [スケジュールするタスクのタイム ゾーン（Time Zone for Scheduling Tasks）]：バックアップや更新などのタスクのスケジュールに使用するタイム ゾーンを選択します。別のゾーンを設定すると、ブラウザのタイム ゾーンはダッシュボードやイベントに使用されます。
- [カラー テーマ（Color Theme）]：ユーザー インターフェイスで使用するカラー テーマを選択します。

ステップ 3 [パスワード（Password）] タブで新しいパスワードを入力し、[変更（Change）] をクリックします。

システムの設定

ネットワークでシステムが正しく機能するためには、初期設定を完了する必要があります。展開を成功させるには、ケーブルを正しく接続し、デバイスをネットワークに挿入し、インター

ネットや他のアップストリームルータに接続するために必要なアドレスを設定する必要があります。次の手順で、このプロセスについて説明します。

始める前に

初期設定を開始する前に、デバイスにはいくつかのデフォルト設定が含まれています。詳細は、初期設定前のデフォルト設定 （28 ページ）を参照してください。

手順

ステップ 1 インターフェイスの接続 （12 ページ）

ステップ 2 セットアップウィザードを使用した初期設定の完了 （24 ページ）

設定の結果の詳細については、初期セットアップ後の設定 （31 ページ）を参照してください。

インターフェイスの接続

デフォルト設定では、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの前提に基づいてネットワーク ケーブルをインターフェイスに接続すると、初期設定の実行が容易になります。

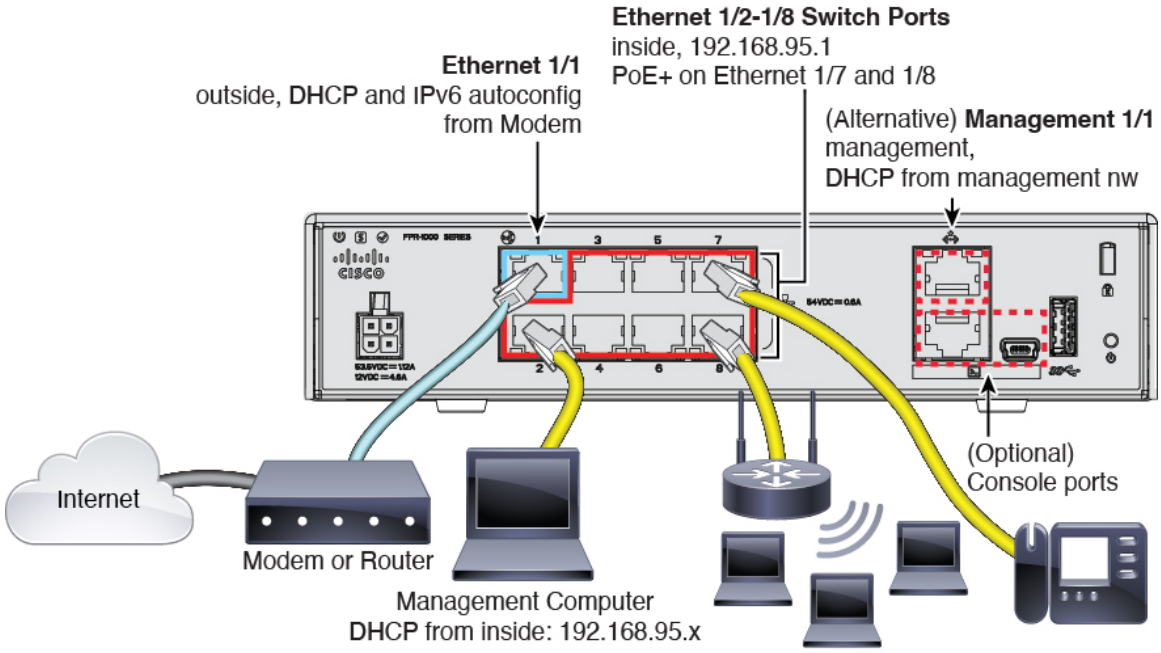
大半のモデルのデフォルト設定は、管理コンピュータを内部インターフェイスに接続するように設計されています。あるいは、管理ポートに直接ワークステーションを接続することもできます。インターフェイスはさまざまなネットワーク上にあるため、内部インターフェイスと管理ポートを同じネットワークに接続しようとしないでください。

内部インターフェイスを、アクティブなDHCPサーバを持つネットワークに接続しないでください。内部インターフェイスですでに稼働中の DHCP サーバと競合してしまいます。ネットワークに別の DHCP サーバを使用する必要がある場合は、初期設定の後に不要な DHCP サーバを無効にします。

次に、デバイスを設定するために内部インターフェイスを使用するときの、このトポロジでのシステムの配線方法を示します。

Firepower 1010 のケーブル配線

図 *1 : Firepower 1010* のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
  - イーサネット 1/2 ー 1/8：管理コンピュータを内部スイッチポートのいずれかに直接接続します（イーサネット 1/2 ー 1/8）。内部にはデフォルトの IP アドレス（192.168.95.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
  - 管理 1/1：管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバーが含まれていることを確認してください。

    Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）CLI での管理ネットワーク設定の変更 （22 ページ）」を参照してください。

  後で、他のインターフェイスから管理アクセスを設定できます。
- 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。

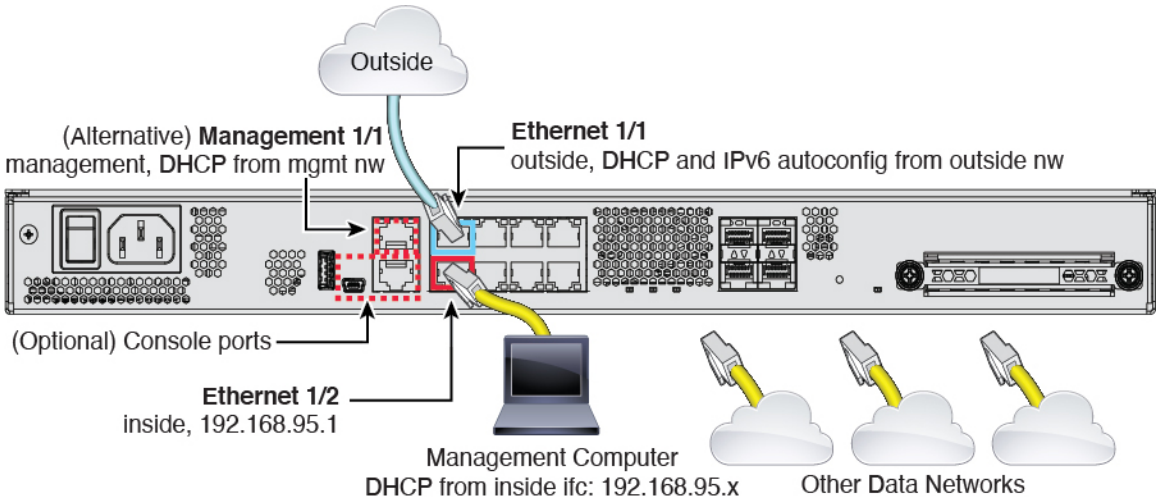
  デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 内部デバイスを残りのスイッチ ポート（Ethernet 1/2 ～ 1/8）に接続します。

  Ethernet 1/7 および 1/8 は Power over Ethernet+（PoE+）ポートです。

（注） PoE は Firepower 1010E ではサポートされていません。

Firepower 1100 のケーブル配線

図 *2 : Firepower 1100* のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
  - Ethernet 1/2：初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。イーサネット 1/2 にはデフォルトの IP アドレス（192.168.95.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
  - Management 1/1（ラベル「MGMT」）：管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバーが含まれていることを確認してください。

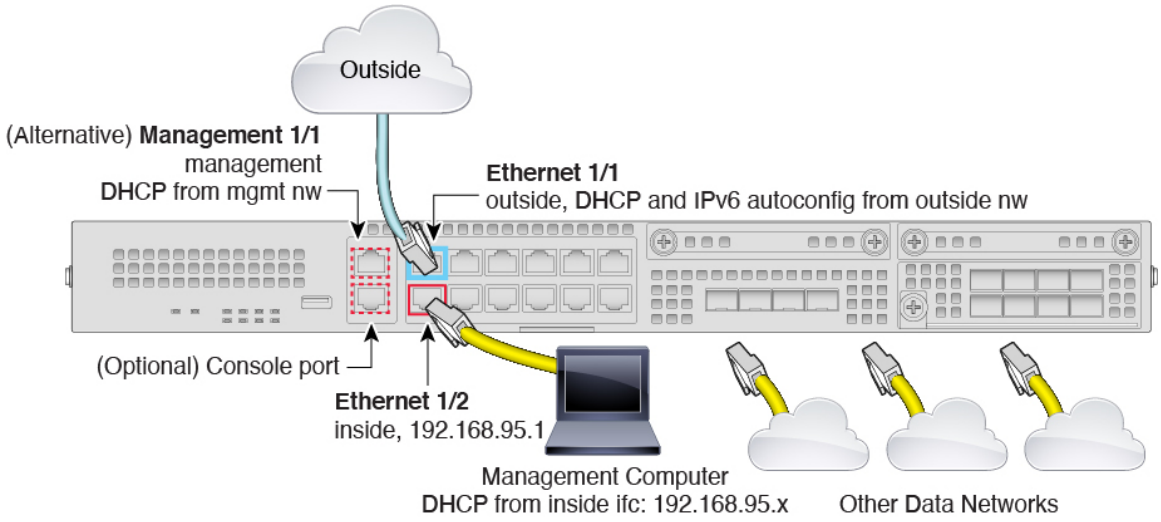
    Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）CLI での管理ネットワーク設定の変更 （22 ページ）」を参照してください。

  後で、他のインターフェイスから管理アクセスを設定できます。
- 外部ネットワークを Ethernet 1/1 インターフェイス（ラベル「WAN」）に接続します。

  デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 残りのインターフェイスに他のネットワークを接続します。

Firepower 2100 のケーブル配線

図 *3 : Firepower 2100* のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
  - Ethernet 1/2：初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。イーサネット 1/2 にはデフォルトの IP アドレス（192.168.95.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
  - Management 1/1（ラベル「MGMT」）：管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバーが含まれていることを確認してください。

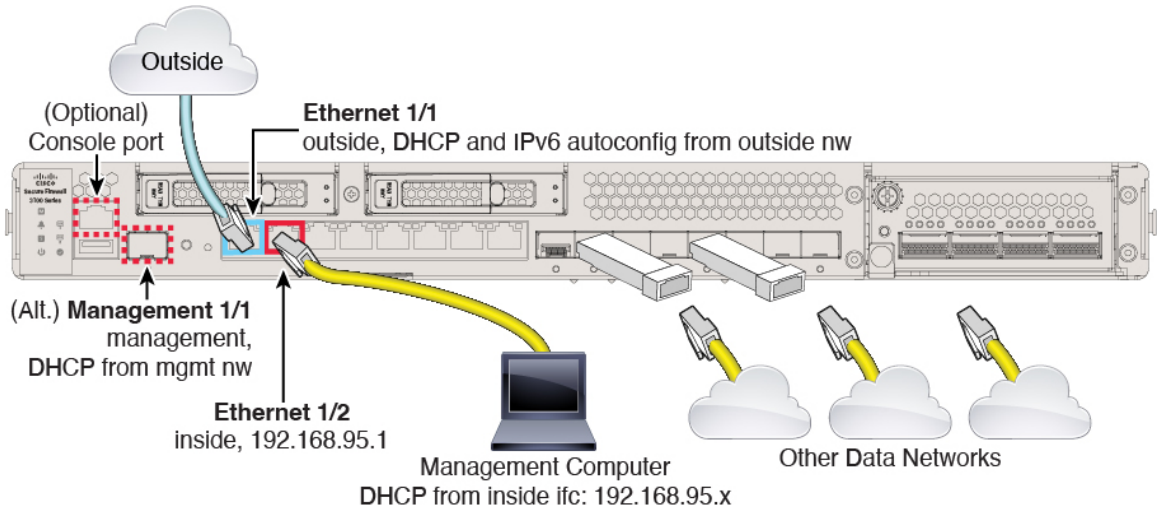
    Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）CLI での管理ネットワーク設定の変更 （22 ページ）」を参照してください。

  後で、他のインターフェイスから管理アクセスを設定できます。
- 外部ネットワークを Ethernet 1/1 インターフェイス（ラベル「WAN」）に接続します。

  デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 残りのインターフェイスに他のネットワークを接続します。

Cisco Secure Firewall 3100 のケーブル配線

図 *4 : Cisco Secure Firewall 3100* のケーブル接続



Management 1/1 または Ethernet 1/2 のいずれかでThreat Defense デバイスを管理します。デフォルト設定でも、Ethernet1/1 を外部として設定します。

- 管理コンピュータを次のいずれかのインターフェイスに接続します。
  - Ethernet 1/2：初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。Ethernet 1/2 にはデフォルトの IP アドレス（192.168.95.1）があり、（管理コンピュータを含む）クライアントに IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワークの設定と競合しないようにしてください。
  - Management 1/1：Management 1/1 を管理ネットワークに接続し、管理コンピュータが管理ネットワーク上にあるか、またはアクセスできることを確認します。Management 1/1 は、管理ネットワーク上の DHCP サーバーから IP アドレスを取得します。このインターフェイスを使用する場合は、管理コンピュータから IP アドレスに接続できるように、ファイアウォールに割り当てられる IP アドレスを決定する必要があります。

    Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）CLI での管理ネットワーク設定の変更 （22 ページ）」を参照してください。

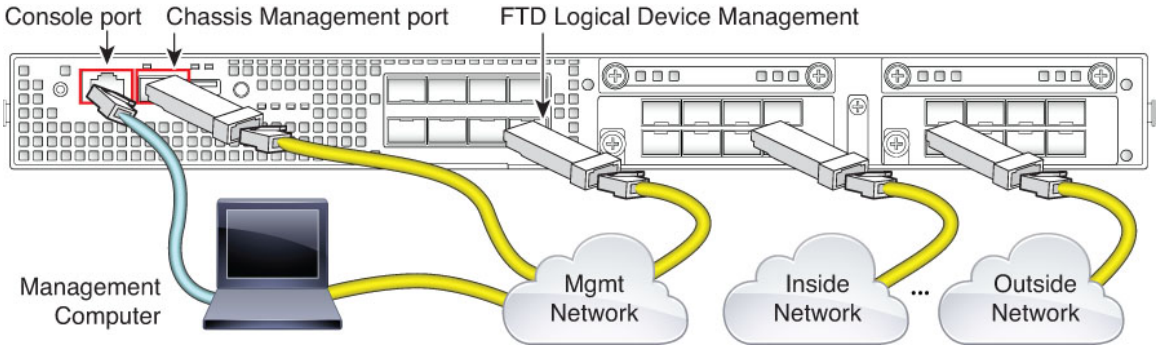
（注） Management 1/1 は、SFP モジュールを必要とする 10 Gb 光ファイバインターフェイスです。

- 外部ネットワークを Ethernet1/1 インターフェイスに接続します。

デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。

- 残りのインターフェイスに他のネットワークを接続します。

Firepower 4100 のケーブル配線



論理デバイスの管理インターフェイスで 脅威に対する防御 の初期設定を実行します。後で、任意のデータ インターフェイスから管理を有効にすることができます。脅威に対する防御 デバイスでは、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、デバイスの展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で Device Manager でその設定が行えます。

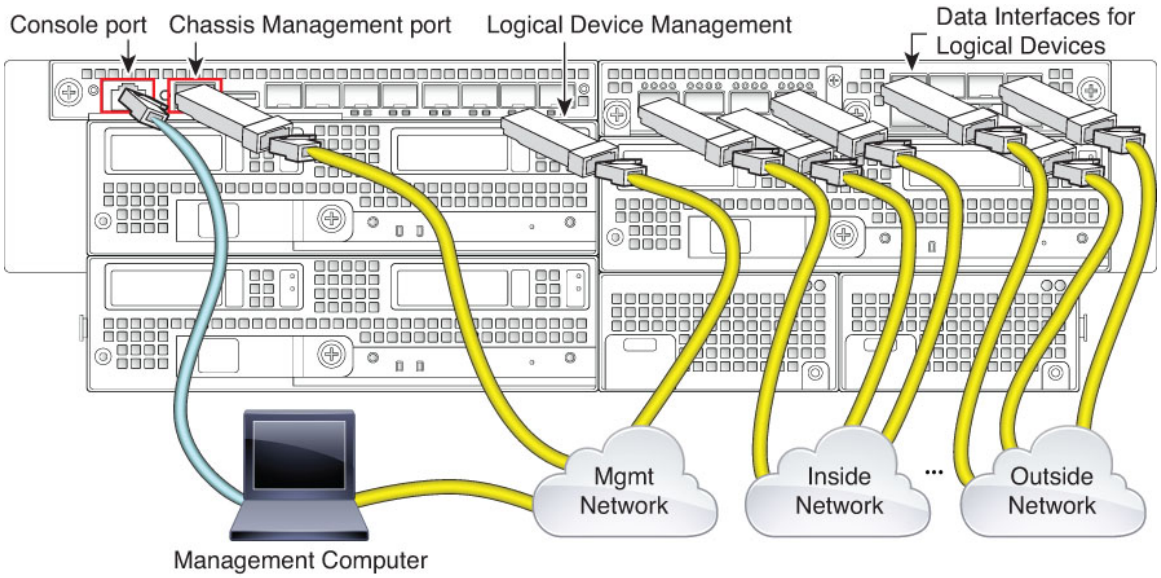
シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- コンソールポート：管理コンピュータをコンソールポートに接続して、シャーシの初期設定を実行します。Firepower 4100 には RS-232–to–RJ-45 シリアルコンソールケーブルが含まれています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。
- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- Threat Defense 論理デバイス管理インターフェイス：FXOS 管理用に予約されているシャーシ管理ポートを除き、シャーシ上の任意のインターフェイスを選択できます。
- データインターフェイス：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、EtherChannel、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。

  高可用性の場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。

（注） コンソール ポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『Hardware Installation Guide』を参照してください。

Firepower 9300 のケーブル配線



論理デバイスの管理インターフェイスで 脅威に対する防御 の初期設定を実行します。後で、任意のデータ インターフェイスから管理を有効にすることができます。脅威に対する防御 デバイスでは、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、デバイスの展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で Device Manager でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- コンソールポート：管理コンピュータをコンソールポートに接続して、シャーシの初期設定を実行します。Firepower 9300 には RS-232–to–RJ-45 シリアルコンソールケーブルが含まれています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。
- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- 論理デバイス管理インターフェイス：1 つ以上のインターフェイスを使用して論理デバイスを管理します。シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。管理インターフェイスは論理デバイス間で共有できます。また、論理デバイスごとに別のインターフェ

イスを使用することもできます。通常は、管理インターフェイスをすべての論理デバイスと共有します。または、別個のインターフェイスを使用する場合は、それらを単一の管理ネットワークに配置します。ただし、正確なネットワーク要件は場合によって異なります。

- データインターフェイス：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、EtherChannel、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。ネットワークのニーズに応じて、複数の論理デバイスを同じネットワークまたは異なるネットワークに配線できます。別の論理デバイスに到達するために、すべてのトラフィックが 1 つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。

  高可用性の場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。

（注） コンソール ポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『Hardware Installation Guide』を参照してください。

Threat Defense Virtual の仮想ケーブル接続

Threat Defense Virtual をインストールするには、http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html で、ご使用の仮想プラットフォームに対応したクイックスタートガイドを参照してください。Device Manager は、次の仮想プラットフォーム（VMware、KVM、Microsoft Azure、Amazon Web Services（AWS））でサポートされています。

Threat Defense Virtual のデフォルト設定では、管理インターフェイスと内部インターフェイスは同じサブネットに配置されます。スマートライセンスを使用する場合やシステムデータベースへの更新プログラムを取得する場合は、管理インターフェイスにインターネット接続が必要です。

そのため、デフォルト設定は、Management 0/0 と GigabitEthernet 0/1（内部）の両方を仮想スイッチ上の同じネットワークに接続できるように設計されています。デフォルトの管理アドレスは、内部 IP アドレスをゲートウェイとして使用します。したがって、管理インターフェイスは内部インターフェイスを介してルーティングし、その後、外部インターフェイスを介してルーティングして、インターネットに到達します。

また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに Management 0/0 を接続するオプションもあります。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

Threat Defense の物理インターフェイスへの VMware ネットワークアダプタとインターフェイスのマッピング方法

VMware Threat Defense Virtual デバイス用に最大 10 のインターフェイスを設定できます。少なくとも 4 つのインターフェイスを設定する必要があります。

Management0-0 送信元ネットワークが、インターネットにアクセスできる VM ネットワークに関連付けられていることを確認します。これは、システムが Cisco Smart Software Manager にアクセスしてシステムデータベース更新をダウンロードすることを可能にするために必要です。

OVF をインストールするときにネットワークを割り当てます。インターフェイスを設定しておけば、後でVMwareクライアントを介して仮想ネットワークを変更できます。ただし、新しいインターフェイスを追加する必要がある場合は、必ずリストの最後にインターフェイスを追加してください。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤った順番になります。

次の表は、VMware ネットワーク アダプタおよび送信元インターフェイスの、Threat Defense Virtual の物理インターフェイス名へのマッピングを示しています。追加のインターフェイスについては、命名は同じパターンに従い、関連する数字を 1 つずつ増やします。すべての追加インターフェイスはデータ インターフェイスです。仮想ネットワークの仮想マシンへの割り当ての詳細については、VMware のオンライン ヘルプを参照してください。

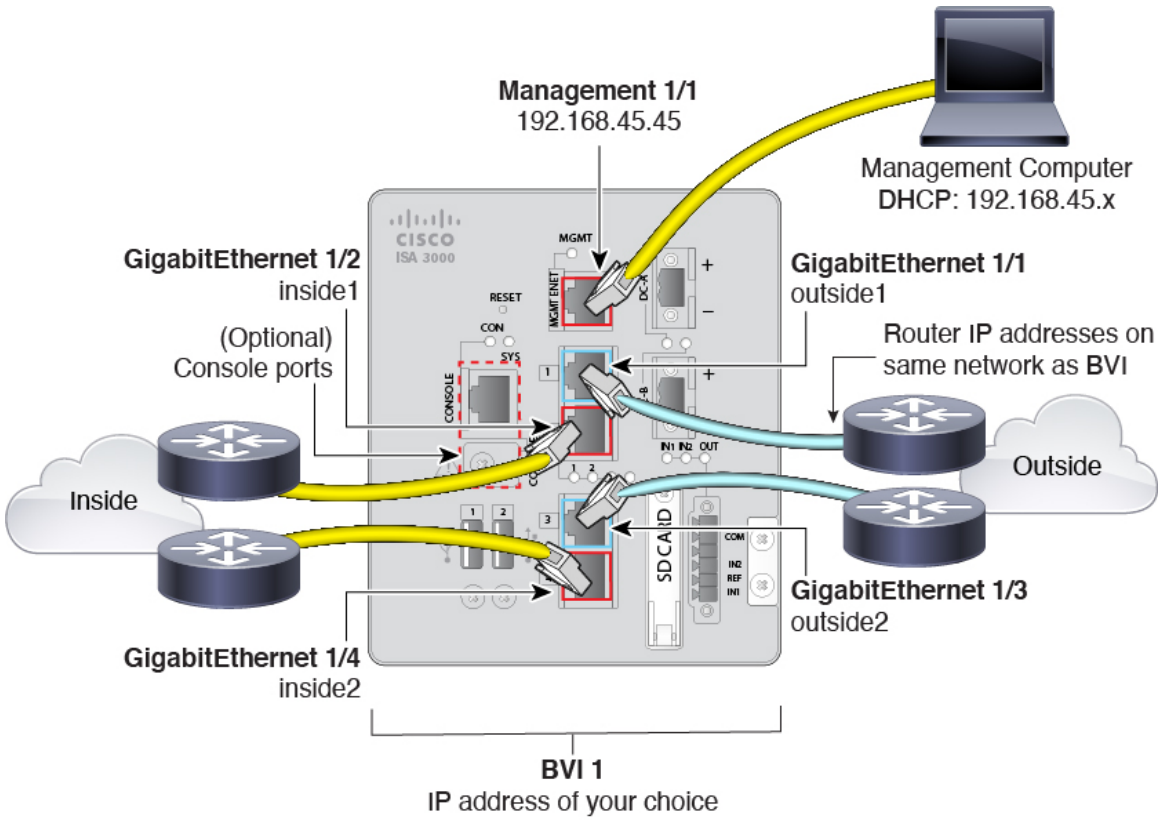
表 *1*: 送信元から宛先ネットワークへのマッピング

ネットワーク アダプタ	送信元ネットワーク	宛先ネットワーク（物理インターフェイス名）	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	内部使用のため予約済み。	内部使用のため予約済み。	内部使用のため予約済み。
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部データ
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データ トラフィック
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データ トラフィック
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データ トラフィック
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データ トラフィック

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク（物理インターフェイス名）	機能
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データ トラフィック
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データ トラフィック

ISA 3000 のケーブル配線

図 *5 : ISA 3000*



- GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。

  これらのインターフェイスによってハードウェアバイパスペアが形成されます。

- GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

  銅線ポートを備えたモデルの場合は、これらのインターフェイスによってハードウェアバイパスペアが形成されます。ファイバはハードウェアバイパスをサポートしていません。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパス

を提供します。これら4つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

- Management 1/1 を管理コンピュータ（またはネットワーク）に接続します。

  Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）CLI での管理ネットワーク設定の変更 （22 ページ）」を参照してください。

（任意）CLI での管理ネットワーク設定の変更

デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。管理インターフェイスのみを設定できます。内部インターフェイスや外部インターフェイスは設定できません。これらは後で GUI を使用して設定できます。

（注） 展開時に IP アドレスを手動で設定するため、Firepower 4100/9300 にこの手順を使用する必要はありません。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップスクリプトを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

手順

ステップ 1 Threat Defense コンソール ポートに接続します。詳細については、CLI（コマンドライン インターフェイス）へのログイン （9 ページ）を参照してください。

ステップ 2 ユーザ名 **admin** を使用してログインします。

デフォルトの admin パスワードは Admin123 です。AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザーデータ（User Data）]**）していなければ、 Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。

ステップ 3 Threat Defense に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意するように求められます。その後、CLI セットアップスクリプトが表示されます。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [管理インターフェイスの IPv4 デフォルトゲートウェイを入力します（Enter the IPv4 default gateway for the management interface）]：手動 IP アドレスを設定した場合は、「**data-interfaces**」またはゲートウェイルータの IP アドレスのいずれかを入力します。**data-interfaces** を設定すると、アウトバウンド管理トラフィックがバックプレーン経由で送信され、データインターフェイスが終了します。この設定は、インターネットにアクセスできる個別の管理ネットワークがない場合に役立ちます。管理インターフェイスから発信されるトラフィックには、インターネットアクセスを必要とするライセンス登録とデータベースの更新が含まれます。**data-interfaces** を使用する場合、管理ネットワークに直接接続していれば管理インターフェイスで Device Manager（または SSH）を引き続き使用できますが、特定のネットワークまたはホストのリモート管理の場合は、**configure network static-routes** コマンドを使用して静的ルートを追加する必要があります。データインターフェイスでの Device Manager の管理は、この設定の影響を受けないことに注意してください。DHCP を使用する場合、システムは DHCP によって提供されるゲートウェイを使用します。DHCP がゲートウェイを提供しない場合は、フォールバックメソッドとして **data-interfaces** を使用します。
- [ネットワーク情報が変更された場合は再接続が必要になります（If your networking information has changed, you will need to reconnect）]：SSH でデフォルトの IP アドレスに接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：または Device Manager を使用するには [はい（yes）] を入力します。[いいえ（no）] と応えると、Management Center デバイスの管理にはオンプレミスまたはクラウド配信を使用することになります。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes
```

>

ステップ 4 新しい管理 IP アドレスで Device Manager にログインしてください。

セットアップウィザードを使用した初期設定の完了

Device Manager に初めてログインする際に、デバイス セットアップ ウィザードを使用してシステムの初期設定を完了します。

ハイ アベイラビリティ設定でデバイスを使用する予定の場合は、2 台の装置でのハイ アベイラビリティの準備 （248 ページ）を参照してください。

（注） Firepower 4100/9300 と ISA 3000 は、セットアップウィザードをサポートしていないため、この手順はこれらのモデルには適用されません。Firepower 4100/9300 の場合、シャーシから論理デバイスを展開するときにすべての初期設定が行われます。ISA 3000 の場合、出荷前に特殊なデフォルト設定が適用されます。

始める前に

データインターフェイスがゲートウェイ デバイス（たとえば、ケーブルモデムやルータなど）に接続されていることを確認します。エッジの導入では、これはインターネット向けのゲートウェイになります。データセンター導入の場合は、これがバックボーン ルータになります。使用モデルのデフォルトの「外部」インターフェイスを使用します（インターフェイスの接続（12 ページ）および初期設定前のデフォルト設定 （28 ページ）を参照）。

以上の確認が済んだら、管理コンピュータをハードウェアモデルの「inside」インターフェイスに接続します。または、管理インターフェイスに接続することもできます。Threat Defense Virtual については、管理 IP アドレスに接続できることを確認するだけで十分です

（管理 IP アドレスからインターネットへの接続が必要な Threat Defense Virtual を除く）。管理インターフェイスをネットワークに接続する必要はありません。デフォルトでは、インターネットに接続するデータインターフェイス（通常、外部インターフェイス）を通じてシステムのライセンシングとデータベースおよびその他の更新が取得されます。独立した管理ネットワークを使用する場合は、Management インターフェイスをネットワークに接続し、初期セットアップ完了後に独立した管理ゲートウェイを設定することもできます。

デフォルトの IP アドレスにアクセスできない場合に管理インターフェイスのネットワーク設定を変更するには、「（任意）CLI での管理ネットワーク設定の変更 （22 ページ）」を参照してください。

手順

ステップ 1 Device Manager にログインします。

a) CLI での初期設定を完了していない場合は、**https://***ip-address* で Device Manager を開きます。このアドレスは次のいずれかになります。

- 内部インターフェイスに接続されている場合：**https://192.168.95.1**
- （Threat Defense Virtual の場合は必須） 管理インターフェイスに接続している場合：**https://192.168.45.45**。
- （他のすべてのモデル）管理インターフェイスに接続している場合：**https://***dhcp_client_ip*

b) ユーザ名 **admin** を使用してログインします。デフォルトの admin パスワードは Admin123 です。AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザーデータ（User Data）]**）していなければ、 Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。。

ステップ 2 これがシステムへの初めてのログインであり、CLI セットアップウィザードを使用していない場合、エンドユーザライセンス契約を読んで承認し、管理パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 3 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

注意 [次へ（Next）] をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

外部インターフェイス

- [IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。デフォルトの内部アドレスと同じサブネットに（静的に、または DHCP を介して）IP アドレスを設定しないでください（初期設定前のデフォルト設定 （28 ページ）を参照）。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。物理インターフェイスの設定 （293 ページ）を参照してください。
- [IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

[管理インターフェイス（Management Interface）]

- [DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは、OpenDNS パブリック DNS サーバ、または DHCP サーバから取得した DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。ISP は、特定の DNS サーバを使用するよう要求する場合があります。ウィザードを完了した後に DNS 解決が機能しない場合は、管理インターフェイスのDNSのトラブルシューティング（1014ページ）を参照してください。
- [ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

ステップ 4 システム時刻を設定し、[次へ（Next）] をクリックします。

- [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
- [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ 5 システムのスマートライセンスを設定します。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、デバイスを登録するオプションを選択し、リンクをクリックして Smart Software Manager アカウントにログインしてから、新しいトークンを生成して、そのトークンを編集ボックスにコピーします。また、サービスリージョンを選択し、Cisco Success Network に使用状況データを送信するかどうかを決定する必要もあります。画面上のテキストは、これらの設定について詳しく説明しています。

デバイスをまだ登録しない場合は、評価モードオプションを選択します。評価期間は最大 90 日です。後でデバイスを登録してスマートライセンスを取得する場合は、[デバイス（Device）] をクリックしてから、[Smart Licenses] グループでリンクをクリックします。

ステップ 6 [終了（Finish）] をクリックします。

次のタスク

- オプションライセンスでカバーされている機能（カテゴリベースのURLフィルタリング、侵入インスペクション、マルウェア対策など）を使用する場合は、必要なライセンスを有効にします。オプションライセンスの有効化または無効化（109ページ）を参照してください。
- 他のデータインターフェイスを個々のネットワークに接続して、それらのインターフェイスを設定します。インターフェイスの設定の詳細については、サブネットを追加する方法（83 ページ）およびインターフェイス（287 ページ）を参照してください。

- 内部インターフェイスを使用してデバイスを管理する場合、内部インターフェイスで CLI セッションを開くには、内部インターフェイスで SSH 接続を開始します。管理アクセスリストの設定 （924 ページ） を参照してください。
- 製品の使用方法については、使用例で学習してください。ベストプラクティス：Threat Defense の使用例 （49 ページ） を参照してください。

外部インターフェイスの IP アドレスを取得できない場合の対処方法

デフォルトのデバイス設定には内部インターフェイスのスタティック IPv4 アドレスが含まれています。初期デバイス セットアップ ウィザードを使用してこのアドレスを変更することはできません。ただし、後で変更することはできます。

デフォルトの内部 IP アドレスが、デバイスに接続されている他のネットワークと競合する可能性があります。これは特に、外部インターフェイスで DHCP を使用してインターネット サービス プロバイダー（ISP）からアドレスを取得する場合に該当します。一部の ISP は、内部ネットワークと同じサブネットをアドレス プールとして使用しています。同じサブネットのアドレスを持つ 2 つのデータ インターフェイスを持つことはできないため、ISP からの競合するアドレスを外部インターフェイスに設定することはできません。

内部スタティック IP アドレスと外部インターフェイスの DHCP が提供するアドレスの間に競合がある場合は、接続図には、外部インターフェイスは管理上動作しているが IPv4 アドレスが割り当てられていないことが示されます。

この場合セットアップ ウィザードは正常に完了し、デフォルト NAT、アクセス、およびその他のポリシーや設定がすべて設定されます。競合を解消するには、次の手順に従います。

始める前に

ISP に正常に接続できることを確認します。サブネット競合がある場合外部インターフェイスのアドレスを取得できませんが、単に ISP への接続がない場合にも外部インターフェイスのアドレスを取得できません。

手順

ステップ 1 [デバイス（Device）] をクリックして、[インターフェイス（Interfaces）] サマリーのリンクをクリックします。

ステップ 2 内部インターフェイス行の [操作（Actions）] カラムにカーソルを置き、[編集（edit）] アイコン（  ）をクリックします。

ステップ 3 [IPv4アドレス（IPv4 Address）] タブで、一意のサブネットのスタティック アドレス（192.168.2.1/24、192.168.46.1/24 など）を入力します。デフォルトの管理アドレスは 192.168.45.45/24 であるため、このサブネットは使用しないでください。

また、内部ネットワークですでに DHCP サーバが実行されている場合は、DHCP を使用してアドレスを取得することもできます。ただし最初に、[このインターフェイスにDHCPサーバーを

定義済み（DHCP SERVER IS DEFINED FOR THIS INTERFACE）] グループで [削除（Delete）] をクリックして、インターフェイスから DHCP サーバーを削除する必要があります。

ステップ 4 [このインターフェイスにDHCPサーバーを定義済み（DHCP SERVER IS DEFINED FOR THIS INTERFACE）] 領域で [編集（Edit）] をクリックして、DHCP プールを新しいサブネットの範囲に変更します（たとえば、192.168.2.5-192.168.2.254）。

ステップ 5 [OK] をクリックしてインターフェイスの変更を保存します。

ステップ 6 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

ステップ 7 [今すぐ展開（Deploy Now）] をクリックします。

展開が完了すると、外部インターフェイスに IP アドレスが割り当てられていることが接続グラフィックで示されるはずです。内部ネットワークのクライアントを使用して、インターネットまたはその他のアップストリーム ネットワークに接続できることを確認します。

初期設定前のデフォルト設定

ローカルマネージャ（Device Manager ）を使用して 脅威に対する防御 デバイスの初期設定を行う前、デバイスには次のデフォルト設定が含まれています。

多数のモデルにおいて、この設定では、デバイスマネージャを内部インターフェイス経由で開き（通常、コンピュータをインターフェイスに直接接続する）、内部インターフェイス上に定義された DHCP サーバを使用してコンピュータに IP アドレスを提供することを前提としています。または、コンピュータを管理インターフェイスに接続し、DHCPを使用してアドレスを取得できます。ただし、一部のモデルではデフォルト設定や管理要件が異なります。詳細については、次の表を参照してください。

（注） ウィザードを使用してセットアップを実行する前に、CLI セットアップ（（任意）CLI での管理ネットワーク設定の変更 （22 ページ））を使用してこれらの設定の多くを事前に設定できます。

デフォルト設定

設定	デフォルト	初期設定時に変更できるか
管理者ユーザのパスワード	Admin123 Firepower 4100/9300：論理デバイスを展開するときのパスワードを設定します。 AWS：初期展開時にユーザデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザデータ（User Data）]**）していなければ、デフォルトは AWS のインスタンス ID です。	可。デフォルトパスワードを変更する必要があります。
管理 IP アドレス	DHCP 経由で取得。 Threat Defense Virtual192.168.45.45 Firepower 4100/9300：論理デバイスの展開時に管理 IP アドレスを設定します。	番号 Firepower 4100/9300の場合：可。
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。このゲートウェイは、from-the-device（デバイスからの出力）トラフィックのみで機能します。デバイスがDHCPサーバからデフォルトゲートウェイを受信した場合は、そのゲートウェイが使用されます。 Firepower 4100/9300：論理デバイスの展開時にゲートウェイIPアドレスを設定します。 ISA 3000：192.168.45.1。 Threat Defense Virtual192.168.45.1	番号 Firepower 4100/9300の場合：可。
管理インターフェイスの DNS サーバ	OpenDNS パブリック DNS サーバ、IPv4：208.67.220.220 と 208.67.222.222、IPv6：2620:119:35::35。DHCP から取得した DNS サーバは使用されません。 Firepower 4100/9300：論理デバイスの展開時に DNS サーバを設定します。	可

設定	デフォルト	初期設定時に変更できるか
内部インターフェイスの IP アドレス	192.168.95.1/24 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：BVI1 IP アドレスは事前に設定されていません。BVI1 にはすべての内部インターフェイスと外部インターフェイスが含まれます。 Threat Defense Virtual192.168.45.1/24	不可。
内部クライアントの DHCP サーバ	内部インターフェイス上で実行されており、アドレスプールは 192.168.95.5 ～ 192.168.95.254 です。 Firepower 4100/9300: No DHCP server enabled. ISA 3000: DHCP サーバが有効になっていません。 Threat Defense Virtual：内部インターフェイスのアドレスプールは 192.168.45.46 ～ 192.168.45.254 です。	不可。
内部クライアントに対する DHCP 自動設定（自動設定では、WINS サーバおよび DNS サーバ用のアドレスがクライアントに提供）	外部インターフェイスで有効です。	可（ただし間接的）。外部インターフェイスにスタティック IPv4 アドレスを設定した場合、DHCP サーバの自動設定が無効になります。
外部インターフェイスの IP アドレス	IPv4：インターネットサービスプロバイダー（ISP）またはアップストリームルータから DHCP を通して取得されます。 IPv6：自動設定。 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：BVI1 IP アドレスは事前に設定されていません。BVI1 にはすべての内部インターフェイスと外部インターフェイスが含まれます。	可

デバイス モデル別のデフォルト インターフェイス

初期設定時に異なる内部および外部インターフェイスを選択することはできません。設定後にインターフェイスの割り当てを変更するには、インターフェイス設定とDHCP設定を編集します。非交換インターフェイスとして設定するには、ブリッジグループからインターフェイスを削除する必要があります。

Threat Defense デバイス	外部インターフェイス	内部インターフェイス
Firepower 1010	Ethernet1/1	VLAN1 には、物理ファイアウォールインターフェイスである外部インターフェイスを除く他のすべてのスイッチポートが含まれます。
Firepower 1120、1140、1150	Ethernet1/1	Ethernet1/2
Firepower 2100 シリーズ	Ethernet1/1	Ethernet1/2
Secure Firewall 3100 シリーズ	Ethernet1/1	Ethernet1/2
Firepower 4100 シリーズ	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Firepower 9300 appliance	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Threat Defense Virtual	GigabitEthernet 0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 および GigabitEthernet1/3 GigabitEthernet1/1（outside1）と 1/2（inside1）、および GigabitEthernet1/3（outside2）と 1/4（inside2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 すべての内部および外部インターフェイスは、BVI1 の一部です。	GigabitEthernet1/2 および GigabitEthernet1/4

初期セットアップ後の設定

セットアップ ウィザードを完了すると、デバイス設定は次のようになります。この表では、個々の設定項目の値が、ユーザーが明示的に選択したものとなるのか、または他の項目の設定に基づき自動的に定義されたものかを示します。「暗黙的」な設定を検証し、ニーズに合わない場合は編集します。

（注） Firepower 4100/9300 と ISA 3000 は、セットアップ ウィザードをサポートしていません。Firepower 4100/9300 の場合、シャーシから論理デバイスを展開するときにすべての初期設定が行われます。ISA 3000 の場合、出荷前に特殊なデフォルト設定が適用されます。

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
管理者ユーザーのパスワード	任意の入力値	明示的
管理 IP アドレス	DHCP 経由で取得。 Threat Defense Virtual：192.168.45.45 Firepower 4100/9300：論理デバイスの展開時に設定した管理 IP アドレス	デフォルト
管理ゲートウェイ	デバイスのデータ インターフェイス。通常、外部インターフェイスがインターネットへのルートになります。管理ゲートウェイは、from-the-device（デバイスからの出力）トラフィックのみで機能します。デバイスが DHCP サーバからデフォルトゲートウェイを受信した場合は、そのゲートウェイが使用されます。 Firepower 4100/9300：論理デバイスの展開時に設定したゲートウェイ IP アドレス ISA 3000：192.168.45.1 Threat Defense Virtual：192.168.45.1	デフォルト
管理インターフェイスの DNS サーバー	OpenDNS パブリック DNS サーバー、IPv4：208.67.220.220、208.67.222.222、IPv6：2620:119:35::35、またはユーザーの入力値。DHCP から取得した DNS サーバーは使用されません。 Firepower 4100/9300：論理デバイスの展開時に設定した DNS サーバー	明示的
管理ホスト名	**firepower** または任意の入力値 Firepower 4100/9300：論理デバイスの展開時に設定したホスト名。	明示的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
データ インターフェイスを通過する管理アクセス	データ インターフェイスの管理アクセス リスト ルールにより、内部インターフェイスを通過する HTTPS アクセスが許可されます。SSH 接続は許可されません。IPv4 および IPv6 接続はいずれも許可されます。 Firepower 4100/9300: デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。 ISA 3000：デフォルトの管理アクセスルールを持つデータインターフェイスはありません。 Threat Defense Virtual: デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。	暗黙的
システム時間	選択したタイム ゾーンおよび NTP サーバー。 Firepower 4100/9300：システム時刻はシャーシから継承されます。 ISA 3000：Cisco NTP サーバー：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。	明示的
スマート ライセンス	基本ライセンスとともに登録したか、または評価期間を開始したか、いずれか選択した方法。 サブスクリプションライセンスは有効化されていません。スマート ライセンスのページに移動して、スマート ライセンスを有効化してください。	明示的
内部インターフェイスの IP アドレス	192.168.95.1/24 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：なし。BVI1 の IP アドレスは手動で設定する必要があります。 Threat Defense Virtual192.168.45.1/24	デフォルト
内部クライアントの DHCP サーバ	内部インターフェイス上で実行されており、アドレスプールは 192.168.95.5 ～ 192.168.95.254 です。 Firepower 4100/9300: No DHCP server enabled. ISA 3000: DHCP サーバが有効になっていません。 Threat Defense Virtual：内部インターフェイスのアドレスプールは 192.168.45.46 ～ 192.168.45.254 です。	デフォルト

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
内部クライアントに対するDHCP自動設定（自動設定では、WINSサーバおよびDNSサーバ用のアドレスがクライアントに提供）	DHCPを使用して外部インターフェイスのIPv4アドレスを取得している場合、DHCP自動設定は外部インターフェイスに対して有効化されます。 静的アドレッシングを使用している場合は、DHCP自動設定は無効になります。	明示的（ただし間接的）
データ インターフェイスの設定	• Firepower 1010：外部インターフェイス Ethernet1/1 は物理ファイアウォール インターフェイスです。その他すべてのインターフェイスは、有効になっているVLAN1（内部インターフェイス）の一部であるスイッチポートです。これらのポートにエンド ポイントまたはスイッチを接続すると、内部インターフェイスのアドレスを DHCP サーバーから取得できます。 • Firepower 4100/9300：データインターフェイスはすべて無効になります。 • ISA 3000：データインターフェイスはすべて有効になり、同じブリッジグループ（BVI1）の一部になります。GigabitEthernet1/1 および 1/3 は外部インターフェイスで、GigabitEthernet1/2 および 1/4 は内部インターフェイスです。GigabitEthernet1/1（外部 1）と 1/2（内部 1）、およびGigabitEthernet1/3（外部 2）と 1/4（内部 2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 • その他すべてのモデル：外部および内部インターフェイスのみが設定され、有効化されます。他のすべてのデータ インターフェイスは無効になります。	デフォルト
外部の物理インターフェイスおよびIPアドレス	デバイス モデルに基づくデフォルトの外部ポート。初期設定前のデフォルト設定 （28 ページ）を参照してください。 IPアドレスはDHCPおよびIPv6自動設定により取得されるか、入力したスタティックアドレスです（IPv4、IPv6、または両方）。 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：なし。BVI1 の IP アドレスは手動で設定する必要があります。	インターフェイスはデフォルト、 アドレッシングは明示的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
スタティック ルート	外部インターフェイスに対してスタティック IPv4 または IPv6 アドレスを設定すると、スタティックなデフォルトルートも IPv4 または IPv6 用に適宜設定され、このアドレスタイプ用に定義されたゲートウェイをポイントします。DHCP を選択した場合は、デフォルトルートは DHCP サーバーから取得されます。 ネットワーク オブジェクトもこのゲートウェイ、および「any」アドレス（IPv4 の場合は 0.0.0.0/0、IPv6 の場合は ::/0）に合わせて作成されます。	暗黙的
セキュリティ ゾーン	内部インターフェイスを含む **inside_zone**。Firepower 4100/9300 では、このセキュリティゾーンにインターフェイスを手動で追加する必要があります。 外部インターフェイスを含む **outside_zone**。Firepower 4100/9300 では、このゾーンにインターフェイスを手動で追加する必要があります。 （これらのゾーンを編集して他のインターフェイスを追加することも、独自のゾーンを作成することも可能）。	暗黙的
アクセス コントロール ポリシー	inside_zone から outside_zone に送信されるすべてのトラフィックを信頼するルール。これにより、インスペクションなしで、ネットワーク内のユーザーからのすべてのトラフィックを外部に出すことができ、これらの接続のすべてのリターン トラフィックが許可されます。 他のすべてのトラフィックに対するデフォルト アクションは、ブロックです。つまり、外部から開始され、ネットワークに進入しようとするすべてのトラフィックが阻止されます。 Firepower 4100/9300：事前設定されたアクセスルールはありません。 ISA 3000：inside_zone から outside_zone へのすべてのトラフィックを信頼するルール、および outside_zone から inside_zone へのすべてのトラフィックを信頼するルール。トラフィックがブロックされます。デバイスには、inside_zone 内のインターフェイスと outside_zone 内のインターフェイス間のすべてのトラフィックを信頼するルールもあります。これにより、内部にいるユーザー間、および外部にいるユーザー間のすべてのトラフィックが検査なしで許可されます。	暗黙的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
NAT	インターフェイスの動的PATルールは、外部インターフェイスへの任意の IPv4 トラフィックの発信元アドレスを、外部インターフェイスの IP アドレス上の一意のポートに変換します。 補足的な非表示の PAT ルールにより、内部インターフェイスを通過する HTTPS アクセス、およびデータ インターフェイスを経由する管理アドレスのルーティングが有効化されます。これらは NAT テーブルには含まれませんが、CLI で **show nat** コマンドを使用すれば確認できます。 Firepower 4100/9300：NAT は事前に設定されていません。 ISA 3000：NAT は事前設定されていません。	暗黙的

設定の基本

ここでは、デバイスの設定に関する基本的な手順について説明します。

デバイスの設定

Device Manager に最初にログインするとき、基本設定の構成のセットアップウィザードを利用できます。ウィザードを完了したら、次の方法を使用してその他の機能を設定し、デバイス設定を管理します。

各項目が視覚的に区別しにくい場合、ユーザー プロファイルから異なるカラー スキームを選択します。ページ右上の [ユーザー（user）] アイコンのドロップダウン メニューから、[プロファイル（Profile）] を選択します。

手順

ステップ 1 [デバイス（Device）] をクリックして **[デバイス概要（Device Summary）]** に移動します。

ダッシュボードには、有効なインターフェイスやキー設定が設定されているか（緑色）またはまだ設定が必要であるかなど、デバイスの視覚的なステータスが表示されます。詳細については、インターフェイスと管理ステータスの表示 （43 ページ）を参照してください。

ステータス イメージの上にはデバイス モデルの概要、ソフトウェア バージョン、VDB（システムと脆弱性のデータベース）バージョンがあり、前回の侵入ルールは更新されています。この領域には、機能を設定するためのリンクを含め、ハイ アベイラビリティ ステータスも表示されます。ハイ アベイラビリティ（フェールオーバー） （233 ページ）を参照してください。

また、クラウド登録ステータスも表示されます。ここには、クラウド管理を使用している場合、デバイスが登録されているアカウントが表示されます。クラウド サービスの設定 （953 ページ）を参照してください。

イメージの下には設定可能なさまざまな機能のグループがあり、各グループの設定の概要、およびシステム設定を管理するために行うことができるアクションが表示されます。

ステップ 2 設定を行うか、またはアクションを実行するには、各グループのリンクをクリックします。

次に、グループの概要を示します。

- [インターフェイス（Interface）]：管理インターフェイスに加えて、少なくとも 2 つのデータ インターフェイスを設定する必要があります。インターフェイス （287 ページ）を参照してください。
- [ルーティング（Routing）]：ルーティングの設定。デフォルト ルートを定義する必要があります。他のルートは設定に応じて必要になります。ルーティング （383 ページ）を参照してください。
- [更新（Updates）]：地理位置情報、侵入ルールと脆弱性のデータベースの更新、およびシステム ソフトウェアのアップグレード。これらの機能を使用する場合、最新のデータベースの更新情報を確実にするため、定期的な更新スケジュールを設定します。定期的なスケジュールの更新が発生する前に更新をダウンロードする必要がある場合にも、このページにアクセスできます。システム データベースおよびフィードの更新 （971 ページ）を参照してください。
- [システム設定（System Settings）]：このグループにはさまざまな設定が含まれます。デバイスの初期設定時に構成し、その後ほとんど変更しない基本設定などがあります。システム設定 （923 ページ）を参照してください。
- [スマートライセンス（Smart License）]：システム ライセンスの現在のステータスを示します。システムを使用するには、適切なライセンスをインストールする必要があります。一部の機能では追加のライセンスが必要です。システムのライセンス （99 ページ）を参照してください。
- [バックアップと復元（Backup and Restore）]：システム設定をバックアップするか、以前のバックアップを復元します。システムのバックアップと復元 （983 ページ）を参照してください。
- [トラブルシューティング（Troubleshoot）]：Cisco Technical Assistance Center の依頼により、トラブルシューティング ファイルを生成します。トラブルシューティング ファイルの作成 （1020 ページ）を参照してください。
- [サイト間VPN（Site-to-Site VPN）]：このデバイスとリモート デバイス間のサイト間バーチャル プライベート ネットワーク（VPN）接続。サイト間 VPN の管理 （789 ページ）を参照してください。
- [リモートアクセスVPN（Remote Access VPN）]：内部ネットワークへの外部クライアントの接続を可能にするリモートアクセス仮想プライベート ネットワーク（VPN）構成です。リモート アクセス VPN の設定 （838 ページ）を参照してください。

- [詳細設定（Advanced Configuration）]：FlexConfig および Smart CLI を使用して、Device Manager を使用して設定できない機能を設定します。詳細設定 （1029 ページ）を参照してください。
- [デバイス管理（Device Administration）]：監査ログを表示するか、設定のコピーをエクスポートします。監査と変更管理 （990 ページ）を参照してください。

ステップ 3 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

変更は、それらを展開するまでデバイスで有効になりません。変更の展開 （40 ページ） を参照してください。

次のタスク

メイン メニューの [ポリシー（Policies）] をクリックし、システムのセキュリティ ポリシーを設定します。また、これらのポリシーで必要なオブジェクトを設定するには、[オブジェクト（Objects）] をクリックします。

セキュリティ ポリシーの設定

組織のアクセプタブル ユース ポリシーを実装して不正侵入やその他の脅威からネットワークを保護するにはセキュリティ ポリシーを使用します。

手順

ステップ 1 [ポリシー（Policies）] をクリックします。

[セキュリティポリシー（Security Policies）] ページには、システムを経由する接続の一般的な流れ、およびセキュリティ ポリシーが適用される順序が表示されます。

ステップ 2 ポリシーの名前をクリックして構成します。

アクセス制御ポリシーは常に必要ですが、各ポリシータイプを構成する必要はない場合があります。次に、ポリシーの概要を示します。

- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。SSL 復号ポリシーの設定 （546 ページ）を参照してください。
- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを

判定するためにアイデンティティ ポリシーを使用します。アイデンティティ ポリシーの設定 （571 ページ）を参照してください。

- [セキュリティ インテリジェンス（Security Intelligence）]：セキュリティ インテリジェンス ポリシーを使用して、選択されている IP アドレスまたは URL との接続をすぐにドロップします。既知の不正なサイトをブロックすれば、アクセス制御ポリシーでそれらを考慮する必要がなくなります。シスコでは、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。セキュリティ インテリジェンスの設定 （588 ページ）を参照してください。
- [NAT]（ネットワーク アドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。NAT の設定 （691 ページ）を参照してください。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザー グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。アクセス コントロール ポリシーを設定する （612 ページ）を参照してください。
- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。侵入ポリシー （639 ページ）を参照してください。

ステップ 3 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

変更は、それらを展開するまでデバイスで有効になりません。変更の展開 （40 ページ） を参照してください。

ルールまたはオブジェクトを検索

ポリシー ルールまたはオブジェクトのリストで全文検索を使用すると、編集する項目を探すことができます。これは、数百のルールのあるポリシーや長いオブジェクトリストを処理するときに特に便利です。

ルールとオブジェクトで検索を使用する方法は、任意のタイプのポリシー（侵入ポリシーを除く）またはオブジェクトの場合と同様です。[検索（Search）] フィールドに検索する文字列を入力し、Enter を押します。

この文字列は、ルールまたはオブジェクトの任意の部分に存在でき、部分文字列にすることができます。アスタリスク*は、0個以上の文字に一致するワイルドカードとして使用できます。次の文字を含めないでください。検索文字列の一部としてサポートされていません。?~!{}<>:%。次の文字は無視されます。;#&。

文字列は、グループのオブジェクト内に出現することがあります。たとえば、IPアドレスを入力し、そのアドレスを指定するネットワークオブジェクトまたはグループを検索することができます。

完了したら、検索ボックスの右側にある [x] をクリックしてフィルタをクリアします。

変更の展開

ポリシーまたは設定を更新した場合、変更がすぐにはデバイスに適用されません。設定の変更には、次の 2 つの手順を実行します。

1. 変更を行います。
2. 変更を展開します。

この手順により、デバイスを「部分的に設定された」状態で実行することなく、関連する変更のグループ化を行えるようになります。ほとんどの場合、展開には変更だけが含まれます。ただし、必要に応じてシステムは設定全体を再適用し、それがネットワークを中断させる場合があります。さらに、いくつかの変更ではインスペクションエンジンの再起動が必要であり、この再起動中にトラフィックがドロップされます。したがって、発生し得る混乱の影響が最小限になるタイミングで変更を展開するように検討してください。

（注） 展開ジョブが失敗した場合、システムは、一部の変更を以前の設定にロールバックする必要があります。ロールバックには、データプレーン設定のクリアと以前のバージョンの再展開が含まれます。これにより、ロールバックが完了するまでトラフィックが中断されます。

目的の変更を完了した後、次の手順を使用して変更を展開します。

注意 Threat Defense デバイスは、インスペクションエンジンがソフトウェアのリソースの問題が原因でビジー状態である、または設定の展開中にエンジンの再起動が必要なためダウンしているときに、トラフィックをドロップします。再起動が必要な変更の詳細については、インスペクション エンジンを再起動する設定の変更 （42 ページ）を参照してください。

手順

ステップ 1 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

[保留中の変更（Pending Changes）] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集された要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

展開でインスペクションエンジンの再起動が必要な場合は、再起動を必要とする変更の詳細を示すメッセージがページに表示されます。この時点で一時的なトラフィック損失を許容できない場合は、ダイアログを閉じ、変更を展開する良いタイミングを待ちます。

アイコンが強調表示されていない場合でも、アイコンをクリックすると最後に成功した展開ジョブの日時を確認できます。展開履歴を表示するリンクもあり、クリックすると展開ジョブだけを表示するようにフィルタ処理された監査ページに移動します。

ステップ 2 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じても、ジョブは停止しません。結果は、タスクリストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴（Deployment History）] リンクをクリックすると結果が表示されます。

状況に応じて、次の手順を実行できます。

- [ジョブの命名（Name the Job）]：展開ジョブに名前を付けるには、[今すぐ展開（Deploy Now）] ボタンのドロップダウン矢印をクリックして、[展開ジョブの命名（Name the Deployment Job）] を選択します。名前を入力して [展開（Deploy）] をクリックします。名前は、ジョブの一部として監査および展開履歴に表示されるため、ジョブの検索が容易になります。

  たとえば、ジョブの名前を「DMZ Interface Configuration」にした場合、成功した展開の名前は「Deployment Completed: DMZ Interface Configuration」になります。さらに、その名前は、展開ジョブに関連する [タスク開始（Task Started）] イベントと [タスク完了（Task Completed）] イベントの [イベント名（Event Name）] として使用されます。

- [完全な展開を強制（Force a full deployment）]：問題があり、システムに変更だけではなく完全な設定を展開するように強制する場合は、[今すぐ展開（Deploy Now）] ボタンのドロップダウン矢印をクリックして [完全な展開を適用（Apply Full Deployment）] を選択することができます。完全な展開の場合はトラフィックが中断されるため、[展開（Deploy）] をクリックする前に、このアクションを実行することを確認する必要があります。

- [変更の破棄（Discard Changes）]：保留中の変更をすべて破棄するには、**[詳細オプション（More Options）]** > **[すべて破棄（Discard All）]** をクリックします。確認を求められます。

- [変更のコピー（Copy Changes）]：変更の一覧をクリップボードにコピーするには、**[詳細オプション（More Options）]**>**[クリップボードにコピー（Copy to Clipboard）]**をクリックします。このオプションは、変更の数が 500 未満の場合にのみ機能します。
- [変更のダウンロード（Download Changes）]：変更の一覧をファイルとしてダウンロードするには、**[詳細オプション（More Options）]**>**[テキストとしてダウンロード（Download as Text）]**をクリックします。自分のワークステーションにファイルを保存するように求められます。このファイルは YAML 形式です。YAML 形式に対応しているエディタがない場合は、テキスト エディタで表示できます。

インスペクション エンジンを再起動する設定の変更

設定の変更を展開した場合、次の設定またはアクションはいずれもインスペクションエンジンを再起動します。

⚠

注意 展開時に、リソース需要が高まった結果、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、一部の設定の展開では、インスペクションエンジンを再起動する必要があり、トラフィック インスペクションが中断され、トラフィックがドロップされます。

展開

一部の変更ではインスペクションエンジンの再起動が必要で、これにより一時的なトラフィック損失が発生します。インスペクションエンジンの再起動が必要な変更は、次のとおりです。

- SSL 復号ポリシーが有効化または無効化された。
- 1 つ以上の物理インターフェイス上（サブインターフェイスではありません）で MTU が変更された。
- アクセス制御ルールのファイル ポリシーを追加または削除します。
- VDB が更新された。
- 高可用性設定が作成または破棄された。

さらに、Snort プロセスがビジー状態で CPU の合計使用率が 60% を超えている場合、展開中に一部のパケットがドロップされることがあります。**show asp inspect-dp snort** コマンドを使用して、Snort の現在の CPU 使用率を確認できます。

システム データベースの更新

ルール データベースまたは VDB に更新プログラムをダウンロードした場合は、それらをアクティブにするために更新プログラムを展開する必要があります。この展開により、インスペクションエンジンが再起動される場合があります。手動で更新プログラムをダウンロードする、

または更新プログラムのスケジュールを設定する場合は、ダウンロードが完了した後に、システムが変更を自動で展開する必要があるかどうかを指定できます。更新プログラムを自動的に展開するシステムがない場合は、次に変更を展開したときに更新プログラムが適用され、その際にインスペクション エンジンが再起動される場合があります。

システム アップデート

システムを再起動せずに、バイナリの変更が含まれるシステム更新プログラムまたはパッチをインストールする場合は、インスペクションエンジンを再起動する必要があります。バイナリの変更には、インスペクション エンジン、プリプロセッサ、脆弱性データベース（VDB）または共有オブジェクトルールの変更が含まれることがあります。場合によって、バイナリの変更を含まないパッチで、Snort の再起動が必要になることもある点に注意してください。

完全な展開を強制するいくつかの変更の設定

ほとんどの場合、展開には変更だけが含まれます。ただし、必要に応じてシステムは設定全体を再適用し、それがネットワークを中断させる場合があります。次に、完全な展開を強制するいくつかの変更を示します。

- セキュリティ インテリジェンス ポリシーまたはアイデンティティポリシーは、最初は有効になっています。
- セキュリティインテリジェンスポリシーとアイデンティティポリシーの両方が無効になっています。
- データを再利用する場合の EtherChannel の作成。
- EtherChannel の削除。
- EtherChannel のメンバー インターフェイス アソシエーションの変更。
- 設定で使用されているインターフェイスの削除。たとえば、アクセスコントロールルールで使用されるセキュリティゾーンの一部であるサブインターフェイスを削除します。
- FlexConfig ポリシーの一部である FlexConfig オブジェクトの変更、またはオブジェクトに negate 行が含まれていない場合のポリシーからのオブジェクトの削除。negate 行を省略すると、FlexConfig オブジェクトによって生成された設定を削除する特定の方法がないため、システムは強制的に完全に展開されます。各 FlexConfig オブジェクトに適切な negate 行を常に含めることで、この問題を回避できます。

インターフェイスと管理ステータスの表示

[デバイスの概要（Device Summary）]には、デバイスのグラフィカル ビューと管理アドレス用の設定が含まれています。[デバイスの概要（Device Summary）] を開くには、[デバイス（Device）] をクリックします。

このグラフィックの要素は、要素のステータスに基づいて色が変わります。要素をマウス オーバーすると、追加情報が提供される場合があります。このグラフィックを使用して、次の項目をモニターできます。

（注） インターフェイス ステータス情報を含む、グラフィックのインターフェイス部分は、[インターフェイス（Interfaces）] ページおよび **[モニタリング（Monitoring）]** > **[システム（System）]** ダッシュボードでも使用可能です。

インターフェイス ステータス

ポートをマウス オーバーすると、その IP アドレスと有効なリンク ステータスが表示されます。IPアドレスはスタティックに割り当てることもできれば、DHCPを使用して取得することもできます。ブリッジ仮想インターフェイス（BVI）をマウスオーバーすると、メンバーインターフェイスのリストが表示されます。

インターフェイス ポートは、次のカラー コーディングを使用します。

- 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
- グレー：インターフェイスは無効です。
- オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。

内部、外部ネットワーク接続

グラフィックは、次の条件に従い、外部（またはアップストリーム）ネットワークおよび内部ネットワークに接続されているポートを示します。

- 内部ネットワーク：「inside」という名前のインターフェイスの場合のみ、内部ネットワークのポートが表示されます。その他に内部ネットワークが存在する場合、それらは表示されません。いずれのインターフェイスにも「inside」と命名していない場合は、ポートは内部ポートとしてマークされません。
- 外部ネットワーク：「outside」という名前のインターフェイスの場合のみ、外部ネットワークのポートが表示されます。内部ネットワークと同様に、この名前は必須であり、存在しない場合は、ポートは外部ポートとしてマークされません。

管理設定のステータス

グラフィックは、管理アドレス用にゲートウェイ、DNS サーバー、NTP サーバー、スマートライセンスが設定されているかどうか、さらに、それらの設定が正常に機能しているかどうかを示します。

緑は機能が設定され正常に動作していることを示し、グレーは機能が設定されていないか、正常に動作していないことを示しています。たとえば、サーバーに到達不能な場合は、DNSボックスがグレーになります。要素をマウス オーバーすると、詳細が表示されます。

問題が見つかった場合は、次のように修正します。

- 管理ポートおよびゲートウェイ：**[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** を選択します。
- DNSサーバー：**[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を選択します。
- NTPサーバー：**[システム設定（System Settings）]** > **[NTP]** を選択します。NTP のトラブルシューティング （1013 ページ）も参照してください。
- スマート ライセンス：[スマートライセンス（Smart License）] グループ内の [設定の表示（View Configuration）] リンクをクリックします。

システム タスク ステータスの表示

システム タスクには、さまざまなデータベースの更新の取得や適用など、直接関与することなく実行されるアクションが含まれます。これらのタスクのリストとそのステータスを表示し、これらのシステム タスクが正常に完了したことを確認できます。

タスク リストには、システム タスクと展開ジョブの統合ステータスが表示されます。監査ログにはより詳細な情報が含まれており、**[デバイス（Device）]** > **[デバイス管理（Device Administration）]** > **[監査ログ（Audit Log）]** の下にあります。たとえば、監査ログにはタスクの開始とタスクの終了ごとに個別のイベントが表示されます。一方、タスク リストではそれらのイベントが単一のエントリにマージされます。さらに、展開の監査ログエントリには、展開された変更に関する詳細情報が含まれています。

手順

ステップ 1 メインメニューの [タスクリスト（Task List）] ボタンをクリックします。

タスク リストが開き、システム タスクのステータスと詳細が表示されます。

ステップ 2 タスクのステータスを評価します。

永続的な問題がある場合は、デバイス設定を修正する必要があります。たとえば、データベースの更新を永続的に取得できない場合、デバイスの管理 IP アドレスにインターネットへのパスがないと示される場合があります。タスクの説明に挙げられている問題については、Cisco Technical Assistance Center（TAC）に問い合わせる必要があります。

タスク リストでは、次の操作を実行できます。

- これらのステータスに基づいてリストをフィルタするには、[成功（Success）] または [失敗（Failures）] ボタンをクリックします。
- タスクをリストから削除するには、[削除（delete）] アイコン（）をクリックします。

- 進行中でないすべてのタスクのリストを空にするには、[完了したタスクをすべて削除（Remove All Completed Tasks）] をクリックします。

CLI コンソールを使用した設定の監視およびテスト

Threat Defense デバイスには、監視およびトラブルシューティングに使用できる CLI（コマンド ライン インターフェイス）が組み込まれています。SSH セッションを開いてすべてのシステムコマンドにアクセスすることはできますが、Device Manager で CLI コンソールを開いて、さまざまな **show** コマンド、**ping**、**traceroute**、および **packet-tracer** などの読み取り専用コマンドを使用することもできます。管理者権限を持っている場合は、**failover**、**reboot**、および **shutdown** コマンドを入力することもできます。

ページ間の移動、設定、および機能の展開を行っている間、CLI コンソールを開いたままにしておくことができます。たとえば、新しいスタティックルートを展開した後で、CLI コンソールで **ping** を使用して、ターゲットネットワークに到達できることを確認できます。

CLI コンソールでは基本 脅威に対する防御 CLI を使用します。CLI コンソールを使用して、診断 CLI、エキスパート モード、および FXOS CLI（FXOS を使用するモデル）に入ることはできません。このような他の CLI モードに入る必要がある場合は、SSH を使用します。

コマンドの詳細については、Cisco Firepower Threat Defense コマンド リファレンス、https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.htmlを参照してください。

注：

- **ping** は CLI コンソールでサポートされていますが、**ping system** コマンドはサポートされていません。
- システムは最大で 2 つのコマンドを同時に処理できます。そのため、別のユーザが（たとえば、REST API を使用して）コマンドを発行している場合は、その他のコマンドの完了を待ってからコマンドを入力する必要があります。問題が解決しない場合は、CLI コンソールの代わりに SSH セッションを使用します。
- コマンドは、展開された設定に基づいて情報を返します。Device Manager で設定を変更しても、展開していない場合は、コマンド出力に変更の結果が表示されません。たとえば、新しいスタティックルートを作成しても展開していない場合、そのルートは **show route** 出力に表示されません。

手順

ステップ 1 Web ページの右上にある [CLIコンソール（CLI Console）] ボタンをクリックします。

ステップ 2 プロンプトにコマンドを入力し、[Enter] を押します。

コマンドの中には他より出力まで時間がかかるものもありますが、しばらくお待ちください。コマンドの実行がタイムアウトになったというメッセージが表示されたら、もう一度試してください。**show perfstats** など、対話型の応答が必要なコマンドを入力した場合にも、タイムアウトエラーが発生します。問題が解決しない場合は、CLI コンソールの代わりに SSH クライアントを使用する必要があります。

このウィンドウを使用する方法について、いくつかのヒントを次に示します。

- コマンドの一部を入力した後で [Tab] キーを押すと、オート コンプリートが作動します。また、Tab はコマンド内のその位置で使用可能なパラメータをリストします。また、Tab は 3 つのレベルまでキーワードを示します。3 つのレベルを過ぎると、コマンド リファレンスを使用して詳細を確認する必要があります。
- コマンドの実行を停止するには、Ctrl+C を押します。
- ウィンドウを移動するには、ヘッダー内の任意の箇所をクリックしたままウィンドウを目的の位置にドラッグします。
- ウィンドウ サイズを変更するには、[展開（Expand）] （  ）または [折りたたみ（Collapse）] （  ）ボタンをクリックします。
- [別のウィンドウに切り離す（Undock Into Separate Window）] （  ）ボタンをクリックすると、ウィンドウが Web ページから独自のブラウザ ウィンドウに切り離されます。再度ドッキングするには、[メインウィンドウにドッキング（Dock to Main Window）] （  ）ボタンをクリックします。
- クリックしてドラッグすると、テキストが強調表示されます。次に Ctrl+C を押すと、出力がクリップボードにコピーされます。
- すべての出力を消去するには、[CLIのクリア（Clear CLI）] （  ）ボタンをクリックします。
- [最後の出力のコピー（Copy Last Output）] （  ）ボタンをクリックすると、最後に入力したコマンドからの出力がクリップボードにコピーされます。

ステップ 3 完了したら、コンソール ウィンドウを閉じます。**exit** コマンドは使用しないでください。

Device Manager へのログインに使用するクレデンシャルにより CLI へのアクセスが検証されますが、コンソール使用時は実際には CLI にログインしていません。

Device Manager と REST API の併用

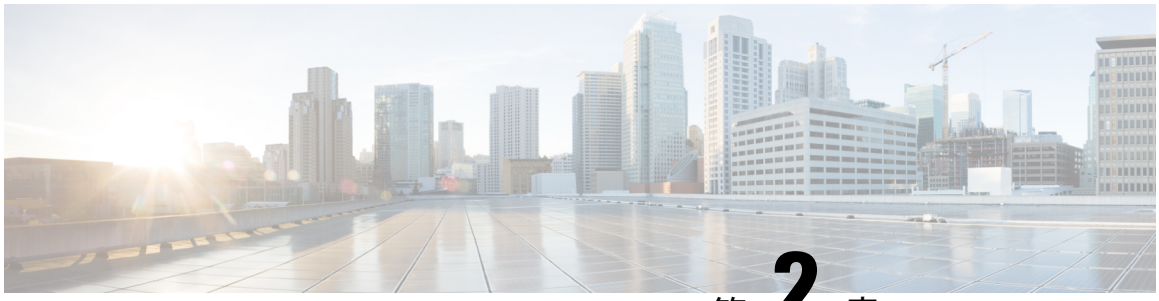
ローカル管理モードでデバイスをセットアップする場合、Device Manager と 脅威に対する防御 REST API を使用してデバイスを設定できます。実際には、Device Manager は REST API を使用してデバイスを設定します。

ただし、REST API は Device Manager で利用できる機能に加えて、その他の機能を提供できることを理解してください。したがって、所定の機能について、Device Manager で設定を確認するときには表示できない、REST API を使用した設定を行うことができます。

REST API で利用できて Device Manager で利用できない機能を設定する場合は、設定が完了していない可能性がある、Device Manager を使用したすべての機能（リモートアクセス VPN など）に変更を加えます。API のみの設定が維持されるかどうかは場合によって異なります。多くの場合、Device Manager で使用できない設定への API の変更は Device Manager の編集により維持されます。所定の機能については、変更が維持されているかどうかを確認する必要があります。

一般的には、所定の機能について Device Manager と REST API の両方を同時に使用しないようにする必要があります。代わりに、デバイスを設定するために、機能ごとにいずれかの方法を選択します。

API エクスプローラを使用して API メソッドを表示および試すことができます。[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。



第 2 章

ベストプラクティス：Threat Defense の使用例

ここでは、Device Manager を使用して 脅威に対する防御 で実行する共通のタスクについていくつか説明します。これらの使用例は、デバイス設定ウィザードが完了しており、この初期設定が保持されていることを前提としています。初期設定を変更した場合でも、これらの例を使用して、製品の使用方法を理解できます。

Device Manager でデバイスを設定する方法

セットアップ ウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 外部インターフェイスと内部インターフェイス。その他のデータインターフェイスは設定されません。
- （Firepower 4100/9300）事前に設定されたデータインターフェイスはありません。
- （ISA 3000）ブリッジグループには 2 つの内部インターフェイスと 2 つの外部インターフェイスが含まれています。セットアップを完了するには、BVI1 の IP アドレスを手動で設定する必要があります。
- （Firepower 4100/9300 を除く）内部インターフェイスおよび外部インターフェイスのセキュリティゾーン。

- （Firepower 4100/9300 を除く）内部から外部へのトラフィックをすべて信頼するアクセスルール。 ISA 3000 の場合、内部から外部、および外部から内部へのすべてのトラフィックを許可するアクセスルールがあります。
- （Firepower 4100/9300 および ISA 3000 を除く）内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有ポートに変換するインターフェイス NAT ルール。
- （Firepower 4100/9300 および ISA 3000 を除く）内部インターフェイスで実行されている DHCP サーバー。

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン（**?**）をクリックしてください。

手順

ステップ 1 [デバイス（Device）] を選択し、[スマートラインセンス（Smart License）] グループで [設定の表示（View Configuration）] をクリックします。

使用するオプションライセンス（IPS 、マルウェア防御、URL）ごとに [有効化（Enable）] をクリックします。セットアップ中にデバイスを登録した場合は、必要な RA VPN ライセンスも有効にできます。必要かどうかわからない場合は、各ライセンスの説明を確認します。

登録していない場合は、このページから登録できます。**[Register Device]** をクリックして、説明に従います。評価ライセンスの有効期限が切れる前に登録してください。

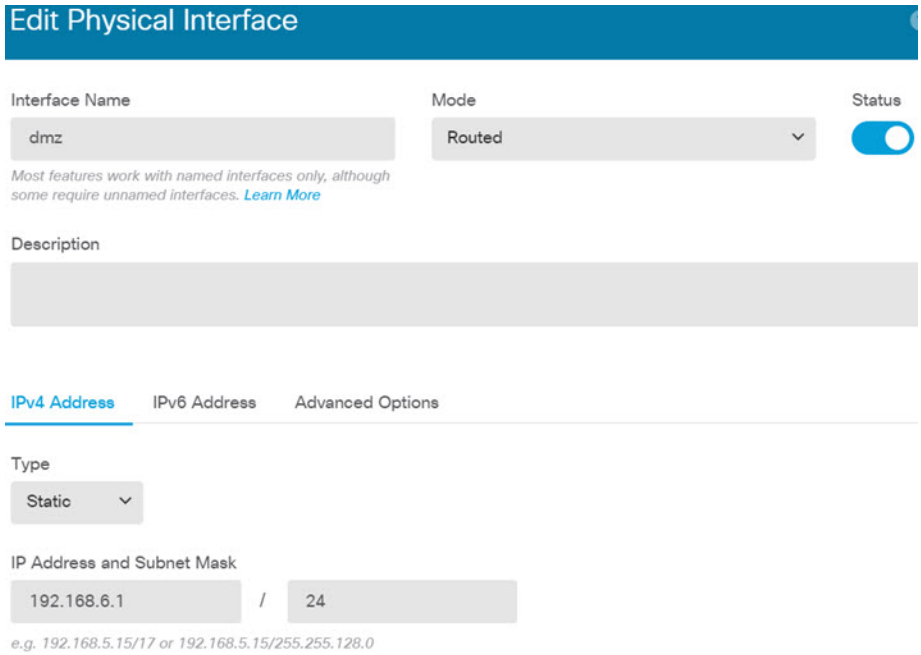
ステップ 2 他のインターフェイスに接続している場合は、[デバイス（Device）] を選択し、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックしてから、インターフェイスのタイプをクリックして、インターフェイスのリストを表示します。

- Firepower 4100/9300 では、名前、IP アドレス、またはセキュリティゾーンを使用して事前に設定されているデータインターフェイスがないため、使用するインターフェイスを有効にして設定する必要があります。
- ISA 3000 はのすべてのデータインターフェイスが含まれるブリッジグループが事前に設定された状態で出荷されるため、これらのインターフェイスを設定する必要はありません。ただし、BVI の IP アドレスを手動で設定する必要があります。ブリッジグループを分割する場合は、ブリッジグループを編集して個別に扱うインターフェイスを除去できます。その後、別々のネットワークをホストするインターフェイスとしてそれらを設定できます。

  他のモデルでは、他のインターフェイスのブリッジグループを作成、別々のネットワークを設定、または両方の組み合わせを設定できます。
- Firepower 1010 の場合、Ethernet1/1（外部）以外のインターフェイスはすべて、VLAN1（内部）に割り当てられたアクセスモードのスイッチポートです。スイッチポートをファイアウォールポートに変更することができます。それには、新しい VLAN インターフェイスを追加してスイッチポートを割り当てます。または、トランクモードのスイッチポートを設定します。

各インターフェイスの[編集（Edit）]アイコン（）をクリックして、IPアドレスなどの設定を定義します。

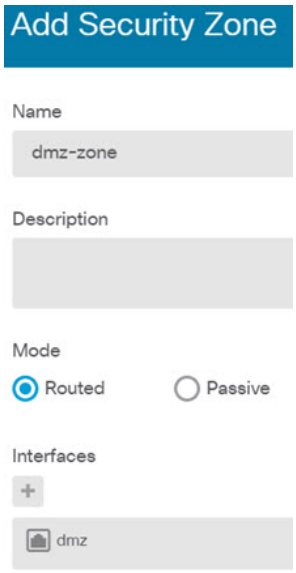
次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。完了したら [保存（Save）] をクリックします。



ステップ 3 新しいインターフェイスを構成する場合は、[オブジェクト（Objects）]を選択し、目次から[セキュリティゾーン（Security Zones）] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後には常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZインターフェイスのために新しいDMZゾーンを作成する方法を示します。

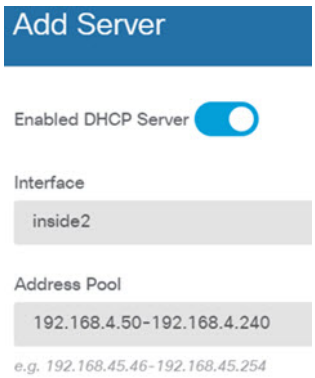


ステップ 4 内部クライアントがDHCPを使用してデバイスからIPアドレスを取得するようにする場合は、[デバイス（Device）] を選択し、次に **[システム設定（System Settings）]** > **[DHCPサーバー（DHCP Server）]** を選択します。[DHCPサーバー（DHCP Servers）] タブを選択します。

すでに内部インターフェイス用に構成されているDHCPサーバーがありますが、アドレスプールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上にDHCPサーバーをセットアップするのがごく一般的です。各内部インターフェイスのサーバーおよびアドレスプールを設定するには、[+]をクリックします。

クライアントに対して提供される WINS および DNS リストを [設定（Configuration）] タブで調整することもできます。

次の例では、アドレス プールの 192.168.4.50 ～ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバーを設定する方法を示しています。



ステップ 5 [デバイス（Device）] を選択し、次に [設定の表示（View Configuration）]を [ルーティング（Routing）] グループでクリックし、デフォルトルートを設定します。

デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4（0.0.0.0/0）、デフォルトの IPv6 ルートは任意の ipv6（::0/0）です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

このページで定義したルートは、データ インターフェイス用のみです。管理インターフェイスには影響しません。管理ゲートウェイは **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** で設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです（アドレスは ISP から取得する必要があります）。[ゲートウェイ（Gateway）] の下部の [新しいネットワークを作成する（Create New Network）] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

ステップ 6 [ポリシー（Policies）] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間のトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーン オブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティ ゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

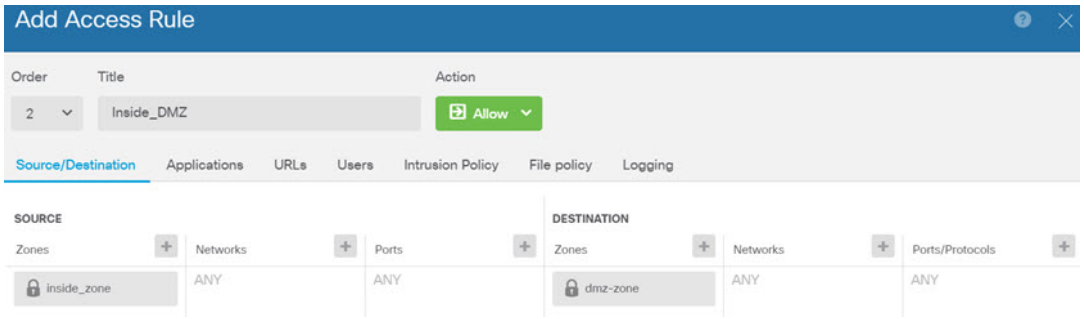
さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要が

あるかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。

- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティ ポリシーを使用します。
- [セキュリティ インテリジェンス（Security Intelligence）]：セキュリティ インテリジェンス ポリシーを使用して、選択されている IP アドレスまたは URL との接続をすぐにドロップします。既知の不正なサイトをブロックすれば、アクセス制御ポリシーでそれらを考慮する必要がなくなります。シスコでは、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT]（ネットワーク アドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザー グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間のトラフィックを許可する方法を示します。この例では、[接続の最後で（At End of Connection）] が選択されている場合、[ロギング（Logging）] を除いて他のいずれのタブでもオプションは設定されません。



ステップ 7 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ネットワーク トラフィックを調べる方法

デバイスの初期設定を完了すると、インターネットまたはその他のアップストリーム ネットワークへのすべての内部トラフィック アクセスを許可するアクセス コントロール ポリシーと、他のすべてのトラフィックをブロックするデフォルト アクションが設定されます。追加のアクセス コントロール ルールを作成する前に、ネットワークで実際に発生しているトラフィックを調べると役立ちます。

Device Manager のモニタリング機能を使用してネットワーク トラフィックを分析できます。以下の質問の回答には Device Manager のレポートが役立ちます。

- ネットワークの用途
- 最も多くネットワークを使用しているユーザ
- ユーザの接続先
- ユーザが使用しているデバイス
- ヒット数が最も多いアクセス コントロール ルール（ポリシー）

初期のアクセス ルールでは、ポリシー、宛先、セキュリティ ゾーンなどのトラフィックについての情報が明らかになります。しかし、ユーザ情報を取得するには、ユーザを認証（識別）する必要があるアイデンティティ ポリシーの設定が必要です。ネットワークで使用されるアプリケーションの情報を取得するには、追加でいくつかの調整を行う必要があります。

次の手順で、トラフィックをモニタするように 脅威に対する防御 デバイスを設定する方法を説明し、設定ポリシーおよびモニタリング ポリシーのエンドツーエンド プロセスの概要を示します。

（注） この手順では、ユーザがアクセスしたサイトの Web サイト カテゴリとレピュテーションの情報は取得されないため、URL カテゴリ ダッシュボードに有用な情報は表示されません。カテゴリおよびレピュテーションのデータを取得するには、カテゴリベースの URL フィルタリングを実装し、URL ライセンスを有効化する必要があります。この情報のみ取得する場合は、許容するカテゴリ（金融など）へのアクセスを許可する新規のアクセスコントロールルールを追加して、アクセス コントロール ポリシーで最初のルールに設定できます。URL フィルタリングの実装の詳細については、アクセプタブル ユース ポリシー（URL フィルタリング）の実装方法 （73 ページ） を参照してください。

手順

ステップ 1 ユーザの動作を調べるには、接続に関連付けられているユーザを識別するアイデンティティポリシーの設定が必要です。

アイデンティティポリシーを有効化すると、ネットワークを使用するユーザおよびそのユーザが使用しているリソースに関する情報を収集できます。この情報は、ユーザの監視ダッシュボードに表示されます。ユーザ情報は、イベントビューアに表示される接続イベントにも表示されます。

この例では、ユーザアイデンティティを取得するためにアクティブ認証を実装します。アクティブ認証を使用すると、デバイスからユーザ名とパスワードを求められます。ユーザは、HTTP 接続に Web ブラウザを使用する場合にのみ認証されます。

ユーザが認証に失敗した場合でも、そのユーザは Web 接続を確立することはできます。これは、単に、接続に関するユーザのアイデンティティ情報がないことを意味します。必要に応じて、認証に失敗したユーザのトラフィックをドロップするアクセス コントロール ルールを作成できます。

a) メイン メニューで、[ポリシー（Policies）] をクリックして、[アイデンティティ（Identity）] をクリックします。

アイデンティティポリシーは、最初は無効化されています。アクティブ認証を使用している場合、アイデンティティポリシーは Active Directory サーバを使用してユーザを認証し、ユーザが使用しているワークステーションの IP アドレスをユーザに関連付けます。その後、システムはその IP アドレスのトラフィックをユーザのトラフィックとして識別します。

b) [アイデンティティポリシーの有効化（Enable Identity Policy）] をクリックします。

c) [アイデンティティルールの作成（Create Identity Rule）] ボタンまたは [+] ボタンをクリックして、アクティブ認証を義務付けるルールを作成します。

この例では、すべての人に認証を義務付けていると仮定しています。

d) ルールの [名前（Name）] を入力します。Require_Authentication など、任意の名前を選択できます。

e) [送信元または宛先（Source/Destination）] タブをデフォルトのままにします。これは、[任意（Any）] 基準に適用されます。

より制限されているトラフィックに合わせて、ポリシーに制約を加えることができます。ただし、アクティブ認証は HTTP トラフィックに対してのみ試行されるため、非 HTTP トラフィックが送信元/宛先条件に一致していることは重要ではありません。アイデンティティポリシーのプロパティの詳細については、を参照してください。アイデンティティ ルールの設定 （575 ページ）

f) [アクション（Action）] で [アクティブ認証（Active Auth）] を選択します。

いくつか未定義の設定があるため、アイデンティティポリシーの設定が行われていないと仮定して、[アイデンティティポリシー設定（Identity Policy Configuration）] ダイアログボックスが開きます。

g) アクティブ認証に必要な [キャプティブ ポータル（Captive Portal）] の設定と [SSL復号（SSL Decryption）] の設定を行います。

アイデンティティルールによりユーザーのアクティブ認証が要求されると、そのユーザーはキャプティブポータルポートにリダイレクトされ、認証を求められます。キャプティブポータルにはSSL復号化ルールが必要です。このルールは、システムによって自動的に生成されますが、SSL 復号化ルールに使用する証明書は選択する必要があります。

- [サーバ証明書（Server Certificate）]：アクティブ認証時にユーザに提示する内部証明書を選択します。事前定義された自己署名の DefaultInternalCertificate を選択するか、[新規内部証明書の作成（Create New Internal Certificate）] をクリックして、ブラウザが信頼している証明書をアップロードできます。

  ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

- [ホスト名にリダイレクト（Redirect to Host Name）]：アクティブな認証要求のキャプティブポータルとして使用するインターフェイスの完全修飾ホスト名を定義するネットワークオブジェクトを選択します。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。

  FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。

  アイデンティティルールによりユーザーのアクティブ認証が要求されているが、リダイレクト FQDN を指定していない場合、ユーザーは、接続されているインターフェイス上のキャプティブポータルポートにリダイレクトされます。

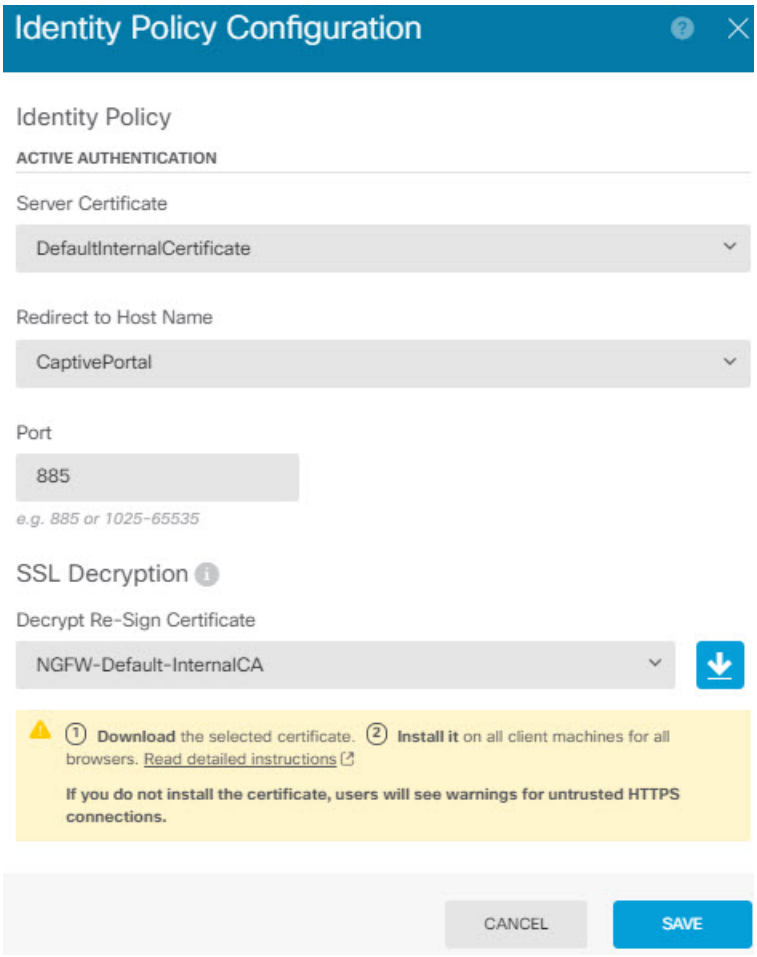
- [ポート（Port）]：キャプティブ ポータル ポート。デフォルトは、885（TCP）です。別のポートを設定する場合は、1025 ～ 65535 の範囲にする必要があります。

- [再署名証明書の復号（Decrypt Re-Sign Certificate）]：再署名証明書での復号を実装するルールに使用する内部 CA 証明書を選択します。事前定義済みの NGFW-Default-InternalCA 証明書（デフォルト）か、作成またはアップロードした証明書を使用できます。証明書がまだ存在しない場合は、[Create Internal CA] をクリックして作成します。SSL 復号化ポリシーをまだ有効にしていない場合にのみ、復号化再署名証明書の入力が求められます。

  クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（  ）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロード （561 ページ）も参照してください。

例：

[アイデンティティポリシーの設定（Identity Policy Configuration）] ダイアログは、次のようになります。



h) [保存（Save）] をクリックしてアクティブ認証の設定を保存します。

[アクティブ認証（Active Authentication）] タブが [アクション（Action）] 設定の下に表示されます。

i) [アクティブ認証（Active Authentication）] タブで、[HTTPネゴシエート（HTTP Negotiate）] を選択します。

これにより、ブラウザおよびディレクトリ サーバは最も強力な認証プロトコルを、NTLM、HTTP ベーシックの順にネゴシエートできます。

（注） [ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザーがキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してリダイレクトされます。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用する場合は、アクティブ認証が必要なすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバーを更新する必要もあります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。 DNS サーバを更新できない、または更新を望まない場合は、その他の認証方式のいずれかを選択します。

j) [ADアイデンティティソース（AD Identity Source）] で [新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。

レルム サーバオブジェクトをすでに作成している場合は、それを選択して、サーバの設定手順をスキップします。

次のフィールドに入力して、[OK] をクリックします。

- [名前（Name）]：ディレクトリ レルムの名前。
- [タイプ（Type）]：ディレクトリ サーバのタイプ。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [ディレクトリユーザ名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

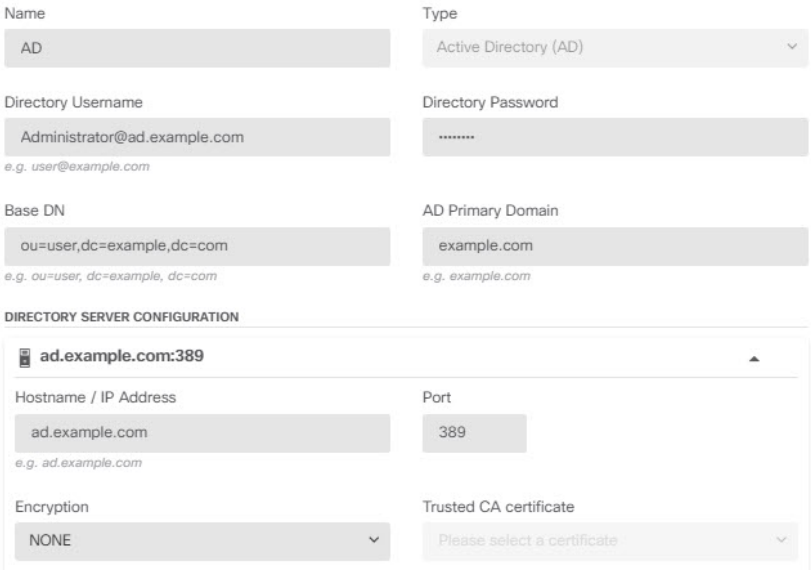
  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=adminisntrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN（Base DN）]：ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリ ツリー。（dc=example,dc=com など）。ベース DN の検索の詳細については、ディレクトリ ベースの DN の決定（194 ページ）を参照してください。
- [ADプライマリドメイン（AD Primary Domain）]：デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。例、example.com。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名またはIPアドレス。サーバに対して暗号化された接続を使用する場合、IPアドレスではなく、完全修飾ドメイン名を入力する必要があります。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは389です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法（[STARTTLS] または [LDAPS]）を選択します。デフォルトでは[なし（None）]になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。
  - [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリ サーバでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモート アクセス VPN にレルムを使用する場合はサポートされません。
  - [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。
- [信頼できるCA証明書（Trusted CA Certificate）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリ サーバ間の信頼できる接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

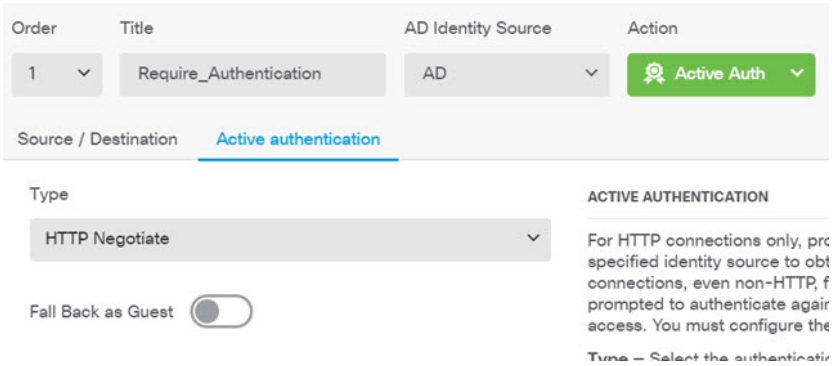
例：

たとえば、次のイメージには、ad.example.com サーバの暗号化されていない接続の作成方法が示されています。プライマリ ドメインは example.com で、ディレクトリ ユーザ名は Administrator@ad.example.com です。すべてのユーザおよびグループの情報は、識別名（DN）ou=user,dc=example,dc=com の下にあります。



k) [ADアイデンティティソース（AD Identity Source）] で、作成したオブジェクトを選択します。

ルールは次のようになります。



l) [OK] をクリックしてルールを追加します。

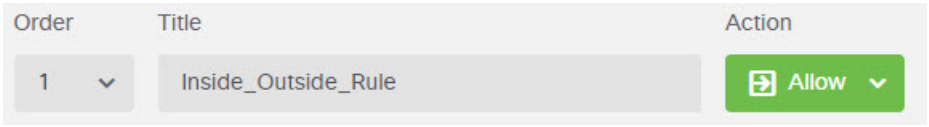
ウィンドウの右上を見ると、[展開（Deploy）] アイコン ボタンにドットが表示されていることがあります。これは、展開されていない変更があることを示します。ユーザインターフェイスを変更するだけでは、デバイスに変更を設定するには不十分です。変更を展開する必要があります。部分的に設定された変更がデバイスで実行される潜在的な問題を避けるために、一連の関連する変更を加えてから変更を展開できます。この手順で、後から変更を展開します。

ステップ 2 Inside_Outside_Rule アクセス コントロール ルールのアクションを [許可（Allow）] に変更します。

Inside_Outside_Rule アクセス ルールは、信頼できるルールとして作成されます。ただし、信頼できるトラフィックのインスペクションは実行されないため、トラフィック一致基準にアプリケーションやその他の条件（ゾーン、IP アドレス、およびポートを除く）が含まれない場合、システムは信頼できるトラフィックの一部の特性（アプリケーションなど）を学習できません。信頼できるトラフィックではなく許可にルールを変更すると、システムはすべてのトラフィックのインスペクションを実行します。

（注）　（ISA 3000）。また、Outside_Inside_Rule、Inside_Inside_Rule および Outside_Outside_Rule を [Trust] から [Allow] に変更することも検討してください。

a) [ポリシー（Policies）] ページの [アクセスコントロール（Access Control）] をクリックします。
b) Inside_Outside_Rule 行の右側にある [アクション（Actions）] セルにマウスを合わせると、[編集（edit）] アイコンと [削除（delete）] アイコンが表示されます。ルールを開くには、[編集（edit）] アイコン（）をクリックします。
c) [アクション（Action）] の [許可（Allow）] を選択します。

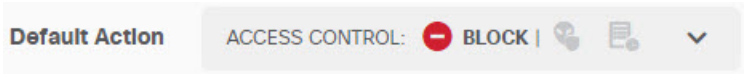


d) [OK] をクリックして変更を保存します。

ステップ 3 アクセス コントロール ポリシーのデフォルト アクションでロギングを有効化します。

接続のロギングが有効なアクセス コントロール ルールと接続が一致する場合にのみ、ダッシュボードに接続情報が表示されます。Inside_Outside_Rule ではロギングが有効ですが、デフォルト アクションのロギングは無効化されています。そのため、ダッシュボードには Inside_Outside_Rule の情報のみが表示され、ルールと一致しない接続は反映されません。

a) アクセス コントロール ポリシー ページの下部のデフォルト アクションで、任意の場所をクリックします。

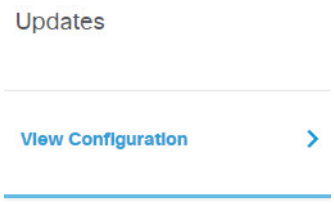


b) **[ログアクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）]** を選択します。
c) [OK] をクリックします。

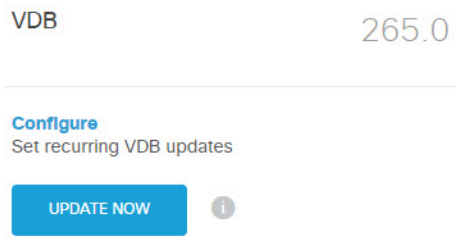
ステップ 4 脆弱性データベース（VDB）の更新スケジュールを設定します。

シスコは VDB の更新を定期的にリリースしています。これには、接続で使用されるアプリケーションを特定できるアプリケーション ディテクタが含まれています。定期的に VDB を更新する必要があります。更新を手動でダウンロードするか、または定期的なスケジュールを設定できます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、VDB の更新は無効化されているため、VDB の更新を取得するには操作を実行する必要があります。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) [更新（Updates）] グループで [設定の表示（View Configuration）] をクリックします。



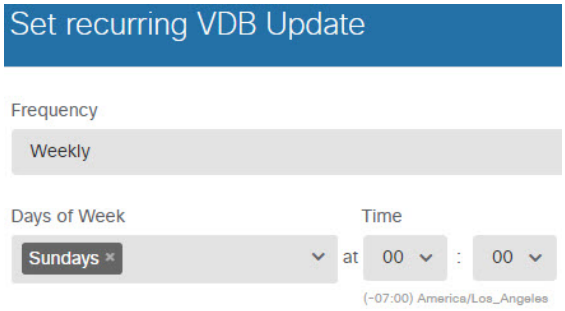
c) [VDB] グループで [設定（Configure）] をクリックします。



d) 更新スケジュールを定義します。

ネットワークを妨害しない時間および頻度を選択します。また、更新をダウンロードすると、システムが自動的に展開することも理解しておいてください。これは、新しいディテクタを有効化するために必要です。そのため、実行して保存したが、展開していない設定変更も展開されます。

たとえば、次のスケジュールでは、VDB が週に 1 回、日曜日の午前 0:00（24 時間方式を使用）に更新されます。



e) [保存（Save）] をクリックします。

ステップ 5 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

次のタスク

この時点から、監視ダッシュボードおよびイベントにユーザおよびアプリケーションの情報が表示されます。望ましくないパターンがないかこの情報を評価し、許容できない使用を制限するための新しいアクセス ルールを展開できます。

侵入およびマルウェアに関する情報の収集を開始する場合、1つまたは複数のアクセス ルールで侵入ポリシーとファイル ポリシーの有効化が必要です。また、これらの機能のライセンスも有効化する必要があります。

URL カテゴリに関する情報の収集を開始するには、URL フィルタリングを実装する必要があります。

脅威をブロックする方法

侵入ポリシーをアクセス コントロール ルールに追加することによって、次世代侵入防御システム（IPS）のフィルタリングを実装できます。侵入ポリシーはネットワーク トラフィックを分析して、トラフィックの内容を既知の脅威と比較します。接続がモニタリング中の脅威と一致した場合、システムはその接続をドロップして攻撃を阻止します。

その他すべてのトラフィックの処理は、ネットワーク トラフィックに侵入の形跡がないかどうかを調べる前に実行されます。侵入ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシーを使用してトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可（allow）] するルールに侵入ポリシーを設定できます。インスペクションは、トラフィックを [信頼（trust）] または [ブロック（block）] するよう設定されたルールでは実行されません。また、デフォルト アクションが [許可（allow）] の場合、デフォルト アクションの一部として侵入ポリシーを設定できます。

侵入ポリシーは Cisco Talos Intelligence Group（Talos）によって設計されており、侵入ルール、プリプロセッサ ルール状態、詳細設定が設定されています。Snort 3 をインスペクション エンジンとして使用している場合は、Talos ポリシーに基づき、独自のカスタム ポリシーを作成できます。

潜在的な侵入を許可するトラフィックの検査に加え、セキュリティ インテリジェンス ポリシーを使用することで、既知の不正 IP アドレスとのすべてのトラフィック、または既知の不正 URL へのすべてのトラフィックを先制的にブロックできます。

手順

ステップ 1 まだ有効化していない場合は、IPS ライセンスを有効化します。

侵入ポリシーとセキュリティ インテリジェンスを使用するには、IPS を有効にする必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) [スマートライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

c) **IPS** グループで [有効化（Enable）] をクリックします。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化（Disable）] ボタンに変わります。

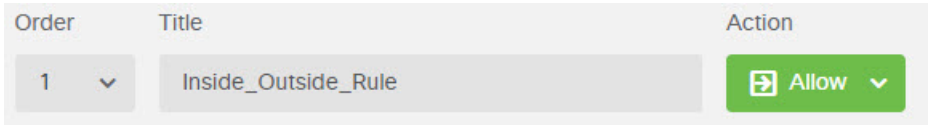
ステップ 2 1 つまたは複数のアクセス ルールの侵入ポリシーを選択します。

脅威がないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule に侵入インスペクションを追加します。

a) メイン メニューで [ポリシー（Policies）] をクリックします。

[アクセスコントロール（Access Control）] ポリシーが表示されることを確認します。

b) Inside_Outside_Rule 行の右側にある [アクション（Actions）] セルにマウスを合わせると、[編集（edit）] アイコンと [削除（delete）] アイコンが表示されます。ルールを開くには、[編集（edit）] アイコン（）をクリックします。
c) まだ選択していない場合は、[アクション（Action）] の [許可（Allow）] を選択します。

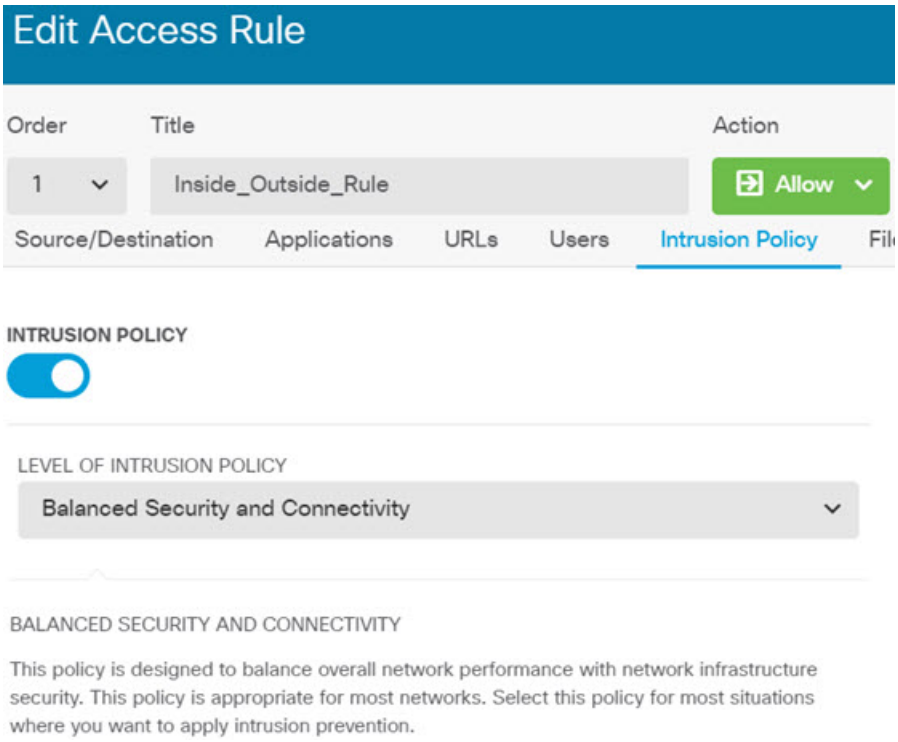


d) [侵入ポリシー（Intrusion Policy）] タブをクリックします。
e) [侵入ポリシー（Intrusion Policy）] トグルをクリックしてから、侵入ポリシーを選択します。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーは、ほとんどのネットワークに適しています。ドロップしたくないトラフィックをドロップする可能性がある、過度に強力な防御ではなく、侵入に対する適切な防御を実現します。ドロップされるトラフィックが多すぎると判断した場合は、[セキュリティより接続を優先する（Connectivity over Security）] ポリシーを選択することによって侵入インスペクションを緩和できます。

セキュリティを強力にする必要がある場合は、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーを試します。[最大検出（Maximum Detection）] ポリシーで

は、ネットワークインフラストラクチャのセキュリティがよりいっそう重視され、動作にさらに大きな影響を及ぼす可能性があります。



f) [OK] をクリックして変更を保存します。

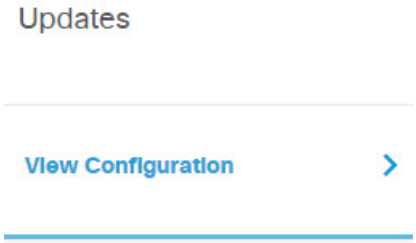
ステップ 3 （任意）**[ポリシー（Policies）]**>**[侵入（Intrusion）]**に移動し、歯車アイコンをクリックして、侵入ポリシーの syslog サーバを設定します。

侵入イベントは、アクセスコントロールルール用に設定されたsyslogサーバを使用しません。

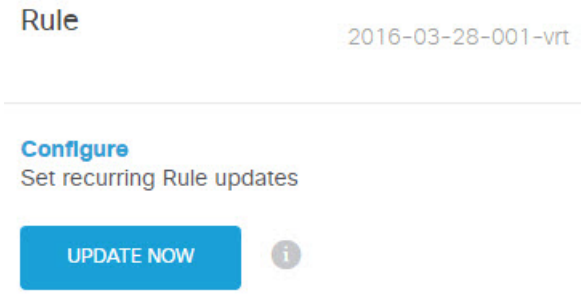
ステップ 4 侵入ルール データベースの更新スケジュールを設定します。

シスコは、接続をドロップするかどうかを決定する侵入ポリシーで使用される、侵入ルールデータベースの更新を定期的にリリースしています。ルールデータベースは定期的に更新する必要があります。更新を手動でダウンロードするか、または定期的なスケジュールを設定できます。次の手順で、スケジュールの設定方法を示します。デフォルトでは、データベースの更新は無効化されているため、更新されたルールを取得するには操作が必要です。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) [更新（Updates）] グループで [設定の表示（View Configuration）] をクリックします。



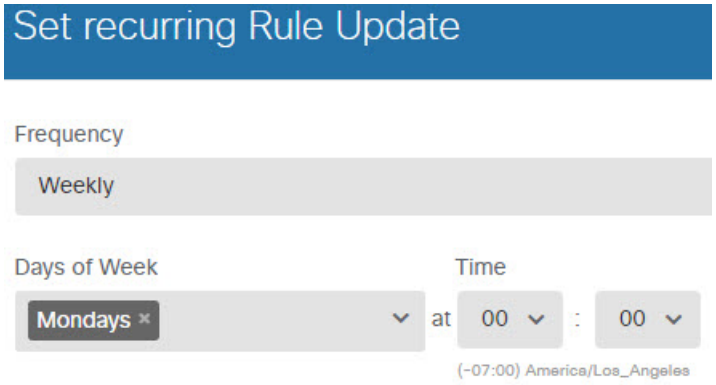
c) [ルール（Rule）] グループで [設定（Configure）] をクリックします。



d) 更新スケジュールを定義します。

ネットワークを妨害しない時間および頻度を選択します。また、更新をダウンロードすると、システムが自動的に展開することも理解しておいてください。これは、新しいルールを有効化するために必要です。そのため、実行して保存したが、展開していない設定変更も展開されます。

たとえば、次のスケジュールでは、ルール データベースが週に 1 回、月曜日の午前 0:00（24 時間方式を使用）に更新されます。



e) [Save] をクリックします。

ステップ 5 既知の不正ホストやサイトとの接続を先制的にドロップするためのセキュリティインテリジェンス ポリシーを設定します。

セキュリティインテリジェンスを使用して、脅威だとわかっているホストやサイトとの接続をブロックすることで、接続ごとに脅威を特定するためのディープ パケット インスペクションに必要な時間を節約できます。セキュリティインテリジェンスにより、不必要なトラフィック

を早期にブロックして、実際に関心があるトラフィックの処理により多くのシステム時間を残すことができます。

a) [デバイス（Device）] をクリックし、[更新（Updates）] グループで [設定の表示（View Configuration）] をクリックします。

b) [セキュリティインテリジェンスフィード（Security Intelligence Feeds）] グループで [今すぐ更新（Update Now）] をクリックします。

c) または、[設定（Configure）] をクリックして、フィードの定期更新を設定します。デフォルトの [毎時（Hourly）] はほとんどのネットワークに適していますが、必要に応じて頻度を減らすことができます。

d) [ポリシー（Policies）] をクリックして、[セキュリティインテリジェンス（Security Intelligence）] ポリシーをクリックします。

e) ポリシーをまだ有効化していない場合は、[セキュリティインテリジェンスの有効化（Enable Security Intelligence）] をクリックします。

f) [ネットワーク（Network）] タブで、ブラック/ドロップリストの [+] をクリックして、[ネットワークフィード（Network Feeds）] タブにあるすべてのフィードを選択します。フィードの横にある [i] ボタンをクリックして、各フィードの説明を確認できます。

   フィードが存在しないというメッセージが表示される場合は、後でもう一度試してください。フィードのダウンロードはまだ完了していません。この問題が解決しない場合は、管理 IP アドレスとインターネット間にパスがあることを確認してください。

g) [OK] をクリックして、選択したフィードを追加します。

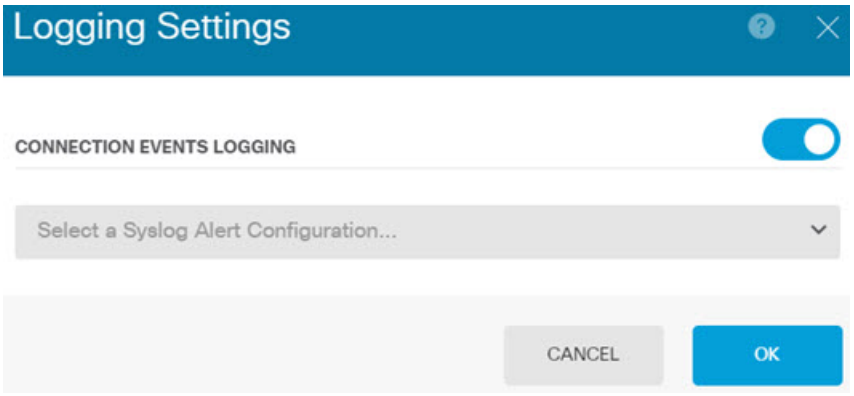
   他にも不正 IP アドレスがある場合は、**[+]** > **[ネットワークオブジェクト（Network Objects）]** をクリックして、それらのアドレスを含むオブジェクトを追加できます。リストの下部にある [新規ネットワークオブジェクトの作成（Create New Network Object）] をクリックして、すぐに追加することもできます。

h) [URL] タブをクリックし、ブラック/ドロップリストの **[+]** > **[URLフィード（URL Feeds）]** をクリックして、すべての URL フィードを選択します。[OK] をクリックして、リストに追加します。

   ネットワークリストと同様に、独自のURLオブジェクトをリストに追加して、フィードに含まれていないその他のサイトをブロックできます。**[+]** > **[URLオブジェクト（URL Objects）]** をクリックします。リストの最後にある [新規URLオブジェクトの作成（Create New URL Object）] をクリックして、新しいオブジェクトを追加できます。

i) [歯車（gear）] アイコンをクリックし、[接続イベントロギング（Connection Events Logging）] を有効にして、一致した接続のセキュリティインテリジェンスイベントをポリシーが生成できるようにします。[OK] をクリックして変更を保存します。

   接続ロギングを有効にしない場合、ポリシーが予想どおりに機能しているかどうかの評価に使用するためのデータを得られません。外部 syslog サーバを定義している場合は、ここで選択することで、そのサーバにもイベントを送信できます。



j) 必要に応じて、各タブの [ブロックしない（Do Not Block）] リストにネットワークオブジェクトまたはURLオブジェクトを追加して、ブロックリストに対する例外を作成できます。

[ブロックしない（Do Not Block）] リストは、ホワイトリストではなく、例外リストです。例外リストにあるアドレスやURLがブロックリストにも表示されている場合、そのアドレスやURLの接続はアクセスコントロールポリシーの通過を許可されます。フィードはこのようにしてブロックできますが、後で必要なアドレスやサイトがブロックされていることに気付いた場合は、例外リストを使用して、フィードを完全に削除することなく、そのブロックをオーバーライドできます。その後、それらの接続はアクセス制御、および侵入ポリシー（設定されている場合）によって評価される点に注意してください。したがって、接続に脅威が含まれている場合は、侵入検査中に特定されてブロックされます。

[アクセスおよびSIルール（Access and SI Rules）] ダッシュボード、およびイベントビューアのセキュリティインテリジェンスビューを使用して、ポリシーによって実際にドロップされているトラフィックを特定し、[ブロックしない（Do Not Block）] リストにアドレスや URL を追加する必要があるかどうかを決めます。

ステップ 6 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

次のタスク

この時点から、侵入が特定された場合は、監視ダッシュボードおよびイベントに攻撃者、ターゲット、および脅威に関する情報が表示されます。この情報を評価して、ネットワークにさら

にセキュリティ対策が必要かどうか、または使用中の侵入ポリシーのレベルを下げる必要があるかどうかを決定できます。

セキュリティインテリジェンスの場合、[アクセスおよびSIルール（Access and SI Rules）] ダッシュボードでポリシーのヒット数を確認できます。セキュリティ インテリジェンス イベントはイベント ビューアでも確認できます。セキュリティ インテリジェンスのブロック数は侵入の脅威情報には反映されません。これは、検査する前にトラフィックがブロックされるためです。

マルウェアをブロックする方法

ユーザは、インターネットサイトまたは電子メールなどのその他の通信方法から、悪意のあるソフトウェア（マルウェア）を取得する危険に常にさらされています。信頼できる Web サイトでも、乗っ取られて、無警戒なユーザにマルウェアを配布することがあります。Webページには、別の送信元からのオブジェクトを含めることができます。このオブジェクトには、イメージ、実行可能ファイル、Javascript、広告などがあります。改ざんされた Web サイトには頻繁に、外部の送信元でホストされているオブジェクトが組み込まれます。真のセキュリティとは、最初の要求だけではなく、各オブジェクトを個別に調べることです。

マルウェア防御を使用してマルウェアを検出するためにファイルポリシーを使用します。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

マルウェア防御は Secure Malware Analytics Cloud を使用して、ネットワークトラフィックで検出された潜在的なマルウェアの性質を取得します。Secure Malware Analytics Cloud にアクセスし、マルウェアルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について Secure Malware Analytics Cloud に問い合わせます。可能性のある性質は、[クリーン（clean）]、[マルウェア（malware）]、または [不明（unknown）]（明確な判定を下せない）になります。 Secure Malware Analytics Cloud に到達できない場合、性質は [不明（unknown）] になります。

ファイルポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、接続時にファイルのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可（allow）] するルールにファイル ポリシーを設定できます。インスペクションは、トラフィックを [信頼（trust）] または [ブロック（block）] するよう設定されたルールでは実行されません。

手順

ステップ 1 まだ有効化していない場合は、マルウェア防御 および IPS ライセンスを有効化します。

ファイルポリシーを使用するには、侵入ポリシーに必要なIPS ライセンスに加えて、マルウェア防御 を有効化する必要があります。現在、評価ライセンスを使用している場合は、それらの

評価ライセンスを有効にします。デバイスを登録している場合は、必要なライセンスを購入して、それらを Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) [スマートライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

c) **マルウェア防御** グループで [有効化（Enable）] をクリックし、**IPS** グループでも [有効化（Enable）] をクリックします（まだ有効化されていない場合）。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化（Disable）] ボタンに変わります。

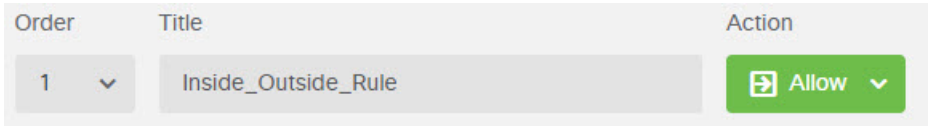
ステップ 2 1 つまたは複数のアクセス ルールのファイル ポリシーを選択します。

マルウェアがないかスキャンされるトラフィックに対応するルールを決定します。この例では、Inside_Outside_Rule にファイル インスペクションを追加します。

a) メイン メニューで [ポリシー（Policies）] をクリックします。

[アクセスコントロール（Access Control）] ポリシーが表示されることを確認します。

b) Inside_Outside_Rule 行の右側にある [アクション（Actions）] セルにマウスを合わせると、[編集（edit）] アイコンと [削除（delete）] アイコンが表示されます。ルールを開くには、[編集（edit）] アイコン（）をクリックします。
c) まだ選択していない場合は、[アクション（Action）] の [許可（Allow）] を選択します。

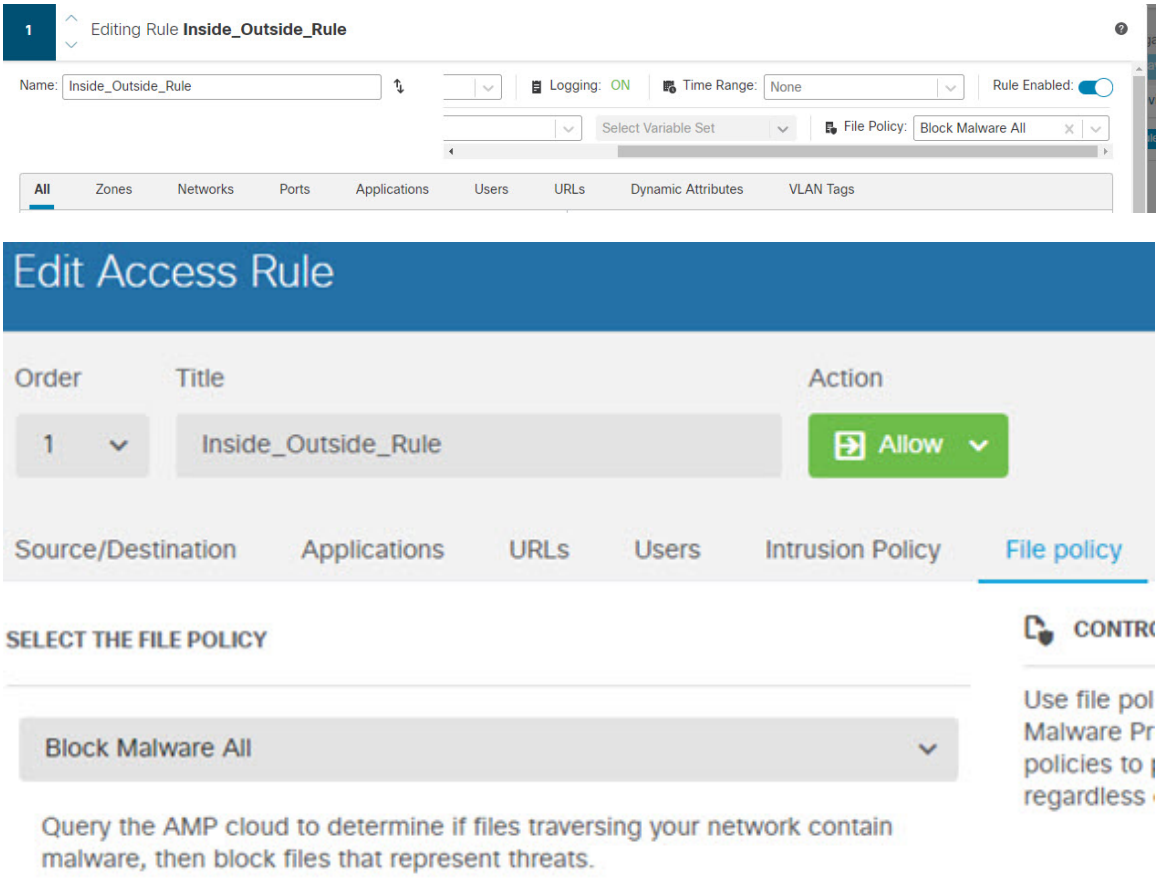


d) [ファイルポリシー（File Policy）] タブをクリックします。
e) 使用するファイル ポリシーをクリックします。

主な選択は、マルウェアと見なされるすべてのファイルをドロップする [マルウェアをすべてブロック（Block Malware All）]、または Secure Malware Analytics Cloud にクエリしてファイルの性質を判断するがブロックはしない [クラウドをすべてルックアップ（Cloud Lookup All）] です。ファイルがどのように評価されるかを確認する場合は、クラウドルックアップを使用します。ファイルが評価される方法に納得したら、後でブロッキング ポリシーに切り替えることができます。

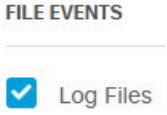
他にも、マルウェアをブロックするために使用できるポリシーがあります。これらのポリシーは、ファイル制御やMicrosoft Office、またはOfficeおよびPDFドキュメントのアップロードのブロックと関連しています。つまり、これらのポリシーを使用すると、マルウェアがブロックされるだけでなく、ユーザはこれらのファイルタイプを他のネットワークに送信できなくなります。ニーズに合う場合は、これらのポリシーを選択できます。

この例では、[マルウェアをすべてブロック（Block Malware All）] を選択します。



f) [ロギング（Logging）] タブをクリックして、[ファイルイベント（File Events）] の下にある [ファイルのロギング（Log Files）] が選択されていることを確認します。

デフォルトでは、ファイル ポリシーを選択するとファイル ロギングは有効化されます。イベントおよびダッシュボードにファイルおよびマルウェア情報を表示するには、ファイル ロギングを有効化が必要です。



g) [OK] をクリックして変更を保存します。

ステップ 3 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

次のタスク

この時点から、ファイルまたはマルウェアが送信される場合に、監視ダッシュボードおよびイベントにファイル タイプやファイルおよびマルウェアのイベントに関する情報が表示されます。この情報を評価し、ファイルの送信に関してネットワークにさらにセキュリティ対策が必要かどうかを決定できます。

アクセプタブル ユース ポリシー（URL フィルタリング）の実装方法

ネットワークのアクセプタブル ユース ポリシーを設定できます。アクセプタブル ユース ポリシーは、組織で適切とされるネットワーク アクティビティと、不適切とされるアクティビティを区別します。通常、これらのポリシーはインターネットの使用に注目し、生産性の維持、法的責任の回避（敵対的でない作業場所の維持など）、Web トラフィックの制御を目的としています。

URL フィルタリングを使用して、アクセス ポリシーと共にアクセプタブル ユース ポリシーを定義できます。広範なカテゴリ（ギャンブルなど）でフィルタリングできるため、ブロックする Web サイトを個別に識別する必要はありません。カテゴリの照合では、サイトの関連レピュテーションを指定して、許可またはブロックすることもできます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と出没する可能性があります。

次の手順で、URL フィルタリングを使用してアクセプタブル ユース ポリシーを実装する方法について説明します。この例では、複数のカテゴリのあらゆるレピュテーションのサイト、高リスクのソーシャル ネットワーキング サイト、および未分類サイトである badsite.example.com をブロックします。

手順

ステップ 1 まだ有効化していない場合は、[URL] ライセンスを有効化します。

URL カテゴリとレピュテーションの情報を使用する場合、またはこれらの情報をダッシュボードとイベントに表示する場合には、URL ライセンスを有効にする必要があります。現在、評価ライセンスを使用している場合は、ライセンスの評価版が有効化されています。デバイスを登録している場合、必要なライセンスを購入して、Cisco.com の Smart Software Manager アカウントに追加する必要があります。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) [スマートライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

c) **[URL]** グループの [有効化（Enable）] をクリックします。

必要に応じて、システムはライセンスをアカウントに登録したり、評価ライセンスを有効化したりします。グループのライセンスが有効なことが示され、ボタンは [無効化（Disable）] ボタンに変わります。

ステップ 2 URL フィルタリングのアクセス コントロール ルールを作成します。

ブロッキング ルールの作成前に、ユーザがアクセスしているサイトのカテゴリを最初に確認できます。その場合、許可するカテゴリ（金融など）に [Allow] アクションを設定したルールを作成できます。すべての Web 接続のインスペクションを実行して、URL がこのカテゴリに属しているかどうかを判断する必要があるため、金融以外のサイトのカテゴリ情報も取得します。

ただし、ブロック対象とすることがすでに判明している URL カテゴリが存在する場合があります。ブロッキング ポリシーでもインスペクションが強制されるため、ブロックされるカテゴリだけでなく、ブロックされないカテゴリへの接続に関するカテゴリ情報も取得します。

a) メイン メニューで [ポリシー（Policies）] をクリックします。

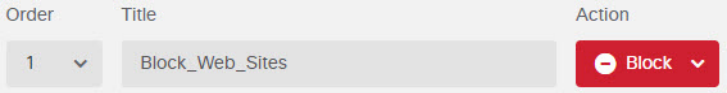
[アクセスコントロール（Access Control）] ポリシーが表示されることを確認します。

b) [+] をクリックして新しいルールを追加します。
c) 順序、タイトル、およびアクションを設定します。

- [順序（Order）]：デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上位）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルール

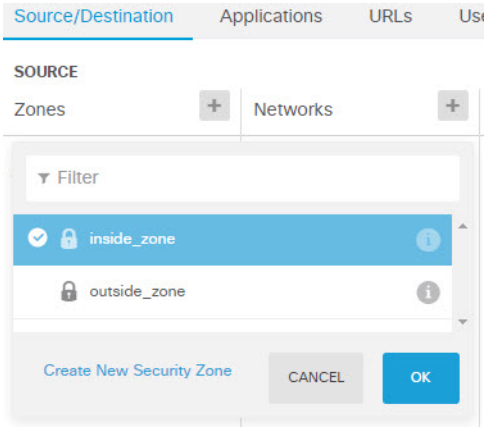
の 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセス コントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。

- [タイトル（Title）]：ルールに Block_Web_Sites などの意味のある名前を付けます。
- [アクション（Action）]：[ブロック（Block）] を選択します。

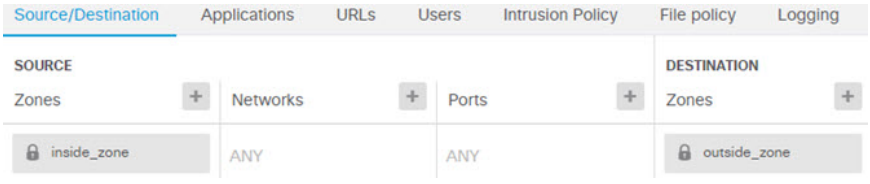


d) [送信元/接続先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。

条件の追加も同じ方法です。[+] をクリックすると小さいダイアログ ボックスが開くため、追加する項目をクリックします。複数の項目をクリックできます。選択した項目をクリックすると選択が解除されます。チェック マークは、選択済みの項目を示します。ただし、[OK（OK）] ボタンをクリックするまでポリシーには何も追加されません。項目を選択するだけでは不十分です。



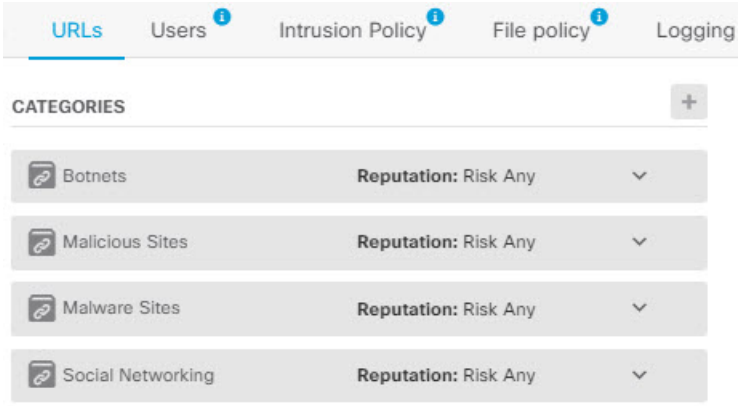
e) 同じ技術を使用して、**[接続先（Destination）]** > **[ゾーン（Zones）]** で [outside_zone] を選択します。



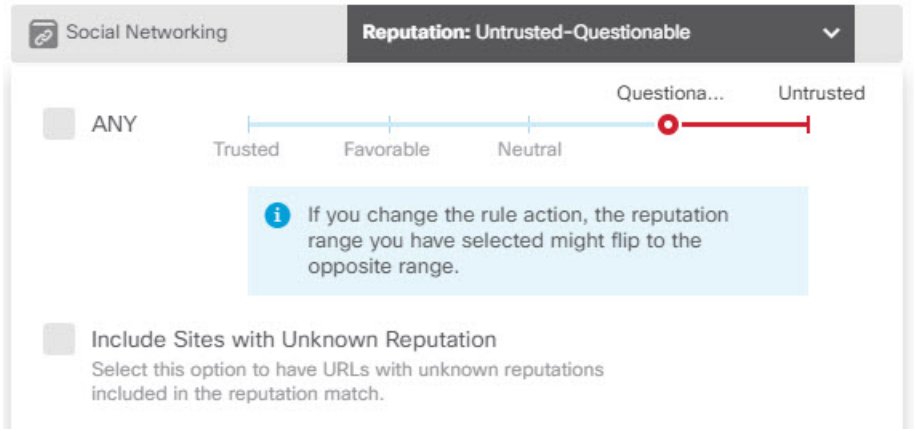
f) [URLs] タブをクリックします。

g) [カテゴリ（Categories）] の [+] をクリックして、完全または部分的にブロックするカテゴリを選択します。

この例では、ボットネット、悪意のあるサイト、マルウェアサイト、およびソーシャルネットワーキングを選択します。ブロックすることが必要な可能性が高い追加カテゴリがあります。ブロックしたいサイトがわかっていても、そのカテゴリがわからない場合は、[URL to Check] フィールドに URL を入力し、[Go] をクリックします。ルックアップ結果を示す Web サイトが表示されます。



h) レピュテーションに影響されるブロッキングを [Social Networking] カテゴリに実装するには、そのカテゴリの [Reputation: Risk Any] をクリックして、[Any] の選択を解除してからスライダを [Questionable] に移動します。閉じるには、スライダをクリックします。



レピュテーション スライダの左側は許可されるサイトを示し、右側はブロックされるサイトを示します。この場合、レピュテーションが [Questionable] と [Untrusted] の範囲内にあるソーシャル ネットワーキング サイトのみがブロックされます。したがって、ユーザは、リスクの少ない、一般的に使用されるソーシャル ネットワーキング サイトにはアクセスできます。

レピュテーションが不明な URL をレピュテーション一致に含めるには、[レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] オプションを選択します。通常、新しいサイトは評価されていません。また、その他の理由でサイトのレピュテーションが不明である（または判断できない）場合もあります。

レピュテーションを使用すると、別の方法で許可したカテゴリ内のサイトを選択的にブロックできます。

i) カテゴリ リストの左側にある [URLS] リストの横の [+] をクリックします。

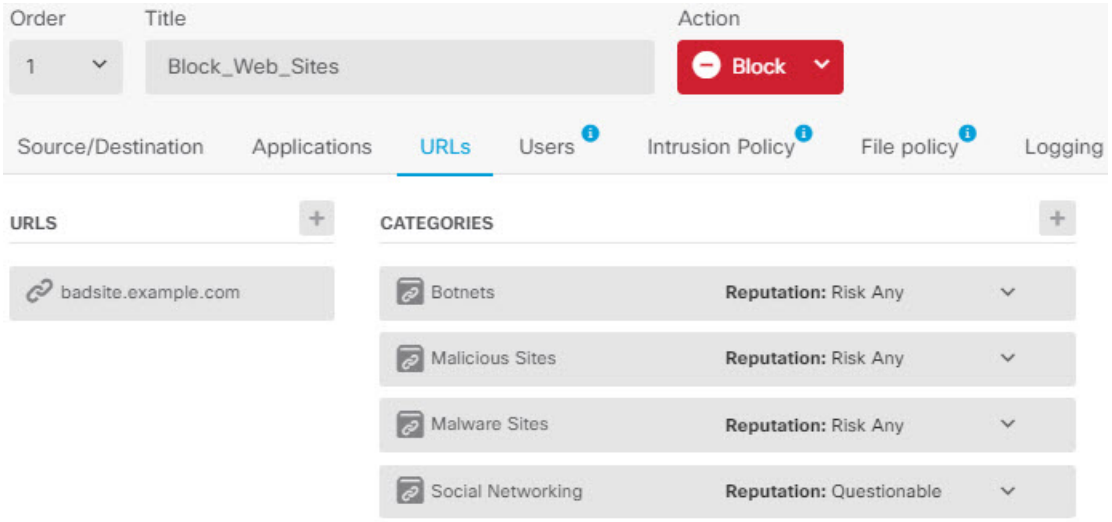
j) ポップアップ ダイアログ ボックスの下部で、[新規URLの作成（Create New URL）] リンクをクリックします。

k) 名前とURLの両方に「badsite.example.com」と入力して、[追加（Add）]、[OK] の順にクリックしてオブジェクトを作成します。

オブジェクトにURLと同じ名前を付けるか、またはオブジェクトに別の名前を付けることができます。URL には、URL のプロトコル部分を含めず、サーバ名のみを追加します。

l) 新規オブジェクトを選択して、[OK] をクリックします。

ポリシーの編集時に新規オブジェクトを追加するだけで、リストにオブジェクトが追加されます。新規オブジェクトは、自動的に選択されません。



m) [ロギング（Logging）] タブをクリックして、**[ログアクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）]** を選択します。

Web カテゴリ ダッシュボードおよび接続イベントにカテゴリおよびレピュテーションの情報を表示するには、ロギングを有効化する必要があります。

n) [OK] をクリックしてルールを保存します。

ステップ 3 （オプション）URL フィルタリングを設定します。

URL ライセンスが有効化されている場合、システムは Web カテゴリ データベースへの更新を自動的に有効化します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。何らかの理由で更新を希望しない場合は、更新をオフにできます。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) **[システム設定（System Settings）] > [トラフィック設定（Traffic Settings）] > [URL フィルタリングの設定（URL Filtering Preferences）]** をクリックします。
c) [URL クエリ ソース（URL Query Source）] で、推奨オプションの [ローカル データベースと Cisco Cloud（Local Database and Cisco Cloud）] を選択します。

インストールされている URL データベースにサイトのカテゴリがない場合、Cisco Cloud にカテゴリが含まれている可能性があります。クラウドからカテゴリとレピュテーションが返されると、カテゴリベースのルールを URL 要求に正しく適用できます。メモリ制限によりインストールされる URL データベースが小さいローエンドのシステムでは、このオプションを選択することが重要です。

あるいは、ルックアップをローカル データベースまたは Cisco Cloud に制限できます。

d) 妥当な [URL 存続可能時間（URL Time to Live）]（24 時間など）を選択します。
e) [Save] をクリックします。

ステップ 4 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

次のタスク

この時点で、URL カテゴリとレピュテーション、およびドロップされた接続に関する情報が監視ダッシュボードとイベントに表示され始めます。この情報を評価して、URL フィルタリングによって好ましくないサイトのみがドロップされているかどうか、または特定カテゴリのレピュテーション設定を緩和する必要があるかどうかを判断できます。

分類およびレピュテーションに基づいて Web サイトへのアクセスをブロックすることを、ユーザに事前に通知することについて検討します。

アプリケーションの使用を制御する方法

ブラウザ ベースのアプリケーション プラットフォームか、企業ネットワークの内部および外部で転送として Web プロトコルを使用するリッチ メディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになっています。

Threat Defense では、接続のインスペクションを実行して、使用するアプリケーションを決定します。これにより、特定の TCP/UDP ポートをターゲットにするのではなく、アプリケーションをターゲットとしたアクセス コントロール ルールを記述できるようになります。したがって、Web ベース アプリケーションが同じポートを使用していても、それらを選択的にブロックまたは許可できます。

特定のアプリケーションを許可またはブロックするよう選択できますが、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性に基づいてルールを記述することもできます。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーション ディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

この使用例では、[アノニマイザー/プロキシ（anonymizer/proxy）] カテゴリに属するアプリケーションをブロックします。

始める前に

この使用例では、使用例 ネットワーク トラフィックを調べる方法 （55 ページ） を完了していることを前提としています。その使用例では、[アプリケーション（Applications）] ダッシュボードで分析できる、アプリケーションの使用状況に関する情報を取得する方法について説明しています。実際に使用されているアプリケーションを理解することで、効率的なアプリケーションベースのルールを設計できます。また、その使用例では、VDB の更新をスケジュールする方法についても説明しています（ここでは繰り返しません）。アプリケーションを正しく識別できるように、定期的に VDB を更新してください。

手順

ステップ 1 アプリケーションベースのアクセス コントロール ルールを作成します。

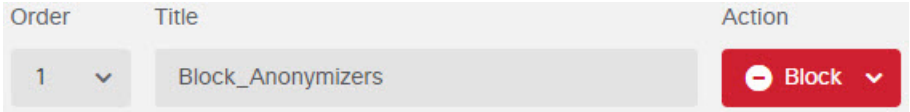
a) メイン メニューで [ポリシー（Policies）] をクリックします。

[アクセスコントロール（Access Control）] ポリシーが表示されることを確認します。

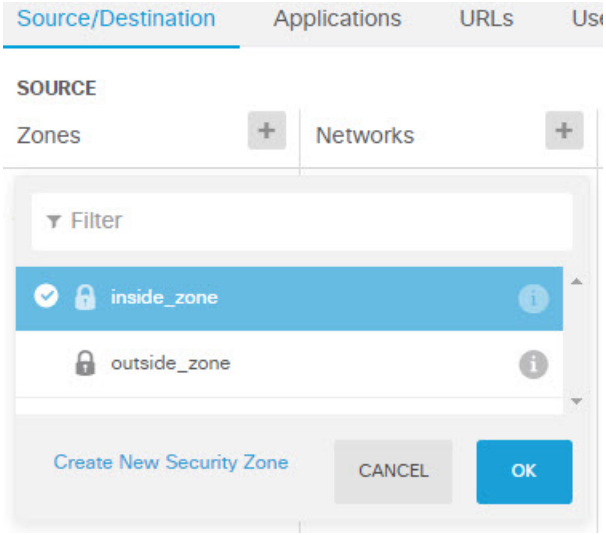
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

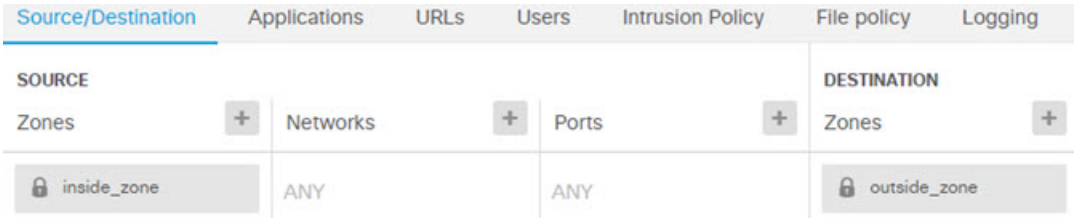
- [順序（Order）]：デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上位）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです）。このルールでは、デバイスの初期設定時に作成した Inside_Outside_Rule と同じ送信元/宛先を使用します。他のルールも同様に作成できます。アクセス コントロールの効率を最大化するには、早い段階で特定のルールを設定し、接続が許可されるか拒否されるかを迅速に決定できるようにすることが最善の方法です。この例では、ルールの順序として [1] を選択します。
- [タイトル（Title）]：ルールに Block_Anonymizers などの意味のある名前を付けます。
- [アクション（Action）]：[ブロック（Block）] を選択します。



d) [送信元/接続先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。



e) 同じ技術を使用して、**[接続先（Destination）]** > **[ゾーン（Zones）]** で [outside_zone] を選択します。



f) [アプリケーション（Applications）] タブをクリックします。

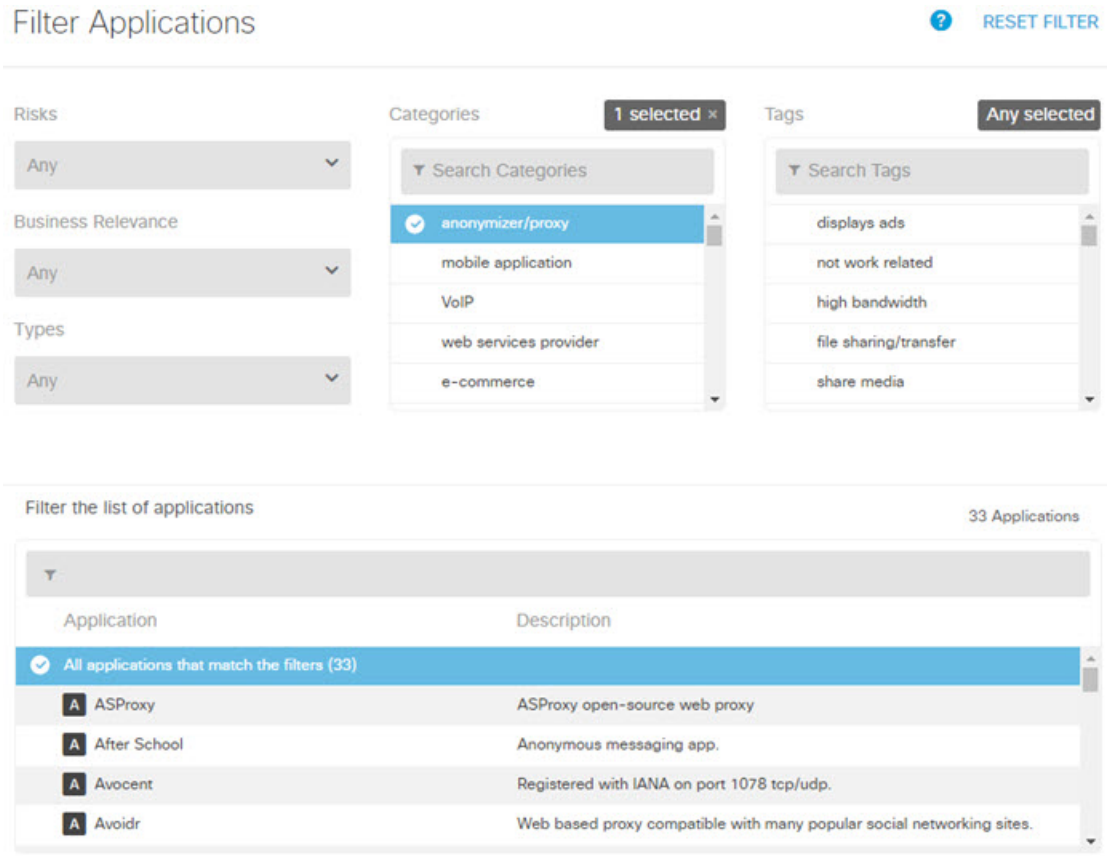
g) [アプリケーション（Applications）] の [+] をクリックして、ポップアップ ダイアログ ボックスの下部にある [高度なフィルタ（Advanced Filter）] リンクをクリックします。

事前にアプリケーション フィルタ オブジェクトを作成して、ここの [アプリケーション フィルタ（Application Filters）] リストで選択できますが、アクセス コントロール ルールで条件を直接指定して、オプションで条件をフィルタ オブジェクトとして保存することもできます。単一のアプリケーションにルールを記述していない場合は、[高度なフィルタ（Advanced Filter）] ダイアログ ボックスを使用して、より簡単にアプリケーションを検索して適切な条件を生成できます。

条件を選択すると、ダイアログ ボックスの下部にある [アプリケーション（Applications）] リストが更新され、条件に一致するアプリケーションが表示されます。記述したルールは、これらのアプリケーションに適用されます。

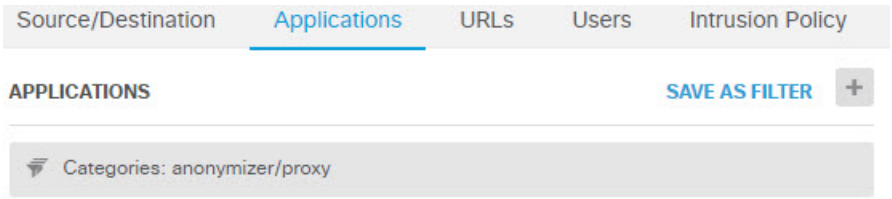
このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、TFPT は非常に高リスクに分類されています。ほとんどの組織は、このアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストは VDB の更新で変更できることを覚えておいてください。

この例では、[カテゴリ（Categories）] リストからアノニマイザー/プロキシを選択します。



h) [高度なフィルタ（Advanced Filters）] ダイアログ ボックスで、[追加（Add）] をクリックします。

フィルタが追加され、[アプリケーション（Applications）] タブに表示されます。



i) [ロギング（Logging）] タブをクリックして、**[ログアクションの選択（Select Log Action）] > [接続の開始時と終了時（At Beginning and End of Connection）]** を選択します。

このルールによってブロックされる接続の情報を取得するには、ロギングを有効化する必要があります。

j) [OK] をクリックしてルールを保存します。

ステップ 2 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 3 [モニタリング（Monitoring）] をクリックして、結果を評価します。

これで、[ネットワークの概要（Network Overview）] ダッシュボードのアプリケーション ウィジェットにドロップされた接続が表示されます。[すべて（All）]/[拒否（Denied）]/[許可（Allowed）] ドロップダウン オプションを使用して、ドロップされたアプリケーションのみに焦点を当てます。

アプリケーションに関する情報は、[Webアプリケーション（Web Applications）] ダッシュボードで検索することもできます。[アプリケーション（Applications）] ダッシュボードにプロトコル関連の結果が表示されます。これらのアプリケーションを使用しようとするユーザがいる場合、アイデンティティ ポリシーが有効で認証が必要なことを前提として、接続を試行しているユーザとアプリケーションを関連付けることができます。

サブネットを追加する方法

デバイスに使用可能なインターフェイスがある場合、スイッチ（または別のルータ）に接続して、別のサブネットにサービスを提供できます。

サブネットを追加する潜在的な理由は多数あります。この使用例では、次の一般的なシナリオに対処します。

- サブネットは、プライベート ネットワーク 192.168.2.0/24 を使用する内部ネットワークです。
- ネットワークのインターフェイスには、スタティック アドレス 192.168.2.1 があります。この例では、物理インターフェイスはこのネットワーク専用です。別の方法では、すでに接続されているインターフェイスを使用して、新しいネットワークのサブインターフェイスを作成します。
- デバイスは、DHCP を使用してネットワーク上のワークステーションにアドレスを提供します。アドレス プールとして 192.168.2.2 ～ 192.168.2.254 を使用します。
- 他の内部ネットワークおよび外部ネットワークへのネットワーク アクセスは、許可されます。外部ネットワークに移動するトラフィックでは、NAT を使用してパブリック アドレスを取得します。

（注） この例では、ブリッジグループに未使用のインターフェイスは含まれていないことを前提としています。現在、未使用のインターフェイスがブリッジ グループ メンバーである場合、次の手順に進む前にこれをブリッジ グループから削除する必要があります。

始める前に

ネットワーク ケーブルを新しいサブネットのインターフェイスおよびスイッチに物理的に接続します。

手順

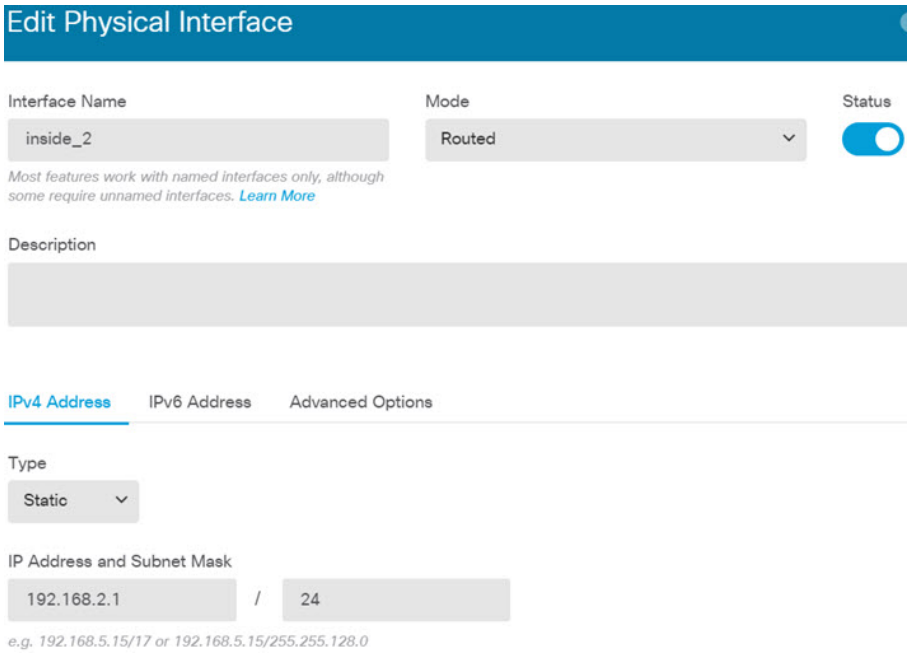
ステップ 1 インターフェイスを設定します。

a) [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、次にインターフェイスタイプをクリックして、インターフェイスのリストを表示します。

b) 接続しているインターフェイスの行の右側にある [アクション（Actions）] セルにマウスを合わせて、[編集（edit）] アイコン（  ）をクリックします。

c) 基本的なインターフェイスのプロパティを設定します。

- [名前（Name）]：インターフェイスに固有の名前 （[Inside_2] など）。
- [モード（Mode）]：[ルーテッド（Routed）] を選択します。
- [ステータス（Status）]：ステータストグルをクリックして、インターフェイスを有効化します。
- [IPv4アドレス（IPv4 Address）] タブ：[タイプ（Type）] に [スタティック（Static）] を選択して、[192.168.2.1/24] を入力します。



d) [保存（Save）] をクリックします。

インターフェイス リストに、更新されたインターフェイス ステータスと設定された IP アドレスが表示されます。

ステップ 2 インターフェイスの DHCP サーバを設定します。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]

b) **[システム設定（System Settings）] > [DHCPサーバ（DHCP Server）]** をクリックします。

c) [DHCPサーバ（DHCP Servers）] タブをクリックします。

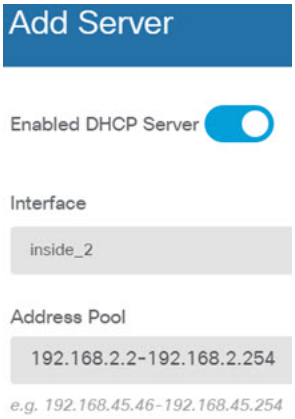
表に、既存の DHCP サーバが表示されます。デフォルト設定を使用している場合、リストには内部インターフェイスのいずれかが含まれます。

d) 表の上部の [+] をクリックします。

e) サーバのプロパティを設定します。

- [DHCPサーバの有効化（Enable DHCP Server）]：このトグルをクリックして、サーバを有効化します。
- [インターフェイス（Interface）]：DHCP サービスを提供しているインターフェイスを選択します。この例では、inside_2 を選択します。
- [アドレスプール（Address Pool）]：サーバがネットワーク上のデバイスに供給できるアドレス。192.168.2.2 ～ 192.168.2.254 を入力します。ネットワーク アドレス（.0）、インターフェイス アドレス（.1）、またはブロードキャスト アドレス（.255）が含まれないようにしてください。また、ネットワーク上のデバイスにスタティック アドレスが必要な場合は、プールからそれらのアドレスを除外します。プールは単一の連続

したアドレスである必要があるため、範囲の最初または最後からスタティックアドレスを選択します。



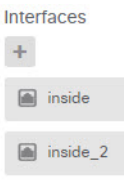
f) [追加（Add）] をクリックします。

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

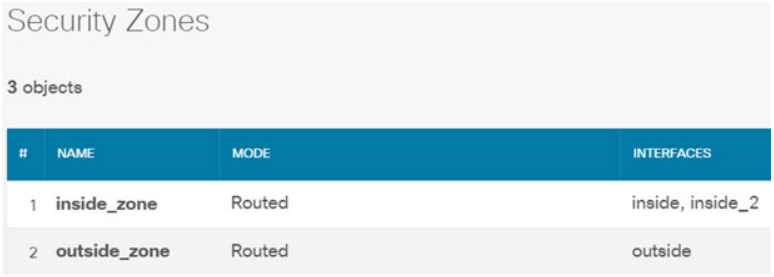
ステップ 3 内部セキュリティ ゾーンにインターフェイスを追加します。

インターフェイスにポリシーを記述するには、インターフェイスはセキュリティゾーンに属している必要があります。セキュリティゾーンのポリシーを記述します。そのため、ゾーンでインターフェイスを追加および削除すると、インターフェイスに適用されたポリシーは自動的に変更されます。

a) メイン メニューで [オブジェクト（Objects）] をクリックします。
b) オブジェクトの目次から、[セキュリティゾーン（Security Zones）] を選択します。
c) [inside_zone] オブジェクトの行の右側にある [アクション（Actions）] セルにマウスを合わせて、[編集（edit）] アイコン（）をクリックします。
d) [インターフェイス（Interfaces）] の下にある [+] をクリックして、inside_2 インターフェイスを選択し、インターフェイス リストで [OK] をクリックします。



e) [保存（Save）] をクリックします。



ステップ 4 内部ネットワーク間のトラフィックを許可するアクセス コントロール ルールを作成します。

トラフィックは、すべてのインターフェイス間で自動的には許可されません。希望のトラフィックを許可するには、アクセス コントロール ルールを作成する必要があります。唯一の例外は、アクセス コントロール ルールのデフォルト アクションでトラフィックを許可している場合です。この例では、デバイスのセットアップ ウィザードで設定したブロックのデフォルト アクションを保持していることを前提としています。したがって、内部インターフェイス間のトラフィックを許可するルールを作成する必要があります。このようなルールをすでに作成している場合は、この手順をスキップします。

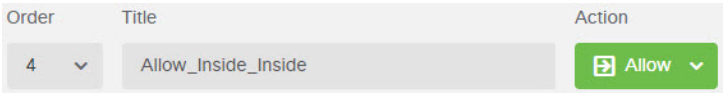
a) メイン メニューで [ポリシー（Policies）] をクリックします。

[アクセスコントロール（Access Control）] ポリシーが表示されることを確認します。

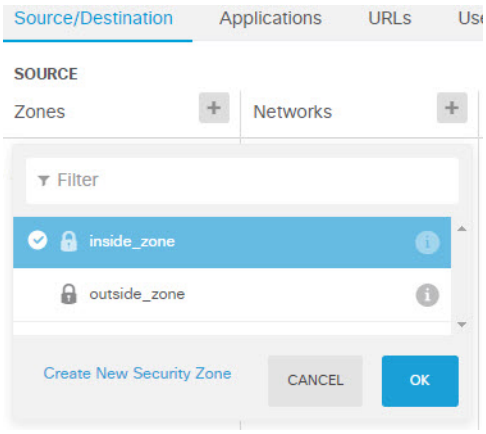
b) [+] をクリックして新しいルールを追加します。

c) 順序、タイトル、およびアクションを設定します。

- [順序（Order）]：デフォルトで、新しいルールはアクセス コントロール ポリシーの最後に追加されます。ただし、同じ送信元/宛先および他の条件を照合するルールの前（上位）にこのルールを配置する必要があります。そうしなければ、ルールは照合されません（接続で照合されるルールは、テーブル内で最初に照合されるルールの 1 つのみです）。このルールでは、一意の送信元/宛先条件を使用するため、リストの最後にルールを追加できます。
- [タイトル（Title）]：ルールに Allow_Inside_Inside などの意味のある名前を付けます。
- [アクション（Action）]：[許可（Allow）] を選択します。

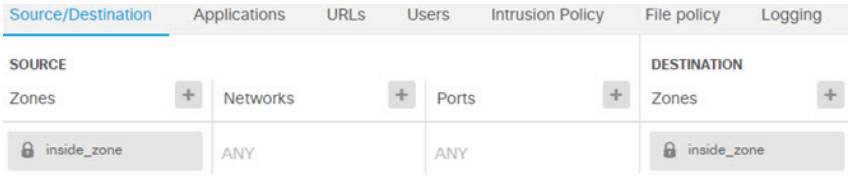


d) [送信元/接続先（Source/Destination）] タブで、**[送信元（Source）]** > **[ゾーン（Zones）]** の [+] をクリックし、[inside_zone] を選択してから、ゾーンのダイアログボックスで [OK] をクリックします。



e) 同じ方法で、**[宛先（Destination）]** > **[Zones（ゾーン）]** の [inside_zone] を選択します。

送信元および宛先に同じゾーンを選択するには、セキュリティ ゾーンに 2 つ以上のインターフェイスが含まれている必要があります。



f) （オプション）侵入およびマルウェアのインスペクションを設定します。

内部インターフェイスは信頼できるゾーン内にありますが、一般的に、ユーザはラップトップをネットワークに接続します。そのため、ユーザは、外部ネットワークまたはWi-Fi ホット スポットからネットワーク内に、知らないうちに脅威を持ち込んでいます。したがって、内部ネットワーク間を移動するトラフィックに侵入やマルウェアの形跡がないかスキャンが必要な場合があります。

次の操作の実行を検討します。

- [侵入ポリシー（Intrusion Policy）] タブをクリックして侵入ポリシーを有効化し、スライダを使用して [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーを選択します。
- [ファイルポリシー（File Policy）] タブをクリックして、[すべてのマルウェアをブロックする（Block Malware All）] ポリシーを選択します。

g) [ロギング（Logging）] タブをクリックして、**[ログアクションの選択（Select Log Action）]** > **[接続の開始時および終了時（At Beginning and End of Connection）]** を選択します。

このルールに一致する接続に関する情報を取得するには、ロギングを有効化する必要があります。ロギングによってダッシュボードにスタティックが追加され、イベント ビューアにイベントが表示されます。

h) [OK] をクリックしてルールを保存します。

ステップ 5 新規サブネットに必要なポリシーが定義されていることを確認します。

inside_zone セキュリティ ゾーンにインターフェイスを追加することによって、inside_zone の既存のポリシーが自動的に新規サブネットに適用されます。ただし、ポリシーのインスペクションには時間がかかるため、ポリシーの追加が必要ないことを確認します。

デバイスの初期設定を完了すると、次のポリシーがすでに適用されています。

- [アクセスコントロール（Access Control）]：Inside_Outside_Rule は、新規サブネットと外部ネットワーク間のすべてのトラフィックを許可します。以前の使用例に従っている場合、ポリシーによって侵入およびマルウェアのインスペクションも提供されます。新規ネットワークと外部ネットワークの間の一部のトラフィックを許可するルールが必要です。このルールがなければ、ユーザはインターネットや他の外部ネットワークにアクセスできません。
- [NAT]：InsideOutsideNATrule は、外部インターフェイスに対するすべてのインターフェイスに適用され、インターフェイス PAT が適用されます。このルールを守っている場合、新規ネットワークから外部に移動するトラフィックの IP アドレスは、外部インターフェイスの IP アドレスの一意のポートに変換されます。すべてのインターフェイスまたは inside_zone インターフェイスに適用されるルールがない場合、外部インターフェイスに移動するときに新しいルールの作成が必要になる場合があります。
- [アイデンティティ（Identity）]：デフォルトのアイデンティティ ポリシーはありません。ただし、以前の使用例に従っている場合、新規ネットワークの認証に必要なアイデンティティ ポリシーがある可能性があります。適用されるアイデンティティ ポリシーがなく、新規ネットワークのユーザベース情報が必要な場合は、新しいポリシーを作成します。

ステップ 6 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

次のタスク

新規サブネットのワークステーションが DHCP を使用して IP アドレスを取得していることと、そのワークステーションが他の内部ネットワークおよび外部ネットワークに到達できることを確認します。監視ダッシュボードおよびイベント ビューアを使用して、ネットワークの使用状況を評価します。

ネットワーク上のトラフィックをパッシブにモニタする方法

脅威に対する防御デバイスは通常、アクティブなファイアウォールおよびIPS（侵入防御システム）セキュリティデバイスとして展開されます。デバイスの中核的機能は、ネットワークに対するアクティブな保護を提供し、不必要な接続や脅威を排除することにあります。

ただし、システムはパッシブモードで展開することもでき、その場合、デバイスは監視対象のスイッチポート上のトラフィックだけを分析します。このモードは、主にデモやテスト目的で使用されます。そうすることで、デバイスをアクティブなファイアウォールとして展開する前にそのデバイスに慣れることができます。パッシブ展開を使用すると、ネットワーク上に現れる脅威の種類（ユーザが参照しているURLカテゴリなど）をモニタできます。

パッシブモードは、通常はデモやテスト目的で使用しますが、防御のないIDS（侵入検知システム）など、必要なサービスが提供される場合は、実稼働環境でパッシブモードを使用することもできます。パッシブインターフェイスをアクティブなファイアウォールのルーテッドインターフェイスと混在させることで、組織が必要とする的確なサービスの組み合わせを提供できます。

次の手順では、限られた数のスイッチポートからのトラフィックを分析するために、システムをパッシブに展開する方法を説明します。

（注） この例は、ハードウェア 脅威に対する防御 デバイス向けです。Threat Defense Virtual にパッシブモードを使用することもできますが、ネットワークの設定は異なります。詳細は、Threat Defense Virtual パッシブインターフェイスの VLAN の設定（343 ページ）を参照してください。それ以外の場合、Threat Defense Virtual にはこの手順が適用されます。

始める前に

次の手順は、内部インターフェイスと外部インターフェイスに接続し、デバイスの初期セットアップウィザードが完了していることを前提としています。パッシブ展開の場合でも、システムデータベースの更新をダウンロードするためにインターネットに接続する必要があります。また、Device Manager を開くために管理インターフェイスにも接続できる必要があります。これは、内部ポートまたは管理ポートへの直接接続を介して可能です。

この例では、**[ポリシー（Policies）]** > **[侵入（Intrusion）]**ページで、侵入ポリシーの syslog を有効にしていることも前提としています。

手順

ステップ 1 スイッチ ポートを SPAN（スイッチド ポート アナライザ）ポートとして設定し、送信元インターフェイスのモニタリング セッションを設定します。

次の例では、Cisco Nexus 5000 シリーズ スイッチの 2 つの送信元インターフェイスに SPAN ポートとモニタリング セッションを設定します。異なる種類のスイッチを使用している場合は、必要なコマンドが異なることがあります。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

確認するには、次の手順に従います。

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ 2 脅威に対する防御 インターフェイスをスイッチの SPAN ポートに接続します。

脅威に対する防御デバイス上の現在未使用のポートを選択することをお勧めします。スイッチの設定例に基づいて、スイッチのイーサネット 1/48 にケーブルを接続します。これはモニタリング セッションの宛先インターフェイスです。

ステップ 3 脅威に対する防御 インターフェイスをパッシブモードで設定します。

a) [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、[インターフェイス（Interfaces）] または [EtherChannel（EtherChannels）] をクリックします。

b) 編集する物理インターフェイスまたは EtherChannel の編集アイコン（  ）をクリックします。

現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブ インターフェイスに変換する場合は、最初にセキュリティ ゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

d) 次を設定します。

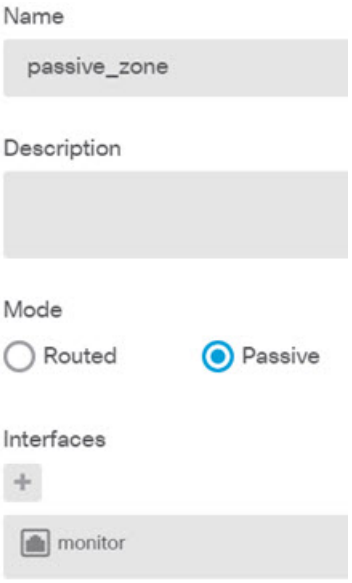
- [インターフェイス名（Interface Name）]：最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、**monitor** などです。

• [モード（Mode）]：[パッシブ（Passive）] を選択します。

e) [OK] をクリックします。

ステップ 4 インターフェイスのパッシブ セキュリティ ゾーンを作成します。

a) [オブジェクト（Objects）] を選択し、次に目次から [セキュリティ ゾーン（Security Zones）] を選択します。
b) [+] ボタンをクリックします。
c) オブジェクトの名前を入力し、任意で説明を入力します。例、**passive_zone**。
d) [モード（Mode）] で [パッシブ（Passive）] を選択します。
e) [+] をクリックして、パッシブ インターフェイスを選択します。



f) [OK] をクリックします。

ステップ 5 パッシブ セキュリティ ゾーン用の 1 つ以上のアクセス制御ルールを設定します。

作成するルールの数と種類は、収集する情報によって異なります。たとえば、IDS（侵入検知システム）としてシステムを設定する場合は、割り当てられた侵入ポリシーを設定した [許可（Allow）] ルールが少なくとも 1 つは必要です。URL カテゴリ データを収集する場合は、URL カテゴリの仕様を含むルールが少なくとも 1 つは必要です。

[ブロック（Block）] ルールを作成して、ルーテッド インターフェイスでアクティブにブロックされる接続を確認できます。インターフェイスがパッシブなので、それらの接続は実際にはブロックされませんが、システムによるネットワーク上のトラフィックの調整方法は明確に確認できます。

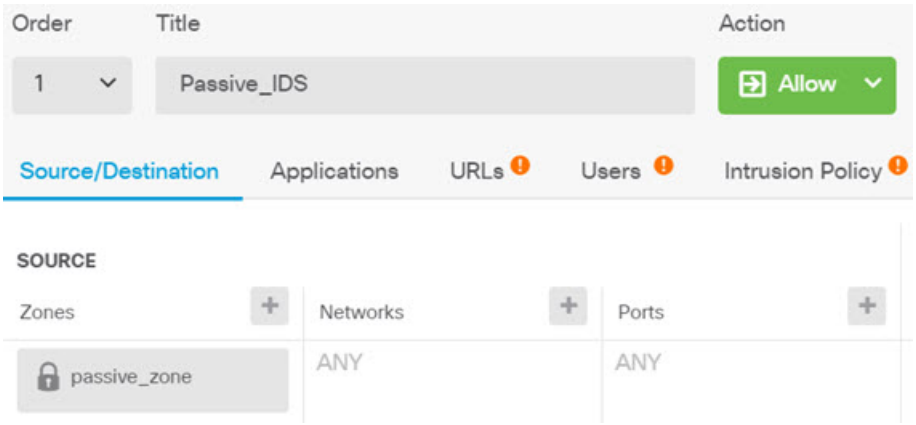
次の使用例では、アクセス制御ルールの主な使用方法について説明します。それらの使用例は、パッシブ インターフェイスにも当てはまります。作成するルールの送信元ゾーンとしてパッシブ セキュリティ ゾーンを選択します。

- 脅威をブロックする方法 （64 ページ）
- マルウェアをブロックする方法 （70 ページ）
- アクセプタブル ユース ポリシー（URL フィルタリング）の実装方法 （73 ページ）
- アプリケーションの使用を制御する方法 （79 ページ）

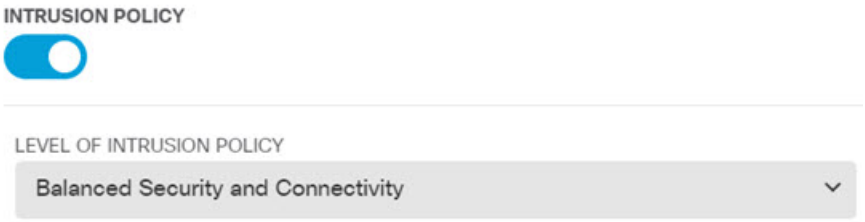
次の手順では、侵入ポリシーを適用して、URL カテゴリ データを収集する 2 つの [許可（Allow）] ルールを作成します。

a) **[ポリシー（Policies）] > [アクセス コントロール（Access Control）]** を選択します。
b) [+] をクリックして、すべてのトラフィックを許可するが、侵入ポリシーを適用するルールを追加します。
c) ルールの順序として **1** を選択します。このルールはデフォルトのルールよりも具体的ですが、デフォルトのルールとはオーバーラップしません。カスタム ルールがすでにある場合は適切な位置を選択し、パッシブ インターフェイス向けのトラフィックが代わりにそれらのルールと一致しないようにします。
d) ルールの名前、**Passive_IDS** などを入力します。
e) [アクション（Action）] として [許可（Allow）] を選択します。
f) [送信元/宛先（Source/Destination）] タブの **[送信元（Source）] > [ゾーン（Zones）]** でパッシブ ゾーンを選択します。このタブの他の設定は変更しないでください。

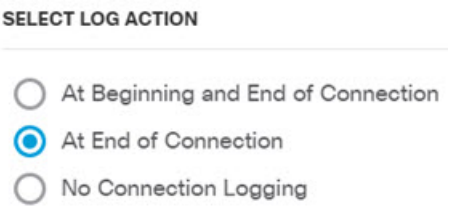
この時点で、評価モードで実行中のルールは次のようになります。



g) [侵入ポリシー（Intrusion Policy）] タブをクリックし、スライダをクリックして [オン（On）] にして、ほとんどのネットワークに推奨される [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーなどの侵入ポリシーを選択します。



h) [ロギング（Logging）] タブをクリックし、ロギング オプションで [接続の終了時（At End of Connection）] を選択します。



i) [OK] をクリックします。

j) [+] をクリックして、URL およびすべての HTTP 要求のカテゴリを判断するためにシステムがディープ インスペクションを実行する必要があるルールを追加します。

このルールにより、ダッシュボードでURLカテゴリ情報を確認できるようになります。処理時間を短縮し、パフォーマンスを向上させるために、URLカテゴリ条件を指定する少なくとも1つのアクセス制御ルールが存在する場合にのみシステムはURLカテゴリを判断します。

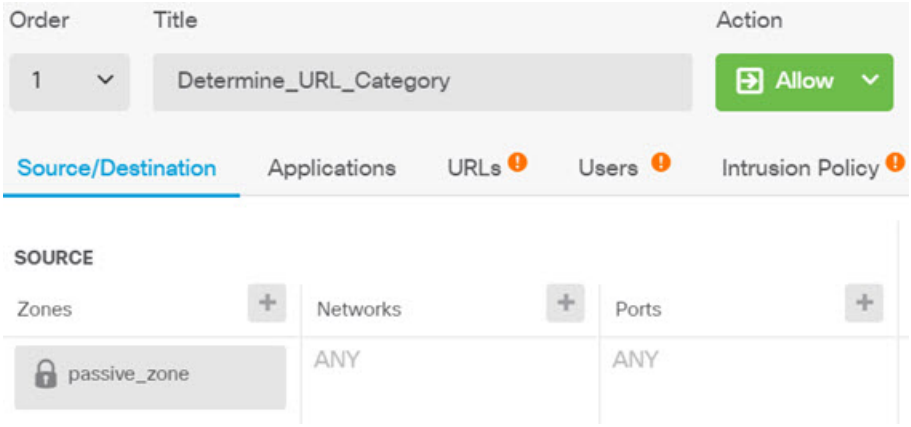
k) ルールの順序として **1** を選択します。これは、前のルール（Passive_IDS）の上に配置されます。（すべてのトラフィックに適用される）ルールの後に配置すると、今作成しているルールは決して一致しません。

l) ルールの名前、**Determine_URL_Category** などを入力します。

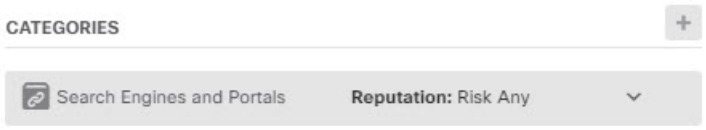
m) [アクション（Action）] として [許可（Allow）] を選択します。

または、[ブロック（Block）] を選択できます。いずれのアクションでも、このルールの目的が達成されます。

n) [送信元/宛先（Source/Destination）] タブの **[送信元（Source）] > [ゾーン（Zones）]** でパッシブ ゾーンを選択します。このタブの他の設定は変更しないでください。



o) [URL（URLs）] タブをクリックし、[カテゴリ（Categories）] 見出しの横にある [+] をクリックして、いずれかのカテゴリを選択します。たとえば、**[Search Engines and Portals]** を選択します。必要に応じて、レピュテーション レベルを選択するか、デフォルトの [任意（Any）] のままにします。



p) [侵入ポリシー（Intrusion Policy）] タブをクリックし、スライダをクリックして [オン（On）] にして、最初のルールに選択したのと同じ侵入ポリシーを選択します。

q) [ロギング（Logging）] タブをクリックし、ロギング オプションで [接続の終了時（At End of Connection）] を選択します。

ただし、アクションとして [ブロック（Block）] を選択した場合は、[接続の開始時と終了時（At Beginning and End of Connection）] を選択します。ブロックされた接続自体は終了しないため、接続の開始時にのみログ情報を取得できます。

r) [OK] をクリックします。

ステップ 6 （オプション）その他のセキュリティ ポリシーを設定します。

次のセキュリティポリシーも設定して、トラフィックにどのような影響を与えるかを確認できます。

- [アイデンティティ（Identity）]：ユーザ情報を収集します。アイデンティティ ポリシーにルールを設定して、送信元 IP アドレスに関連付けられているユーザが確実に特定されるようにできます。パッシブ インターフェイスのアイデンティティ ポリシーの実装プロセスは、ルーテッド インターフェイスのプロセスと同じです。ネットワーク トラフィックを調べる方法 （55 ページ）で説明されている使用例を参照してください。
- [セキュリティインテリジェンス（Security Intelligence）]：既知の不正な IP アドレスと URL をブロックします。詳細は、脅威をブロックする方法 （64 ページ）を参照してください。

（注） パッシブインターフェイス上のすべての暗号化されたトラフィックは復号不可として分類されるため、SSL 復号化ルールは無効になり、パッシブインターフェイスには適用されません。

ステップ 7 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 8 監視ダッシュボードを使用して、ネットワーク経由で到達するトラフィックや脅威の種類を分析します。脅威に対する防御デバイスに不要な接続をアクティブにドロップさせる場合は、デバイスを再展開して、監視対象ネットワークに対するファイアウォール保護を提供するアクティブなルーテッド インターフェイスを設定できます。

その他の例

使用例の章の例に加えて、特定のサービスについて説明している一部の章で設定例が示されています。場合によっては次の例が役立つ可能性があります。

アクセス制御

- Trustsec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法 （631 ページ）

Network Address Translation（NAT）

IPv4 アドレス用の NAT

- 内部 Web サーバーへのアクセスの提供（スタティック自動 NAT） （741 ページ）
- FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック自動 NAT） （744 ページ）
- 宛先に応じて異なる変換（ダイナミック手動 PAT） （751 ページ）
- 宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT） （756 ページ）
- DNS 応答修正：外部の DNS サーバー （769 ページ）
- DNS 応答修正：ホスト ネットワーク上の DNS サーバー （773 ページ）
- NAT からのサイト間 VPN トラフィックの除外 （809 ページ）

IPv6 アドレス用の NAT

- NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット （726 ページ）
- NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク （729 ページ）
- NAT66 の例：ネットワーク間のスタティック変換 （735 ページ）
- NAT66 の例：シンプルな IPv6 インターフェイス PAT （737 ページ）
- DNS 64 応答修正 （763 ページ）

リモート アクセス仮想プライベート ネットワーク（RA VPN）

- RADIUS 認可変更の実装方法 （868 ページ）
- Duo LDAP を使用した二要素認証の設定方法 （878 ページ）
- 外部インターフェイスでリモート アクセス VPN ユーザーにインターネット アクセスを提供する方法（ヘア ピニング） （887 ページ）
- リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方法 （892 ページ）
- グループによって RA VPN アクセスを制御する方法 （908 ページ）
- 異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法 （913 ページ）
- セキュアクライアント のアイコンとロゴをカスタマイズする方法 （917 ページ）

サイト間仮想プライベート ネットワーク（VPN）

- NAT からのサイト間 VPN トラフィックの除外 （809 ページ）
- 外部インターフェイスで外部のサイト間 VPN ユーザーにインターネット アクセスを提供する方法（ヘア ピニング） （816 ページ）
- サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法 （823 ページ）

SSL/TLS の復号

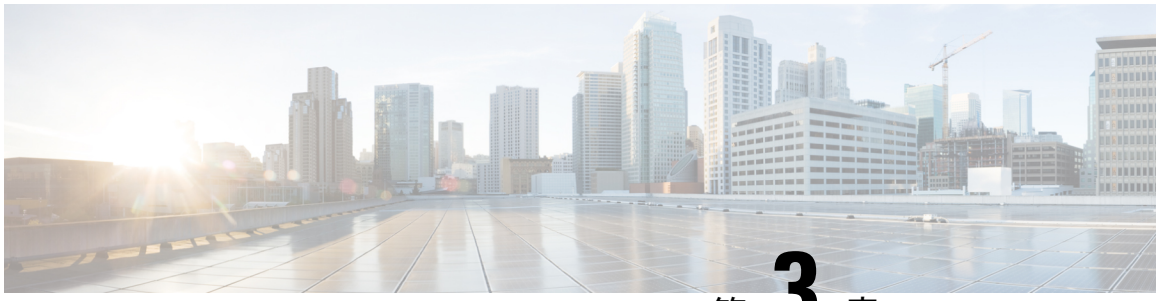
- 例：ネットワークからの古い SSL/TLS バージョンのブロック （563 ページ）

FlexConfig ポリシー（FlexConfig Policy）

- グローバル デフォルト インスペクションを有効/無効にする方法 （1058 ページ）
- FlexConfig の変更を元に戻す方法 （1064 ページ）
- 一意のトラフィック クラスのインスペクションを有効にする方法 （1066 ページ）

仮想ルーティング

- 重複するアドレス空間を持つ複数の仮想ルータへのインターネットアクセスを提供する方法 （421 ページ）
- 複数の仮想ルータを介して遠隔サーバーにルーティングする方法 （415 ページ）
- 異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法 （913 ページ）
- サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法 （823 ページ）



第 3 章

システムのライセンス

ここでは、Threat Defense デバイスにライセンスを付与する方法について説明します。

ファイアウォールシステムのスマートライセンス

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。

Cisco Smart Software Manager

Threat Defense 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（https://software.cisco.com/#SmartLicensing-Inventory）で管理します。Cisco Smart Software Manager を使用すると、組織のプライマリアカウントを作成できます。

デフォルトでは、ライセンスはプライマリアカウントの下のデフォルト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、たとえば、地域、部門、または子会社ごとに、追加の仮想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アプライアンスの管理を行うことができます。

ライセンスとアプライアン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アプライアンスのみが、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。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

Cisco Smart Software Manager にデバイスを登録する際は、製品インスタンスの登録トークンを Cisco Smart Software Manager で作成し、そのトークンを Device Manager に入力します。登録済みデバイスが、使用されているトークンに基づいて仮想アカウントに関連付けられます。

Cisco Smart Software Manager の詳細については、マネージャのオンライン ヘルプを参照してください。

ライセンス認証局との定期通信

Threat Defense デバイスの登録に製品インスタンス登録トークンを使用すると、デバイスはシスコのライセンス認証局に登録されます。ライセンス認証局は、デバイスとライセンス認証局の間の通信用に 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 ヵ月ごとに更新されます。ID証明書の期限が切れた場合（通常は、9ヵ月または1年間通信がない状態）、デバイスは登録が解除された状態になり、ライセンスされた機能は使用停止になります。

デバイスは、定期的にライセンス認証局と通信します。Cisco Smart Software Manager に変更を加えた場合は、すぐに変更が有効になるようにデバイス上で認証を更新できます。また、スケジュールどおりにデバイスが通信するのを待つこともできます。通常のライセンスに関する通信は 12 時間ごとに行われますが、これには猶予期間があり、デバイスはホームをコールすることなく最大で 90 日間は動作します。90 日が経過する前にライセンス認証局と連絡を取る必要があります。

スマート ライセンスのタイプ

次の表に、Threat Defense デバイスで使用可能なライセンスを示します。

Threat Defense デバイスを購入すると、自動的にEssentialsライセンスが含まれます。すべての追加ライセンスはオプションです。

表 *2:* スマート ライセンスのタイプ

ライセンス	期間	付与される機能
Essentials	永久	オプションのターム ライセンスでカバーされないすべての機能。 Essentials ライセンスは登録時にアカウントに自動的に追加されます。ただし、Secure Firewall 3100 の場合は例外です。ファイアウォールを購入すると、基本ライセンスが取得され、そのライセンスはアカウントに含まれる他のライセンスと同様に管理されます。たとえば、登録時にライセンスが正しいバーチャルアカウントに含まれていることを確認する必要があります。 [このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）]かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。
IPS	ターム ベース	次のポリシーを使用するために必要です。 • 侵入（Intrusion） • ファイル（File）（マルウェア防御 も必要） • セキュリティ インテリジェンス（Security Intelligence）
マルウェア防御	ターム ベース	ファイルポリシー（IPS も必要）
URL	ターム ベース	URLポリシー：カテゴリおよびレピュテーションベースの URL フィルタリングまたは DNS ルックアップ要求フィルタリング。 このライセンスなしでも、個々のURLでURLフィルタリングを実行できます。

ライセンス	期間	付与される機能
RA VPN： • Secure Client Advantage • Secure Client Premier • Secure Client VPN のみ	ライセンスタイプに基づきタームベースまたは永久	リモートアクセス VPN の設定RA VPN を設定するには、基本ライセンスによるエクスポート制御機能を許可する必要があります。デバイスを登録するときに、エクスポート要件を満たすかどうかを選択します。 Device Manager は、任意の有効な セキュアクライアント ライセンスを使用できます。使用できる機能はライセンス タイプによって異なります。まだ購入していない場合は、リモートアクセス VPN のライセンス要件（837 ページ）を参照してください。 『*Cisco AnyConnect Ordering Guide*』（http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf）も参照してください。
通信事業者	ターム ベース	モバイル ネットワーク プロトコルのインスペクション。GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定するには、このライセンスが必要です。これらのインスペクションを設定するには、FlexConfig を使用します。

Threat Defense Virtual のライセンス

このセクションでは、Threat Defense Virtual で使用可能なパフォーマンス階層ライセンスの権限について説明します。

すべての Threat Defense Virtual ライセンスを、サポートされているすべての Threat Defense Virtual vCPU/メモリ構成で使用できます。これにより、Threat Defense Virtual 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実行できるようになります。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。Threat Defense Virtual VM を設定する場合、サポートされる最大コア（vCPU）数は 16 個です。また、サポートされる最大メモリ容量は 32 GB RAM です。

Threat Defense Virtual スマートライセンスのパフォーマンス階層

RA VPN に対するセッション制限は、インストールされている Threat Defense Virtual プラットフォームの権限付与階層によって決定され、レートリミッタによって適用されます。次の表は、権限付与層とレート制限に基づくセッション制限をまとめたものです。

表 *3 : Threat Defense Virtual* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

Threat Defense Virtual パフォーマンス階層ライセンスのガイドラインと制限事項

Threat Defense Virtual デバイスのライセンスを取得する際は、次の注意事項と制限事項に注意してください。

- Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。
- すべての Threat Defense Virtual ライセンスを、サポートされているすべての Threat Defense Virtual コア/メモリ構成で使用できます。これにより、Threat Defense Virtual 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実行できるようになります。
- Threat Defense Virtual を展開する際、デバイスが評価モードであるか、すでに Cisco Smart Software Manager に登録されているかに関係なく、パフォーマンス階層を選択できます。

（注） お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。使用アカウントにあるライセンスと一致する階層を選択することが重要です。Threat Defense Virtual をバージョン 7.0 にアップグレードする場合は、[FTDv - Variable] を選択して現在のライセンスコンプライアンスを維持できます。Threat Defense Virtual は、ご使用のデバイスの機能（コア/RAM の数）に基づいてセッション制限を引き続き実行します。

- REST API を使用して、新しい Threat Defense Virtual デバイスを展開する場合や Threat Defense Virtual をプロビジョニングする場合、デフォルトのパフォーマンス階層は FTDv50 です。

- Essentials ライセンスはサブスクリプションベースで、パフォーマンス階層にマッピングされます。バーチャルアカウントには、Threat Defense Virtual デバイスの Essentials ライセンス権限と、IPS 、マルウェア防御、および URL のライセンスが必要です。
- 各 HA ピアは 1 つの権限を消費します。各 HA ピアの権限は Essentials ライセンスを含めて一致している必要があります。
- HA ペアのパフォーマンス階層の変更は、プライマリピアに適用される必要があります。
- ユニバーサル PLR ライセンスは、HA ペアの各デバイスに個別に適用されます。セカンダリデバイスが、プライマリデバイスのパフォーマンス階層を自動的にミラーリングすることはありません。手動で更新する必要があります。

暗号化機能に対するエクスポート制御設定の影響

デバイスを登録する場合、**このトークンに登録された製品の輸出規制された機能を許可する**かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。

評価モードは、非輸出準拠アカウントを使用して登録する場合と同じように扱われます。つまり、評価モードで実行している場合、リモートアクセス VPN を設定したり、高度な暗号化アルゴリズムを使用したりはできません。

特に、DES 標準は評価モードまたは非輸出準拠モードでのみ使用できます。

したがって、サイト間 VPN などの暗号化機能を設定したり、高アベイラビリティグループのフェールオーバー接続を暗号化したりすると、輸出準拠アカウントに登録した後に接続の問題が発生する可能性があります。機能が評価モードで DES を使用していた場合、アカウントの登録後にその機能の設定が破損します。

暗号化関連の問題を回避するには、次の推奨事項を考慮してください。

- サイト間 VPN や暗号化されたフェールオーバー接続などの暗号化機能は、デバイスを登録するまで設定しないでください。
- 輸出準拠アカウントを使用してデバイスを登録した後、評価モードで設定したすべての暗号化機能を編集し、より安全な暗号化アルゴリズムを選択します。各暗号化機能をテストおよび検証して、正しく機能していることを確認します。

（注） 評価モードで HA フェールオーバー暗号化を設定した場合は、HA グループ内の両方のデバイスをリブートして、より強力な暗号化の使用を開始する必要もあります。両方のデバイスが自身をアクティブユニットと見なすスプリットブレイン状態を回避するために、最初に暗号化を削除することを推奨します。

期限切れまたは無効なオプション ライセンスの影響

次のいずれかのオプションライセンスが期限切れになっても、そのライセンスを必要とする機能は引き続き使用できます。ただし、ライセンスは非準拠とマークされます。ライセンスを準拠状態に戻すには、ライセンスを購入してアカウントに追加する必要があります。

オプションのライセンスを無効にすると、システムは次のように反応します。

- マルウェア防御：システムは Secure Malware Analytics Cloud への問い合わせを停止し、Secure Malware Analytics Cloud から送信される遡及的イベントの確認応答も停止します。ファイルポリシーが含まれている既存のアクセス コントロール ポリシーは再展開できません。マルウェア防御ライセンスが無効にされた後、システムが既存のキャッシュファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは Unavailable という性質をこれらのファイルに割り当てます。
- IPS ：システムは、侵入ポリシーまたはファイルポリシーを適用しなくなります。セキュリティ インテリジェンス ポリシーの場合、システムはこのポリシーを適用せず、フィード更新のダウンロードを停止します。ライセンスを必要とする既存のポリシーを再展開することはできません。
- [URL]：URL カテゴリ条件を使用したアクセスコントロールルールは URL または DNS ルックアップ要求のフィルタリングを直ちに停止し、システムは URL データに対する更新をダウンロードしなくなります。既存のアクセス コントロール ポリシーに、カテゴリベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。
- [RA VPN]：リモート アクセス VPN 設定は編集できませんが、削除は可能です。ユーザーは引き続き RA VPN 設定を使用して接続できます。ただし、デバイスの登録を変更してシステムがエクスポートに準拠しなくなると、リモート アクセス VPN 設定はただちに停止し、リモート ユーザーは VPN に接続できなくなります。

スマート ライセンスの管理

システムの現在のライセンス ステータスを表示するには、[スマートライセンス（Smart License）] ページを使用します。システムにはライセンスが必要です。

このページには、90 日間の評価ライセンスを使用しているかどうか、または Cisco Smart Software Manager に登録済みかどうかが表示されます。登録すると、Cisco Smart Software Manager への接続のステータス、および各ライセンス タイプのステータスを確認できます。

使用認証により、スマート ライセンス エージェントのステータスが特定されます。

- 承認済み（「接続/接続中」、「十分なライセンス」）：デバイスは、アプライアンスのライセンス権限を承認した License Authority に正常に登録されています。このデバイスはインコンプライアンスの状態です。

- アウトオブコンプライアンス：デバイスで使用可能なライセンス権限がありません。ライセンスされた機能は動作を継続します。ただし、インコンプライアンスにするためには、追加の権限を購入するか、または解放する必要があります。
- 認証期限切れ：デバイスは 90 日以上ライセンス認証局と通信していません。ライセンスされた機能は動作を継続します。この状態の場合、スマート ライセンス エージェントは認証要求を再試行します。再試行に成功すると、エージェントはアウトオブコンプライアンスまたは承認済み状態になり、新たな承認期間が始まります。手動でデバイスの同期を試します。

（注） スマート ライセンスのステータスの横にある [i] ボタンをクリックすると、バーチャル アカウント、輸出管理機能を確認でき、Cisco Smart Software Manager を開くリンクが表示されます。輸出管理機能により、国家安全保障、外交ポリシー、反テロリズム法令を対象としたソフトウェアが制御されます。

次の手順では、システム ライセンスの管理方法の概要について説明します。

始める前に

システムのインターネットへのパスがない場合は、スマートライセンスを使用できません。代わりに、パーマネントライセンス予約（PLR）モードに切り替えます。詳細については、エアギャップネットワークでの永久ライセンスの適用 （111 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 デバイスを登録します。

オプション ライセンスを割り当てる前に、Cisco Smart Software Manager に登録する必要があります。評価期間の終了前に登録してください。

デバイスの登録 （107 ページ）を参照してください。

（注） 登録する際に、使用状況データをシスコに送信するかどうかを選択します。選択内容は、[歯車（gear）] アイコンの横にある [Cisco Success Networkにアクセス（Go To Cisco Success Network）] リンクをクリックすると変更できます。

ステップ 3 オプション機能のライセンスをリクエストして管理します。

ライセンスによって制御される機能を使用するためには、オプション ライセンスを登録する必要があります。オプション ライセンスの有効化または無効化 （109 ページ）を参照してください。

ステップ 4 システム ライセンスを維持します。

次の作業を実行できます。

- Cisco Smart Software Manager との同期 （110 ページ）
- デバイスの登録解除 （111 ページ）

デバイスの登録

Threat Defense デバイスを購入すると、自動的に Essentials ライセンスが含まれます。Essentials ライセンスは、オプションライセンスではカバーされないすべての機能をカバーしています。これは永久ライセンスです。

システムの初期設定時に、Cisco Smart Software Manager にデバイスを登録するように求められます。登録せずに 90 日間の評価ライセンスを使用する場合、評価期間の終了前にデバイスを登録する必要があります。

デバイスを登録すると、バーチャル アカウントからデバイスにライセンスが割り当てられます。デバイスを登録すると、有効にしているすべてのオプション ライセンスも登録されます。

始める前に

デバイスの登録時には、そのデバイスだけが登録されます。高可用性のために設定されているデバイスの場合は、その装置を登録するために、高可用性ペアにあるその他の装置にログインする必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 **[Register Device]** をクリックして、説明に従います。

a) リンクをクリックして Cisco Smart Software Manager を開いて自分のアカウントにログインするか、必要に応じて新しいアカウントを作成します。

b) 新しいトークンを生成します。

トークンを作成する際に、トークンの有効使用期間を指定します。推奨の有効期間は 30 日です。この期間はトークン自体の有効期限を定義するものであるため、トークンを使用して登録するデバイスには影響しません。使用前にトークンが期限切れになった場合は、簡単に新しいトークンを生成できます。

[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] かどうかも指定する必要があります。このオプションは、自国が輸出管理の標準規格に適合している場合のみ選択できます。このオプションは、高度な暗号化や、高度な暗号化を必要とする機能の使用を制御します。

c) トークンをコピーして、[スマートライセンスの登録（Smart License Registration）] ダイアログ ボックスの編集ボックスに貼り付けます。

d) Threat Defense Virtualデバイスのパフォーマンス階層（**Threat Defense Virtualのみ**）を選択するか、デフォルトの選択のままにします。

パフォーマンス階層が選択されていない場合、Threat Defense Virtual デバイスはレガシーモードで動作します。デフォルト設定は4コア/8GBです。詳細については、Threat Defense Virtual パフォーマンス階層の変更 （108 ページ）を参照してください。

e) シスコ クラウドサービスの登録リージョンを選択します。

登録後、このリージョンを変更する必要がある場合は、デバイスの登録を解除してから再度登録し、新しいリージョンを選択する必要があります。

f) 使用状況データをシスコに送信するかどうかを決定します。

Cisco Success Network ステップの情報を読み、[サンプルデータ（Sample Data）] をクリックして収集された実際のデータへのリンクを表示して、[Cisco Success Networkを有効にする（Enable Cisco Success Network）] オプションを選択したままにするかどうかを決定します。

g) **[デバイスの登録（Register Device）]** をクリックします。

Threat Defense Virtual パフォーマンス階層の変更

Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。すべての Threat Defense Virtual ライセンスを、サポートされているすべての Threat Defense Virtual コア/メモリ構成で使用できます。これにより、Threat Defense Virtual 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実行できるようになります。Threat Defense Virtual スマートライセンスのパフォーマンス階層 （102 ページ）を参照してください。

Threat Defense Virtual をバージョン 7.0+ にアップグレードすると、デバイスは自動的に「FTDv 変数」 階層状態に移行し、権限付与レベルを選択するまで非階層化権限を使用し続けます。

次の点を考慮してください。

- スループットまたはRA VPNの要件に基づいて、導入ニーズに合わせてパフォーマンス階層を変更できます。Threat Defense Virtual は、調整可能なコアおよびメモリリソースを使用して展開することに注意してください。選択したパフォーマンス階層は、デバイスの仕様を超えることはできません。
- AWS では、パフォーマンス階層の変更はサポートされていません。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 [パフォーマンス階層（Performance Tier）] ドロップダウンリストから目的のオプションを選択します。

- FTDv5（4 コア/8 GB）
- FTDv10（8 コア/8 GB）
- FTDv20（8 コア/8 GB）
- FTDv30（8 コア/16 GB）
- FTDv50（12 コア/24 GB）
- FTDv100（16 コア/24 GB）

（注） 現在のデバイス仕様に基づいて最適な階層が強調表示されます。

ステップ 3 選択内容とデバイスの仕様を確認します。

（注） Threat Defense Virtual VM を設定する場合、サポートされる最大コア（vCPU）数は 12 個です（VMware および KVM での FTDv100 の場合は 16 個）。また、サポートされる最大メモリ容量は 24 GB RAM です。選択したパフォーマンス階層は、デバイスの仕様を超えることはできません。

ステップ 4 [はい（Yes）] をクリックして、パフォーマンス階層を変更します。

オプション ライセンスの有効化または無効化

オプションのライセンスを有効化（登録）または無効化（リリース）できます。ライセンスによって制御される機能を使用するには、ライセンスを有効にする必要があります。

オプションのタームライセンスの対象となる機能を使用しなくなった場合、ライセンスを無効化できます。ライセンスを無効にすると、Cisco Smart Software Manager アカウントでライセンスがリリースされるため、別のデバイスにそのライセンスを適用できるようになります。

評価モードで動作させる場合は、これらのライセンスの評価バージョンを有効にすることもできます。評価モードでは、デバイスを登録するまでライセンスは Cisco Smart Software Manager に登録されません。ただし、評価モードでは RA VPN ライセンスまたはキャリアライセンスを有効化できません。

始める前に

ライセンスを無効にする前に、そのライセンスが使用中でないことを確認します。ライセンスを必要とするポリシーは書き換えるか削除します。

高可用性の設定で動作する装置の場合は、アクティブな装置でのみライセンスを有効化または無効化します。スタンバイ装置が必要なライセンスを要求（または解放）すると、次の設定の

展開時にスタンバイ装置に変更内容が反映されます。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 必要に応じて、それぞれのオプション ライセンスの [有効化/無効化（Enable/Disable）] コントロールをクリックします。

- [有効化（Enable）]：Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化（Disable）]：Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。

ステップ 3 RA VPN ライセンスを有効にしている場合、アカウントで使用可能なライセンス タイプを選択します。

Cisco Smart Software Manager との同期

ライセンス情報は、定期的に Cisco Smart Software Manager と同期されます。通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、アプライアンスはホームをコールすることなく最大で 90 日間は動作します。

しかし、Smart Software Manager に変更を加えた場合は、デバイス上で認証を更新し、即座に変更を有効にできます。

同期により、ライセンスの現在のステータスが取得され、認証と ID 証明書が更新されます。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 歯車のドロップダウンリストから [接続の再同期（Resync Connection）] を選択します。

デバイスの登録解除

デバイスを使用しなくなった場合は、Cisco Smart Software Manager からデバイスの登録を解除できます。登録を解除すると、仮想アカウントでデバイスに関連付けられているEssentialsライセンスとすべてのオプションライセンスが解放されます。オプションライセンスは他のデバイスに割り当てることができます。また、デバイスはクラウドおよびクラウドサービスから登録解除されます。

デバイスの登録を解除すると、デバイスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

始める前に

デバイスの登録解除時には、そのデバイスだけが登録解除されます。ハイアベイラビリティのために設定されているデバイスの場合は、その装置を登録解除するために、ハイアベイラビリティ ペアにあるその他の装置にログインする必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 歯車ドロップダウンリストから [デバイスの登録解除（Unregister Device）] を選択します。

ステップ 3 警告を確認し、デバイスの登録を本当に解除する場合は [登録解除（Unregister）] をクリックします。

エアギャップネットワークでの永久ライセンスの適用

エアギャップネットワークは、インターネットへのパスがないネットワークです。これらは、外部からの侵入や攻撃の可能性を完全に防ぐことを目指した高セキュリティネットワークです。インターネットへのパスがないため、Cisco Smart Software Manager にデバイスを直接登録することはできません。代わりに、永久ライセンス予約（PLR）モードを使用して、デバイスに適用可能なライセンスを取得できます。

PLR モードを使用する必要がある場合は、次のことに注意してください。

- ファイルポリシー、URL ルックアップ、パブリック Web サイトへの状況に応じた相互起動といった、インターネットへのアクセスを必要とする機能は使用できません。
- Web 分析と Cisco Success Network を有効にしても、インターネットへのアクセスがないため、シスコは関連データを収集しません。
- 地理位置情報データベース、侵入ルール、および脆弱性データベース（VDB）に更新を手動でアップロードする必要があります。たとえば、更新をフラッシュドライブにダウンロードし、そのドライブをセキュリティ保護された建物に持ち込んで、セキュリティ保護されたワークステーションからアップロードすることができます。

（注） Cisco Smart Software Manager は、デバイスのシリアル番号を使用して永久ライセンスを割り当てます。デバイスの登録を解除する必要があるものの、通常の登録解除プロセスまたはキャンセルプロセスでライセンス割り当ての削除に失敗した場合、シスコテクニカルサポートに連絡して、Cisco Smart Software Manager から登録を削除する必要があります。デバイスを再イメージ化しても、ライセンス登録は削除されません。

次のトピックでは、各タイプの永久ライセンス、それらを適用する方法、およびデバイスの登録をキャンセルまたは解除する方法について詳しく説明します。

ユニバーサル永久ライセンスと特定ライセンス予約

ライセンス予約には、次の 2 つの異なるタイプがあります。

- ユニバーサル永久ライセンス予約（ユニバーサル PLR または UPLR）：ユニバーサル永久ライセンスでは、サポートされているファイアウォール製品（すべてのオプションライセンスを含む）を無期限かつ無制限で使用できます。ユニバーサル永久ライセンスを購入して適用すると、適用される機能ライセンスが、無期限に適用されます（通常は時間ベース）。ただし、スマート ライセンス アカウントで有効期限が切れた場合は、交換用ライセンスを購入する必要があります。
- 特定ライセンス予約：特定ライセンス予約には、標準スマートライセンスと同じ数およびタイプのライセンスが必要です。このライセンスを取得する場合は、基本ライセンスに追加するオプションの機能ライセンスを選択します。このライセンスは有効期限があるため、定期的に更新する必要があります。

Device Manager ではユニバーサル PLR だけがサポートされています。

Cisco Smart Software Manager（CSSM）アカウントでユニバーサル永久ライセンス予約（PLR）モードを有効にする場合は、シスコの担当者と協同で作業する必要があります。

スマートアカウントがユニバーサルライセンスを提供できることの確認

永久ライセンスを取得して適用できることを確認するには、CSSMアカウントにログインし、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** > **[インベントリ（Inventory）]** ページに移動して、[ライセンス（Licenses）] タブをクリックします。[ライセンスの予約（License Reservation）] ボタンが表示された場合は、永久ライセンス予約を取得する権限があります。

ただし、このボタンを使用すると、ユニバーサルライセンスと特定の永久ライセンスの両方に対して機能するウィザードが開始します。

また、デバイスのユニバーサルライセンスがあることを確認するには、使用可能なライセンスのリストを参照する必要があります。このライセンスは、[ライセンスの予約（License

Reservation）] ボタンで起動するウィザードのステップ 2 で選択可能な項目として表示されます。

[ライセンスの予約（License Reservation）] ボタンが表示され、ユニバーサルライセンスを取得できる場合は、永久ライセンスを使用するためのシステムの変換に進めます。ボタンが表示されない場合、または特定のライセンスのみを予約できる場合は、シスコの担当者に連絡し、お客様のアカウントに対してユニバーサル PLR モードを有効にするように依頼してください。

PLR モードへの切り替えおよびユニバーサルライセンスの適用

スマートアカウントがユニバーサルライセンスを提供できることの確認（112 ページ）の説明に従い、永久ライセンスを取得できることを確認し、必要なユニバーサルライセンスを購入したら、永久ライセンス予約（PLR）モードに切り替えてライセンスを適用できます。

注意 現在評価モードになっている場合、PLR モードに切り替えた後で評価モードに戻ることはできません。

始める前に

デバイスが高可用性用に設定されている場合は、HA グループ内の両方のデバイスに対して、このタスクを個別に実行する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマート ライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 スマートライセンスを使用してすでにデバイスを登録している場合は、歯車 ドロップダウンリストから [デバイスの登録解除（Unregister Device）] を選択し、登録解除を確認します。登録解除タスクが完了するのを待ってから、次に進みます。

ステップ 3 歯車 ドロップダウンリストから [ユニバーサルPLRに切り替え（Switch to Universal PLR）] を選択して、ユニバーサル永久ライセンス予約（PLR）モードに切り替えます。

警告を読み、[はい（Yes）] をクリックしてスイッチを確認します。

システムが PLR モードに切り替わり、PLR 登録プロセスが開始されます。

ステップ 4 PLR 登録を完了します。

a) [ユニバーサル永久ライセンス予約（Universal Permanent License Reservation）] ダイアログボックスが開いたら、最初のステップで必要な要求コードを含めます。テキストファイルに保存する場合は [テキストで保存（Save AS TXT）] をクリックし、印刷する場合は [印刷（Print）] をクリックします。文字列を強調表示し、Ctrl+C を押してクリップボードにコピーすることもできます。

モードの切り替え後にプロセスをキャンセルした場合は、[ライセンス（Licensing）] ページの [予約の続行（Continue Reservation）] ボタンをクリックして、この時点から再開できます。

b) CSSM アカウントにログインし、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）] > [インベントリ（Inventory）]** ページに移動して、[ライセンス（Licenses）] タブをクリックします。

c) [ライセンス予約（License Reservation）] ボタンをクリックし、ウィザードの指示に従います。生成した要求コードの入力を求められ、入力すると、承認コードを入手できます。

ウィザードには、次のステップが含まれています。

1. ライセンス要求コードを入力するか、コードを含むテキストファイルをアップロードして、[次へ（Next）] をクリックします。
2. ステップ 2 では、ライセンスを取得しているシステムの製品の詳細と、使用可能なライセンスの箇条書きリストが表示されます。ローカルで管理されている Threat Defense デバイスのユニバーサルライセンスを選択し、[次へ（Next）] をクリックします。
3. ステップ 3 では、適切なライセンスが選択されていることを確認し、[承認コードの生成（Generate Authorization Code）] をクリックします。
4. ステップ 4 では、承認コードが表示されます。必要に応じて、[ファイルとしてダウンロード（Download As File）] または [クリップボードにコピー（Copy to Clipboard）] をクリックして、コードを保存します。
5. [Close] をクリックしてウィザードを終了します。

d) Device Manager に戻り、承認コードを適切なフィールドに貼り付けます。

ユニバーサルライセンスの有効な承認コードの形式は次のとおりです。XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX。ここで X は英数字です。承認コードが XML ファイルである場合、特定のライセンスを保有していますが、このシステムでは使用できません。PLR 登録のキャンセル （115 ページ）の説明に従って登録をキャンセルし、CSSM で予約済みライセンスをリリースしてください。次に、シスコの担当者と協力して、スマートアカウントをユニバーサル PLR に変換します。

e) [登録（Register）] をクリックします。

登録プロセスが開始されます。[ライセンス（Licensing）] ページを更新して、登録ステータスを確認します。

ステップ 5 必要に応じて、オプションの機能ライセンスを有効にします。

ユニバーサルライセンスでは、Essentialsライセンスに対してのみデバイスが登録されます。必要な機能ライセンスごとに、[有効化（Enable）] をクリックできます。

PLR 登録のキャンセル

ユニバーサル永久ライセンス予約（PLR）要求は、完了する前にキャンセルできます。たとえば、PLR 登録プロセスを開始したが、Smart Software Manager アカウントが PLR に対して設定されていない場合は、PLR モードの承認を取得している間にプロセスをキャンセルし、スマート ライセンス アカウントを適切に設定できます。

PLR 登録プロセスが完了している場合は、キャンセルできません。代わりに、PLR モードでのデバイスの登録解除 （116 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマート ライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 歯車 ドロップダウンリストから [PLRのキャンセル（Cancel PLR）] を選択して、キャンセルプロセスを開始します。

ステップ 3 状況に適したオプションを選択します。

- [CSSMにライセンスがあります（I have a license in CSSM）]：Cisco Smart Software Manager（CSSM）でライセンス登録ウィザードを実行し、承認コードを取得している場合は、このオプションを使用します。この時点で、CSSM に予約されているライセンスがあるため、それらのライセンスをリリースする必要があります。
- [CSSMにライセンスがありません（I do not have a license in CSSM）]：承認コードを取得した時点でCSSM ウィザードを完了していない場合は、このオプションを使用します。たとえば、Device Manager で PLR 登録を開始したが、自分のスマートアカウントに [ライセンス予約（License Reservation）] ボタンがないことに気付いた場合に使用します。

ステップ 4 （[CSSMにライセンスがあります（I have a license in CSSM）] を選択した場合）ライセンスが使用中としてマークされていないことを確認するには、CSSMからリリースコードを取得する必要があります。取得しないと、それらのライセンスは他のデバイスで使用可能な状態になりません。

a) （登録時に）CSSM から取得した承認コードを [キャンセル（Cancellation）] ダイアログボックスに貼り付け、[リリースコードの生成（Generate Release Code）] をクリックします。

b) [ライセンスコードのリリース（Release License Code）] フィールドにコードがある場合は、[テキストで保存（Save As TXT）] をクリックしてテキストファイルに保存するか、[印刷（Print）] をクリックして印刷します。コードを選択し、Ctrl+C を押してクリップボードにコピーすることもできます。

c) CSSM の **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** > **[インベントリ（Inventory）]** ページでデバイスを見つけ（[名前（Name）] はデバイスのシリアル番号）、**[アクション（Action）]** > **[削除（Remove）]** をクリックして、リリースコードを入力します。

CSSM に製品が正常に削除されたことが表示されるまで待ちます。

ステップ 5 [OK] をクリックしてキャンセルプロセスを完了します。

システムがスマートライセンスモードに戻ります。ただし、デバイスは登録解除されるため、評価モードは再開できません。この時点で、スマートライセンスを使用してデバイスを登録するか、PLR モードに切り替えて、使用するデバイスを再度登録する必要があります。

PLR モードでのデバイスの登録解除

デバイスの使用を停止する、別のファシリティに移動するなどによりデバイスのライセンスを必要としなくなった場合、デバイスの登録を解除できます。

デバイスの登録を解除すると、ライセンスが未使用の状態に戻ります。デバイスの登録を解除しない場合、ライセンスは使用中としてマークされたままになり、他の目的で使用することはできません。

手順

ステップ 1 [デバイス（Device）] をクリックし、[スマート ライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 歯車 ドロップダウンリストから [ユニバーサルPLRの登録解除（Unregister Universal PLR）] を選択し、警告を読み、[はい（Yes）] をクリックしてプロセスを開始します。

ステップ 3 [ユニバーサル永久ライセンス予約の登録解除（Unregister Universal Permanent License Reservation）] ダイアログボックスが開くと、[リリースライセンスコード（Release License Code）] フィールドには、CSSM アカウントに現在割り当てられているライセンスを解放するために必要なコードが入力されます。このコードのコピーを保持するには、[テキストで保存（Save as TXT）] または [印刷（Print）] をクリックします。コードを選択し、Ctrl+C を押してクリップボードにコピーすることもできます。

ステップ 4 CSSM アカウントに移動し、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）] > [インベントリ（Inventory）]** ページでデバイスを見つけ（[名前（Name）] はデバイスのシリアル番号）、**[アクション（Action）] > [削除（Remove）]** をクリックして、リリースコードを入力します。

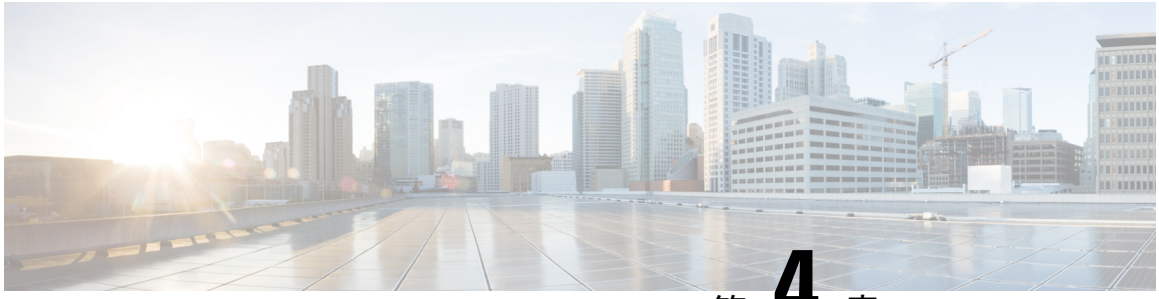
CSSM に製品が正常に削除されたことが表示されるまで待ちます。

ステップ 5 Device Manager に戻り、[デバイスの登録解除（Unregister Device）] ダイアログボックスで [登録解除（Unregister）] をクリックします。

これでプロセスは完了です。この時点で、CSSMのライセンスは他のデバイスに自由に割り当てることができ、Threat Defense デバイスのライセンスは解除されます。

第 I 部

システム モニタリング



第 4 章

デバイスのモニタリング

システムには、デバイスとデバイスを通過するトラフィックをモニターするために使用できるダッシュボードとイベント ビューアが含まれています。

トラフィック統計情報を取得するためにロギングを有効にする

モニタリング ダッシュボードおよびイベント ビューアを使用して、幅広いトラフィック統計をモニターできます。ただし、どの統計情報を収集すべきかシステムに知らせるためにロギングを有効にする必要があります。ロギングでは、システムを通過する接続に対して有用な情報を提供するさまざまな種類のイベントを生成します。

ここでは、イベントおよび提供される情報について、特に接続ロギングに重点を置いて詳しく説明します。

イベント タイプ

システムでは、以下のタイプのイベントが生成されます。監視ダッシュボードで関連する統計を表示するには、これらのイベントを生成する必要があります。

Connection Events

ユーザーが生成するトラフィックがシステムを通過する場合、この接続に対してイベントを生成できます。これらのイベントを生成するには、アクセス ルールで接続ロギングを有効にします。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールでロギングを有効にすると、接続イベントを生成できます。

接続イベントには接続に関する幅広い種類の情報が含まれ、これには送信元と宛先の IP アドレスおよびポート、使用された URL およびアプリケーション、送信されたバイト数

またはパケット数などがあります。この情報には、実行されたアクション（接続の許可またはブロックなど）、接続に適用されたポリシーも含まれます。

Intrusion Events

システムは、ネットワークを通過するパケットを検査し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある、悪意のあるアクティビティについて調べます。システムは潜在的な侵入を識別すると、侵入イベントを生成します。これには、エクスプロイトの日時とタイプ、攻撃とそのターゲットについての状況説明が記録されます。侵入イベントは、アクセス制御ルールのロギング設定に関係なく、ブロックまたはアラートするように設定された侵入ルールに対して生成されます。

ファイル イベント

ファイル イベントは、作成したファイル ポリシーに基づき、ネットワーク トラフィック内でシステムによって検出（オプションとしてブロック）されたファイルを表します。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールに対してファイル ロギングを有効にする必要があります。

システムはファイル イベントを生成する場合、基になったアクセス コントロール ルールのロギング設定にかかわらず、関連する接続の終了についても記録します。

マルウェア イベント

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。マルウェア防御 は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキストデータを含むマルウェアイベントを生成できます。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールに対してファイル ロギングを有効にする必要があります。

ファイルの判定結果は、正常からマルウェア、マルウェアから正常などに変更できます。マルウェア防御 が Secure Malware Analytics Cloudにファイルについて照会し、クエリから 1 週間以内に判定結果が変更されたことがクラウドに特定されると、システムはレトロスペクティブ マルウェア イベントを生成します。

Security Intelligence Events

セキュリティ インテリジェンス イベントは、ポリシーによってブロックまたはモニターされた各接続の、セキュリティ インテリジェンス ポリシーによって生成された接続イベントの一種です。すべてのセキュリティ インテリジェンス イベントには、自動入力された [セキュリティインテリジェンスカテゴリ（Security Intelligence Category）] フィールドがあります。

これらのイベントのそれぞれについて、対応する「通常」の接続イベントがあります。セキュリティインテリジェンスポリシーはアクセス コントロールなどのその他多数のセキュリティ ポリシーより前に評価されるため、セキュリティ インテリジェンスによって接続がブロックされると、その結果のイベントには、以降の評価から収集される情報（ユーザー アイデンティティなど）は含まれません。

設定可能な接続ロギング

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。

システムは 1 つの接続をさまざまな理由でロギングすることがあるため、1 ヵ所でロギングを無効にしても、一致する接続がロギングされないとは限りません。

接続ロギングは次の場所で設定できます。

- アクセス制御ルールおよびデフォルトアクション：接続終了時点のロギングは、接続に関するほとんどの情報を提供します。接続の開始も記録できますが、これらのイベントの情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡するトラフィックを対象とする各ルール（およびデフォルトのアクション）でこれを有効にする必要があります。
- セキュリティ インテリジェンス ポリシー：ブロックされた接続ごとにセキュリティ インテリジェンス接続イベントを生成するようにロギングを有効にすることができます。セキュリティインテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。
- SSL 復号ルールとデフォルトのアクション：接続の最後にロギングを設定できます。ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセス コントロール ルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

自動接続ロギング

他のロギング設定に関係なく、次の接続終了イベントは自動的に保存されます。

- システムは、接続がアクセス コントロール ポリシーのデフォルトのアクションで処理される限り、侵入イベントに関連付けられている接続を自動的に記録します。一致するトラフィックの侵入イベントを取得するには、デフォルトアクションでロギングを有効にする必要があります。
- システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。接続イベントのみ：必要に応じてファイルおよびマルウェア イベントの生成を無効にできます。

接続ロギングのためのヒント

ロギング設定および関連する統計情報の評価を検討する際は、次のヒントに注目してください。

- アクセス コントロール ルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、トラフィックをさらに検査し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックできます。ただし、暗号化されたペイロードに対するファイル インスペクションと侵入インスペクションはデフォルトで無効になっていることに注意してください。侵入またはファイル ポリシーが接続をブロックする理由を発見した場合、接続ログ設定を問わず、システムは接続終了イベントをただちにログに記録します。ロギングが許可された接続は、ネットワーク内のトラフィックのほとんどの統計情報を提供します。
- 信頼されている接続は、信頼アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによって処理される接続です。ただし、信頼されている接続では、ディスカバリ データ、侵入、または禁止されたファイルやマルウェアがインスペクションされません。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。
- トラフィックをブロックするアクセス コントロール ルールおよびアクセス コントロール ポリシーのデフォルト アクションの場合は、システムは接続開始イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。
- サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニターするかどうかを検討します。
- リモート アクセス VPN 接続プロファイルの設定時に、[復号されたトラフィックでアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択した場合、または **sysopt connection permit-vpn** コマンドをイネーブルにした場合は、すべてのサイト間またはリモート アクセス VPN トラフィックがインスペクションとアクセス コントロール ポリシーをバイパスします。したがって、このトラフィックに対する接続イベントは発生せず、トラフィックは統計ダッシュボードには反映されません。

外部の Syslog サーバーへのイベントの送信

イベントを格納する容量が限られている、Device Manager を通してイベントを表示する以外に、外部の Syslog サーバーにイベントを送信するルールとポリシーを設定することもできます。この機能と、選択した syslog サーバ プラットフォームの追加のストレージを使用して、イベント データを表示および分析できます。

外部の syslog サーバにイベントを送信するには、各ルール、デフォルトのアクション、または接続のログ記録を有効にするポリシーを編集し、ログ設定の syslog サーバ オブジェクトを選択します。侵入イベントを syslog サーバーに送信するには、侵入ポリシーの設定でサーバーを設定します。Syslog サーバーにファイル/マルウェア イベントを送信するには、**[デバイス（Device）] > [システム設定（System Settings）] > [ロギング設定（Logging Settings）]** でサーバーを設定します。

詳細については、各ルールとポリシーの種類に応じたヘルプおよびSyslog サーバーの設定 （175 ページ）を参照してください。

Cisco Cloud ベースのサービスを使用したイベントの評価

イベント ビューアと独自の syslog サーバーを使用することに加えて、接続イベントおよび高プライオリティの侵入/ファイル/マルウェア関連イベントをシスコのクラウドベース サーバーに送信できます。Threat Response など、シスコのクラウドベースのサービスでは、クラウド サーバーからイベントをプルし、各サービスを使用してそれぞれのイベントを評価できます。

これらのクラウドベースのサービスは、脅威に対する防御 デバイスと Device Manager で分離されています。イベントを Cisco Cloud に送信する必要があるサービスを使用することを選択する場合は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** ページで接続を有効にする必要があります。Cisco Cloud へのイベントの送信 （957 ページ） を参照してください。

トラフィックのモニタリングおよびシステム ダッシュボード

システムには、デバイスを通過するトラフィックおよびセキュリティ ポリシーの結果を分析するために使用できる複数のダッシュボードがあります。ダッシュボード情報は、構成全体の有効性を評価し、ネットワークの問題を特定して解決するために使用します。

ハイ アベイラビリティ グループ内の装置のダッシュボードには、そのデバイスの統計情報のみ表示されます。統計情報は装置間で同期されません。

（注） トラフィック関連のダッシュボードで使用されるデータは、接続またはファイル ロギングを有効にするアクセス制御ルール、およびロギングを許可するその他のセキュリティ ポリシーから収集されます。ダッシュボードには、ロギングが有効になっていないルールと一致するトラフィックは反映されません。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザー情報はユーザー ID を収集するアイデンティティ ルールを設定している場合にのみ利用できます。最後に、侵入、ファイル、マルウェア、および URL カテゴリの情報を使用できます。ただし、これを使用できるのは、これらの機能に関するライセンスを所有しており、機能を使用するルールを設定している場合のみです。

手順

ステップ 1 メイン メニューの [モニタリング（Monitoring）] をクリックして、[ダッシュボード（Dashboards）] ページを開きます。

ダッシュボードのグラフと表に表示されるデータを制御するために、定義済みの時間範囲（最後の時間や週など）を選択できます。また、特定の開始時刻と終了時刻を指定してカスタムの時間範囲を定義することもできます。

トラフィック関連のダッシュボードには、次のタイプの表示が含まれます。

- 上位 5 つの棒グラフ：これらのグラフは [ネットワークの概要（Network Overview）] ダッシュボードに表示されます。また、ダッシュボードテーブルで項目をクリックした場合、項目ごとのサマリーのダッシュボードにも表示されます。[トランザクション（Transactions）] または [データの使用状況（Data Usage）]（送受信バイトの合計）のカウント間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、または拒否トランザクションを表示するために表示を切り替えることもできます。グラフと関連付けられている表を確認する場合は、[追加表示（View More）] をクリックします。

- [テーブル（Tables）]：テーブルには、特定のタイプの項目（アプリケーションまたはURLカテゴリなど）およびその項目の合計トランザクション数、許可トランザクション数、ブロック トランザクション数、データ使用量、および送受信バイト数が表示されます。未加工の [値（Values）] と [パーセンテージ（Percentages）] 間の数字は切り替えることができ、上位 10、100、または 1000 エントリが表示されます。項目がリンクの場合、そのリンクをクリックして、より詳細な情報が含まれているサマリー ダッシュボードを表示します。

ステップ 2 目次にある [ダッシュボード（Dashboard）] リンクをクリックして、次のデータのダッシュボードを表示します。

- [ネットワークの概要（Network Overview）]：ネットワークのトラフィックに関するサマリー情報を表示します。これには、一致したアクセス ルール（ポリシー）、トラフィックを開始したユーザ、接続で使用されたアプリケーション、一致した侵入シグネチャ、アクセスされた URL の URL カテゴリ、および最も頻繁に接続される宛先が含まれます。

- [ユーザー（Users）]：ネットワークの上位ユーザーが表示されます。ユーザー情報を表示するには、アイデンティティ ポリシーを設定する必要があります。ユーザーアイデンティティがない場合は、送信元 IP アドレスが含まれます。以下の特殊なエンティティが表示される場合があります。

  - [認証失敗（Failed Authentication）]：ユーザーは認証を求められましたが、最大許容試行回数内に有効なユーザー名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザーのネットワークへのアクセスは妨げられませんが、これらのユーザーのネットワーク アクセスを制限するためのアクセス ルールを記述できます。

  - [ゲスト（Guest）]：ゲストユーザーは、これらのユーザーをゲストと呼ぶようにアイデンティティ ルールが設定されている点を除き、認証失敗ユーザーと同様です。ゲストユーザーは認証を求められましたが、最大試行回数内に認証されることができませんでした。

  - [認証不要（No Authentication Required）]：ユーザーの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザーは認証を求められませんでした。

- [不明（Unknown）]：IPアドレスのユーザーマッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

- [アプリケーション（Applications）]：ネットワークで使用されている上位アプリケーション（HTTPなど）を示します。この情報は、インスペクションを実行済みの接続にのみ提供されます。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロック ルールと一致するかどうかのインスペクションが実行されます。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Webアプリケーション（Web Applications）]：ネットワークで使用されている上位 Web アプリケーション（Google など）を示します。 Web アプリケーション情報を収集するための条件は、アプリケーション ダッシュボードの場合と同じです。
- **[URLカテゴリ（URL Categories）]**：参照する Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトのカテゴリ（ギャンブルや教育機関など）を示します。この情報を入手するには、トラフィック一致基準として URL カテゴリを使用する少なくとも 1 つのアクセス制御ルールが存在する必要があります。情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判断するためにインスペクションを実行する必要があるトラフィックに関してのみ提供されます。最初の Web カテゴリのアクセス コントロール ルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。
- [アクセスおよび SI ルール（Access And SI Rules）]：ネットワーク トラフィックで一致した上位アクセス ルールおよびセキュリティ インテリジェンス ルールに相当するものを示します。
- [ゾーン（Zones）]：デバイスに入ってから出ていくトラフィックの上位セキュリティ ゾーンのペアを示します。
- [宛先（Destinations）]：ネットワーク トラフィックの上位の宛先が表示されます。
- [攻撃者（Attackers）]：侵入イベントをトリガーする接続の送信元である上位の攻撃者が表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ターゲット（Targets）]：攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [脅威（Threats）]トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ファイルログ（File Logs）]：ネットワーク トラフィックで確認された上位のファイル タイプが表示されます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
- [マルウェア（Malware）]：上位マルウェアのアクションとディスポジションの組み合わせを示します。 ドリルダウンして、関連付けられているファイル タイプの情報を参照でき

ます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。

- 可能なアクション：マルウェア クラウドルックアップ、ブロック、アーカイブブロック（暗号化）、検出、カスタム検出、クラウドルックアップのタイムアウト、マルウェアブロック、アーカイブブロック（深さ超過）、カスタム検出ブロック、TIDブロック、アーカイブブロック（検査失敗）。
- 可能なディスポジション：マルウェア、不明、クリーン、カスタム検出、使用不可。

- [SSL復号（SSL Decryption）]：デバイスを経由した暗号化トラフィックとプレーンテキスト トラフィックの内訳、およびSSL 復号ルールに従った暗号化トラフィックの復号方法の内訳を示します。
- [システム（System）]：インターフェイスとそのステータス（マウスをインターフェイスに合わせるとIP アドレスが表示される）、全体的なシステムの平均スループット（最大1 時間で5 分間のバケット、より長い期間で1 時間のバケット）、およびシステム イベント、CPU使用率、メモリ使用率、ディスク使用率に関する概要情報の表示を含む、システムの全体図を示します。すべてのインターフェイスではなく特定のインターフェイスを表示するように、スループット グラフを制限できます。

（注） [システム（System）]ダッシュボードに表示される情報は、全体的なシステムレベルの情報です。デバイスのCLIにログインすると、さまざまなコマンドを使用して詳細情報を確認できます。たとえば、**show cpu** および **show memory** コマンドには、他の詳細を示すパラメータが含まれますが、これらのダッシュボードには **show cpu system** および **show memory system** コマンドからのデータが表示されます。

ステップ3 目次でこれらのリンクをクリックすることもできます。

- [イベント（Events）]：イベント発生時にイベントが表示する場合に選択します。個々のアクセス ルールに関連する接続イベントを表示するには、それぞれのアクセス ルールで接続のロギングを有効にする必要があります。また、セキュリティ インテリジェンス ポリシーおよびSSL 復号ルールでロギングを有効にして、セキュリティ インテリジェンス イベントおよびその他の接続イベントデータを参照します。これらのイベントは、ユーザーの接続の問題を解決するのに役立ちます。
- [セッション（Sessions）]：Device Manager ユーザーセッションを表示および管理します。詳細については、Device Manager ユーザーセッションの管理 （1003 ページ）を参照してください。

コマンドラインを使用した追加の統計情報のモニタリング

Device Manager ダッシュボードには、デバイスを介して移動するトラフィックや一般的なシステム使用状況に関連するさまざまな統計情報が表示されます。ダッシュボードが対応していない領域に関する追加情報は、CLI コンソールを使用するか、またはデバイス CLI にログインすることで得られます（CLI（コマンドライン インターフェイス）へのログイン （9 ページ）を参照）。

CLI にはこうした統計情報を提供するためのさまざまな **show** コマンドが含まれます。CLI は一般的なトラブルシューティングにも使用することが可能で、**ping** および **traceroute** といったコマンドが含まれます。ほとんどの **show** コマンドには、統計情報を 0 にリセットする **clear** コマンドがあります（CLI コンソールから統計情報をクリアすることはできません）。

コマンドのドキュメントは、Cisco Firepower Threat Defense コマンド リファレンス（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）にあります。

たとえば、次のコマンドが役に立ちます。

- **show nat** は NAT ルールのヒット数を表示します。
- **show xlate** はアクティブな実際の NAT 変換を表示します。
- **show conn** はデバイスを経由する現在の接続に関する情報を提供します。
- **show dhcpd** はインターフェイスで設定した DHCP サーバーに関する情報を提供します。
- **show interface** は各インターフェイスの使用状況の統計情報を提供します。

イベントの表示

ロギングを有効にしたセキュリティ ポリシーによって生成されるイベントを表示できます。また、イベントは、トリガーされた侵入ポリシーとファイル ポリシーから生成されます。

イベント ビューア テーブルには、リアルタイムに生成されたイベントが示されます。新しいイベントが生成されると、古いイベントはテーブルから削除されます。

始める前に

特定のタイプのイベントが生成されるかどうかは、関連するポリシーに一致する接続に加えて、次の要素によって決まります。

- 接続イベント：アクセス ルールは、接続ロギングを有効化する必要があります。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールで接続ロギングを有効にすることもできます。

- 侵入イベント：アクセス ルールは、侵入ポリシーを適用する必要があります。
- ファイルおよびマルウェア イベント：アクセスルールでファイルポリシーを適用し、ファイル ロギングを有効にする必要があります。
- セキュリティ インテリジェンス イベント：セキュリティ インテリジェンス ポリシーを有効にして設定し、ロギングを有効にする必要があります。

手順

ステップ 1 メイン メニューの [モニタリング（Monitoring）] をクリックします。

ステップ 2 コンテンツのテーブルから [イベント（Events）] を選択します。

イベント ビューアでは、イベントのタイプに基づいてイベントがタブに分類されます。詳細については、イベント タイプ （119 ページ）を参照してください。

ステップ 3 表示するイベント タイプのタブをクリックします。

イベント リストでは、次の操作を実行できます。

- イベントをより簡単に検索、分析できるようにするために、新しいイベントの追加を停止するには、[一時停止（Pause）] をクリックします。新しいイベントが表示されるようにするには、[再開（Resume）] をクリックします。
- 新しいイベントの表示速度を制御するには、別のリフレッシュ レート（5、10、20、60 秒）を選択します。
- 必要なカラムを含むカスタム ビューを作成します。カスタム ビューを作成するには、タブ バーの [+] ボタンをクリックするか、[カラムの追加/削除（Add/Remove Columns）] をクリックします。事前設定されているタブは変更できないため、カラムを追加または削除すると新しいビューが作成されます。詳細については、カスタム ビューの設定 （129 ページ）を参照してください。
- カラム幅を変更するには、カラム ヘッダーの境界をクリックして、目的の幅までドラッグします。
- イベントに関する詳細情報を表示するには、イベントの上にカーソルを置き、[詳細の表示（View Details）] をクリックします。イベントの各フィールドの説明については、イベント フィールドの説明 （131 ページ）を参照してください。

ステップ 4 必要な場合は、テーブルにフィルタを適用することで、さまざまなイベント属性に基づいて目的のイベントを見つけることができます。

新規フィルタを作成するには、ドロップダウン リストからアトミック要素を選択してフィルタを手動で入力し、フィルタの値を入力するか、フィルタリングの基準となる値を含むイベント テーブルのセルをクリックしてフィルタを作成します。同じカラムにある複数のセルをクリックして値の間に OR 条件を作成するか、異なるカラムにあるセルをクリックしてカラムの間に AND 条件を作成できます。セルをクリックしてフィルタを作成した場合は、得られたフィル

タを編集して、適切に調整することもできます。フィルタの作成ルールの詳細については、イベントのフィルタリング （130 ページ）を参照してください。

フィルタを作成したら、次の操作を実行します。

- フィルタを適用してテーブルを更新し、フィルタと一致するイベントのみが表示されるようにするには、[フィルタ（Filter）] ボタンをクリックします。
- 適用したフィルタをすべてクリアして、フィルタリングされていない状態のテーブルに戻るには、[フィルタ（Filter）] ボックスの [フィルタのリセット（Reset Filters）] をクリックします。
- フィルタのいずれかのアトミック要素をクリアするには、要素の上にカーソルを置き、要素の [X] をクリックします。[フィルタ（Filter）] ボタンをクリックします。

カスタム ビューの設定

独自のカスタム ビューを作成して、イベントの表示に必要なカラムが簡単に表示されるようにできます。また、事前定義ビューは編集または削除できませんが、カスタム ビューは編集または削除できます。

手順

ステップ 1 **[モニタリング（Monitoring）] > [イベント（Events）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のカスタム（または事前定義された）ビューに基づいて新規ビューを作成するには、そのビューのタブをクリックしてから、ビュー タブの左側にある [+] ボタンをクリックします。
- 既存のカスタム ビューを編集するには、そのビューのタブをクリックします。

（注） カスタム ビューを削除するには、ビューのタブにある [X] ボタンをクリックします。削除すると、元に戻すことはできません。

ステップ 3 右側のイベント テーブルの上にある [追加/削除カラム（Add/Remove Columns）] アイコン ボタンをクリックし、選択したリストに、ビューに含めるカラムのみが含まれるようになるまで、カラムを選択または選択解除します。

使用可能な（ただし使用されていない）リストと選択されているリストの間で、カラムをクリックしてドラッグします。選択されているリスト内でカラムをクリックしてドラッグし、左から右に向かうテーブル内でのカラムの順番を変更することもできます。カラムについては、イベント フィールドの説明 （131 ページ）を参照してください。

完了したら [OK] をクリックして、カラムの変更を保存します。

（注） 事前定義されたビューを表示しながらカラムの選択を変更すると、新規ビューが作成されます。

ステップ 4 必要に応じてカラムのセパレータをクリックしてドラッグし、カラムの幅を変更します。

イベントのフィルタリング

複雑なフィルタを作成してイベントテーブルを制限し、現在関心のあるイベントのみが表示されるようにできます。次の手法を単独または組み合わせて使用して、フィルタを作成できます。

カラムのクリック

フィルタを作成する最も簡単な方法は、フィルタリングの基準となる値を含むイベントテーブルのセルをクリックすることです。セルをクリックすると、その値とフィールドの組み合わせに正しく定式化されているルールを使用して、[フィルタ（Filter）]フィールドが更新されます。ただし、この手法を使用するには、イベントの既存のリストに目的の値が含まれている必要があります。

すべてのカラムをフィルタリングすることはできません。セルのコンテンツをフィルタリングできる場合は、そのセルの上にカーソルを合わせたときに下線が表示されます。

アトミック要素の選択

[フィルタ（Filter）]フィールドをクリックして、ドロップダウンから目的のアトミック要素を選択した後、照合値を入力することでフィルタを作成することもできます。これらの要素には、イベント テーブルのカラムとして表示されないイベント フィールドが含まれます。また、表示するイベントと入力された値との関係を定義するオペレータが含まれます。カラムをクリックすると必ず、「equals (=)」フィルタが表示されますが、要素を選択すると、数値フィールドに「greater than (>)」または「less than (<)」も選択できるようになります。

[フィルタ（Filter）]フィールドに要素を追加する方法に関係なく、フィールドに入力してオペレータまたは値を調整できます。テーブルにフィルタを適用するには、[フィルタ（Filter）]をクリックします。

イベント フィルタの演算子

イベント フィルタには、次の演算子を使用できます。

=	等しい。イベントは指定した値と一致します。ワイルドカードを使用することはできません。
!=	等しくない。イベントは指定した値と一致しません。「等しくない」の式を作成するには、感嘆符（!）を入力する必要があります。
>	次の値より大きい。イベントに、指定した値よりも大きい値が含まれます。この演算子はポートや IP アドレスなど、数値のみに使用できます。

<	次の値より小さい。イベントに、指定した値よりも小さい値が含まれます。この演算子は、数値のみに使用できます。

複雑なイベント フィルタのルール

複数のアトミック要素を含む複雑なフィルタを作成する場合、次のルールに注意してください。

- 同じタイプの要素には、そのタイプのすべての値の間に OR 関係があります。たとえば、Initiator IP=10.100.10.10 と Initiator IP=10.100.10.11 を含めると、送信元としてこれらのいずれかのアドレスを持つイベントが照合されます。
- 異なるタイプの要素には、AND 関係があります。たとえば、Initiator IP=10.100.10.10 と Destination Port/ICMP Type=80 を含めると、この送信元アドレスと宛先ポートのみを持つイベントが照合されます。10.100.10.10 から異なる宛先ポートへのイベントは表示されません。
- IPv4 アドレスや IPv6 アドレスなどの数値要素は範囲を指定できます。たとえば、Destination Port=50-80 を指定して、この範囲内のポートのすべてのトラフィックを取得できます。ハイフンを使用して、開始と終了の数字を区切ります。すべての数値フィールドに対して、範囲を使用できるわけではありません。たとえば、[送信元（Source）] 要素に IP アドレスを範囲で指定することはできません。
- ワイルドカードまたは正規表現は使用できません。

イベント フィールドの説明

イベントには次の情報が含まれます。これらの情報は、イベントの詳細情報を表示すると確認できます。また、イベント ビューア表に列を追加すると、最も関心のある情報を表示できます。

以下に、使用可能なフィールドの完全なリストを示します。すべてのフィールドがどのイベントタイプにも適用されるわけではありません。個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにして接続を記録したかによって異なることに注意してください。

[アクション（Action）]

接続イベントまたはセキュリティ インテリジェンス イベントの場合、接続をロギングしたアクセス制御ルールまたはデフォルト アクションに関連付けられたアクション。

[許可（Allow）]

明示的に許可された接続。

[信頼（Trust）]

信頼できる接続。最初のパケットが信頼ルールによって検出された TCP 接続のみ、接続終了イベントを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。

[ブロック（Block）]

ブロックされている接続。[ブロック（Block）] 動作は、次の条件下で、アクセス許可ルールに関連付けることができます。

- 侵入ポリシーによってエクスプロイトがブロックされた接続。
- ファイルがファイル ポリシーによってブロックされている接続。
- セキュリティ インテリジェンスによってブロックされた接続。
- SSL ポリシーによってブロックされている接続。

[デフォルトアクション（Default Action）]

接続はデフォルト アクションによって処理されました。

ファイルイベントまたはマルウェアイベントの場合は、ファイルが一致したルールのルール アクションに関連付けられたファイル ルール アクションと、すべての関連するファイル ルール アクションのオプション。

[許可された接続（Allowed Connection）]

システムがイベントのトラフィック フローを許可したかどうか。

[アプリケーション(Application）]

接続で検出されたアプリケーション。

[アプリケーションのビジネスとの関連性（Application Business Relevance）]

接続で検出されたアプリケーショントラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

[アプリケーションカテゴリ、アプリケーションタグ（Application Categories, Application Tag）]

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

[ブロックタイプ（Block Type）]

イベントでトラフィック フローが一致したアクセス制御ルールで指定されたブロックのタイプ：block または interactive block。

[クライアントアプリケーション、クライアントバージョン（Client Application, Client Version）]
接続で検出されたクライアントのクライアント アプリケーションとバージョン。

[クライアントのビジネスとの関連性（Client Business Relevance）]

接続で検出されたクライアントトラフィックに関連するビジネスとの関連性：Very High、High、Medium、Low、またはVery Low。接続で検出されたクライアントのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

[クライアントカテゴリ、クライアントタグ（Client Application, Client Version）]

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[クライアントリスク（Client Risk）]

接続で検出されたクライアント トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

[接続（Connection）]

内部的に生成されたトラフィック フローの固有 ID。

[接続ブロックタイプインジケータ（Connection Blocktype Indicator）]

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

[接続バイト（Connection Bytes）]

接続の合計バイト数。

[接続時間（Connection Time）]

接続の開始時刻。

[接続タイムスタンプ（Connection Timestamp）]

接続が検出された時刻。

[拒否された接続（Denied Connection）]

システムがイベントのトラフィック フローを拒否したかどうか。

[宛先の国または大陸（Destination Country and Continent）]

受信ホストの国および大陸。

[宛先 IP アドレス（Destination IP）]

侵入、ファイル、またはマルウェア イベントで受信側ホストによって使用された IP アドレス。

[宛先ポート/ICMPコード、宛先ポート、宛先Icode（Destination Port/ICMP Code; Destination Port; Destination Icode）]

セッション レスポンダが使用するポートまたは ICMP コード。

宛先セキュリティグループタグ、宛先セキュリティグループタグ名

宛先に関連付けられているTrustSecセキュリティグループタグの番号と名前（存在する場合）。

[方向（Direction）]

ファイルの送信方向。

[傾向（Disposition）]

ファイルの性質。

[マルウェア（Malware）]

Secure Malware Analytics Cloudでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイルポリシーで定義されたマルウェアしきい値を超えていることを示します。ローカルマルウェア分析では、ファイルをマルウェアとしてマークすることもできます。

[クリーン（Clean）]

Secure Malware Analytics Cloudでそのファイルがクリーンとして分類されているか、ユーザーがファイルをクリーンリストに追加したことを示します。

不明

システムが Secure Malware Analytics Cloudに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、Secure Malware Analytics Cloudがファイルを正しく分類していませんでした。

Custom Detection

ユーザがカスタム検出リストにファイルを追加したことを示します。

Unavailable

システムが Secure Malware Analytics Cloudに問い合わせることができなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

[該当なし（N/A）]

ファイル検出ルールまたはファイルブロックルールでファイルが処理され、システムが Secure Malware Analytics Cloudに問い合わせなかったことを示します。

[出力インターフェイス、出力セキュリティ ゾーン（gress Interface, Egress Security Zone）]

接続がデバイスを通り抜けたゾーンとインターフェイス。

[出力仮想ルータ（Egress Virtual Router）]

宛先インターフェイスが属する仮想ルータ（存在する場合）の名前。

[イベント、イベントタイプ（Event, Event Type）]

イベントのタイプ。

[イベント秒、イベントマイクロ秒（Event Seconds, Event Microseconds）]

イベントが検出された時刻（秒またはマイクロ秒単位）。

[ファイルカテゴリ（File Category）]

ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

[ファイルイベントタイムスタンプ（File Event Timestamp）]

ファイルまたはマルウェア ファイルが作成された日時。

[ファイル名（File Name）]

ファイルの名前。

[ファイルルールのアクション（File Rule Action）]

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

[ファイルSHA-256（File SHA-256）]

ファイルの SHA-256 ハッシュ値。

[ファイル サイズ（File Size）（KB）]

ファイルのサイズ（KB 単位）。システムがファイルを完全に受信する前にブロックした場合、ファイル サイズが空白になる場合があります。

[ファイルタイプ（File Type）]

ファイルのタイプ（HTML や MSEXE など）。

[ファイル/マルウェアポリシー（File/Malware Policy）]

イベントの生成に関連付けられているファイル ポリシー。

[ファイルログブロックタイプインジケータ（Filelog Blocktype Indicator）]

イベントでトラフィック フローが一致したファイル ルールで指定されたブロックのタイプ：block または interactive block。

[ファイアウォールポリシールール、ファイアウォールルール（Firewall Policy Rule, Firewall Rule）]

接続を処理したアクセス コントロール ルールまたはデフォルト アクション。

[最初のパケット（First Packet）]

セッションの最初のパケットが検出された日時。

[HTTPリファラ（HTTP Referrer）]

接続で検出されたHTTPトラフィックの要求されたURLの参照元を表すHTTP参照元（別のURLへのリンクを提供したWebサイトや別のURLからのリンクをインポートしたWebサイトなど）。

[HTTPレスポンス（HTTP Response）]

クライアントからの接続経由のHTTP要求に応じて送信されるHTTPステータス コード。

[IDSの分類（IDS Classification）]

イベントを生成したルールが属している分類。

[入力インターフェイス、入力セキュリティゾーン（Ingress Interface, Ingress Security Zone）]

接続がデバイスに入ったゾーンとインターフェイス。

[入力仮想ルータ（Ingress Virtual Router）]

送信元インターフェイスが属する仮想ルータ（存在する場合）の名前。

[イニシエータバイト、イニシエータパケット（Initiator Bytes, Initiator Packets）]

セッション イニシエータが送信した合計バイト数またはパケット数。

[イニシエータの国または大陸（Initiator Country and Continent）]

セッションを開始したホストの所在地の国と地域の名前。イニシエータのIPアドレスがルーティング可能であるときにのみ使用できます。

[イニシエータ IP（Initiator IP）]

接続またはセキュリティ インテリジェンス イベントでセッションを開始したホストIPアドレス（およびDNS解決が有効になっている場合のホスト名）。

[インライン結果（Inline Result）]

インライン モードで動作しているときに、侵入イベントをトリガーしたパケットをシステムがドロップした、またはドロップするはずだったか。ブランクは、トリガーとして使用されたルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていないことを示します

[侵入ポリシー（Intrusion Policy）]

イベントを生成したルールが有効にされた侵入ポリシー。

[IPSブロックタイプインジケータ（IPS Blocktype Indicator）]

イベントのトラフィック フローと一致する侵入ルールのアクション。

[最後のパケット（Last Packet）]

セッションの最後のパケットが検出された日時。

[MPLSラベル（MPLS Label）]

この侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

[マルウェアブロックタイプインジケータ（Malware Blocktype Indicator）]

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

[メッセージ（Message）]

侵入イベントの場合、イベントの説明テキスト。マルウェアまたはファイルイベントの場合は、マルウェア イベントに関連付けられている追加情報。

NAT 宛先 IP（NAT Destination IP）

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の宛先 IP アドレス。

NAT 宛先ポート（NAT Destination Port）

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の宛先ポート。

NAT 送信元 IP（NAT Source IP）

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の送信元 IP アドレス。

NAT 送信元ポート（NAT Source Port）

ネットワークアドレス変換（NAT）の対象となるパケットの場合は、変換後の送信元ポート。

[NetBIOSドメイン（NetBIOS Domain）]

セッションで使用された NetBIOS ドメイン。

[元のクライアントの国と大陸（Original Client Country and Continent）]

セッションを開始した元のクライアントホストの所在地の国と地域の名前。元のクライアントの IP アドレスがルーティング可能であるときにのみ使用できます。

[クライアントのオリジナルIP（Original Client IP）]

HTTP 接続を開始したクライアントの元の IP アドレス。このアドレスは、X-Forwarded-For（XFF）または True-Client-IP HTTP のヘッダー フィールド、またはそれらの同等品から取得されます。

[ポリシー、ポリシーの改訂（Policy, Policy Revision）]

アクセス コントロール ポリシーとその改訂版。イベントに関連付けられているアクセス（ファイアウォール）ルールを含みます。

[プライオリティ（Priority）]

Cisco Talos Intelligence Group（Talos）：[高（high）]、[中（medium）]、または [低（low）] によって決まるイベントの優先度。

[プロトコル（Protocol）]

接続に使用されるトランスポート プロトコルです。

[理由（Reason）]

次の表では、接続が記録された理由を説明しています。これ以外の場合、このフィールドは空です。

理由	説明
[DNS ブロック（DNS Block）]	ドメイン名とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[DNS ブロック（DNS Block）] の理由は、DNS ルール アクションに応じて、[ブロック（Block）]、[ドメインが見つかりません（Domain not found）]、[シンクホール（Sinkhole）] のアクションと対として組み合わされます。
DNS モニタ（DNS Monitor）	システムはドメイン名とセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニターするように設定されています。
エレファントフロー	接続は、エレファントフローと見なすのに十分な大きさです。このフローは、システム全体のパフォーマンスに影響を与えるのに十分な大きさです。デフォルトでは、エレファントフローとは 1GB/10 秒を超えるフローです。**system support elephant-flow-detection** コマンドを使用して、デバイス CLI でエレファントフローを識別するためのバイトしきい値と時間しきい値を調整できます。
[ファイルブロック（File Block）]	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] アクションと対として組み合わされます。
ファイル カスタム検出（File Custom Detection）	カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いでいます。
[ファイルモニタ（File Monitor）]	システムが接続において特定のファイルの種類を検出しました。
[ファイル復帰許可（File Resume Allow）]	ファイル送信がはじめに [ファイルブロック（Block Files）] ルールまたは [マルウェアブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。
[ファイル復帰ブロック（File Resume Block）]	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェアクラウドルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。

理由	説明
[侵入ブロック（Intrusion Block）]	接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の理由は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
[侵入モニター（Intrusion Monitor）]	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。
[IPブロック（IP Block）]	IPアドレスとセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[IPブロック（IP Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
[SSL ブロック（SSL Block）]	システムが SSL インスペクション設定に基づいて暗号化接続をブロックしました。[SSL ブロック（SSL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
[URLブロック（URL Block）]	URL とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[URLブロック（URL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。

[受信時間（Receive Times）]

イベントが生成された日時。

[参照ホスト（Referenced Host）]

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

[レスポンダバイト、レスポンダパケット（Responder Bytes, Responder Packets）]

セッション レスポンダが送信した合計バイト数またはパケット数。

[レスポンダの国または大陸（Responder Country and Continent）]

セッションに応答したホストの所在地の国と地域の名前。レスポンダの IP アドレスがルーティング可能であるときにのみ使用できます。

[レスポンダ IP（Responder IP）]

接続またはセキュリティ インテリジェンス イベントのセッションレスポンダのホスト IP アドレス（および DNS 解決が有効になっている場合のホスト名）。

[SIカテゴリID (セキュリティインテリジェンスカテゴリ)（SI Category ID (Security Intelligence Category)）]

ネットワーク名や URL オブジェクト名、フィードカテゴリの名前など、ブロック項目が含まれるオブジェクトの名前。

[シグネチャ（Signature）]

ファイル/マルウェア イベントの署名 ID。

[ソースの国または大陸（Source Country and Continent）]

送信ホストの国と大陸。送信元 IP アドレスがルーティング可能であるときにのみ使用できます。

[ソースIP（Source IP）]

侵入、ファイル、マルウェア イベントで送信側ホストによって使用された IP アドレス。

[送信元ポート/ICMPタイプ、送信元ポート、送信元ポートItype（Source Port/ICMP Type; Source Port; Source Port Itype）]

セッション イニシエータが使用するポートまたは ICMP タイプ。

送信元セキュリティ グループ タグ、送信元セキュリティ グループ タグ名

送信元に関連付けられている TrustSec セキュリティグループタグの番号と名前（存在する場合）。

[実際のSSLアクション（SSL Actual Action）]

システムによって接続に適用される実際のアクション。これは期待される動作とは異なることがあります。たとえば、接続が復号化を適用するルールと一致しても、いくつかの理由で復号化できないことがあります。

アクション	説明
ブロック/リセット付きブロック（Block/Block with reset）	ブロックされた暗号化接続を表します。
[復号（再署名）（Decrypt (Resign)）]	再署名サーバ証明書を使用して復号された発信接続を表します。
[復号（キーの交換）（Decrypt (Replace Key)）]	置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
[復号（既知のキー）（Decrypt (Known Key)）]	既知の秘密キーを使用して復号化された着信接続を表します。

アクション	説明
[デフォルトアクション（Default Action）]	接続がデフォルト アクションによって処理されたことを示します。
[復号しない（Do not Decrypt）]	システムが復号化しなかった接続を表します。

[SSL証明書のフィンガープリント（SSL Certificate Fingerprint）]

証明書の認証に使用する SHA ハッシュ値。

[SSL証明書ステータス（SSL Certificate Status）]

これは、認証ステータスのSSLルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックがSSLルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- [自署（Self Signed）]
- [有効（Valid）]
- [署名が無効（Invalid Signature）]
- [発行元が無効（Invalid issuer）]
- [期限切れ（Expired）]
- [不明（Unknown）]
- [まだ有効ではない（Not Valid Yet）]
- [失効（Revoked）]

復号できないトラフィックが SSL ルールと一致する場合、[チェックしていない（Not Checked）] がこのフィールドに表示されます。

[SSL暗号スイート（SSL Cipher Suite）

接続に使用された暗号スイート。

[予期されたSSLアクション（SSL Expected Action）]

接続が一致した SSL ルールで指定されたアクション。

[SSLフローフラグ（SSL Flow Flags）]

暗号化された接続の最初の 10 デバッグ レベル フラグ。

[SSLフローメッセージ（SSL Flow Messages）]

HELLO_REQUEST や CLIENT_HELLO など、SSL ハンドシェイク中にクライアントとサーバ間で交換された SSL/TLS メッセージ。TLS 接続で交換されたメッセージの詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。

[SSLポリシー（SSL Policy）

接続に適用された SSL 復号ポリシーの名前。

[SSLルール（SSL Rule）]

接続に適用された SSL 復号ルールの名前。

[SSLセッションID（SSL Session ID）]

SSL ハンドシェイク時にクライアントとサーバー間でネゴシエートされた 16 進数のセッション ID。

[SSLチケットID（SSL Ticket ID）]

SSL ハンドシェイク中に送信されたセッション チケット情報の 16 進数のハッシュ値。

[SSLURLカテゴリ（SSL URL Category）]

SSL 復号処理中に決定された宛先 Web サーバの URL カテゴリ。

[SSLバージョン（SSL Version）]

接続に使用された SSL/TLS バージョン。

[TCPフラグ（TCP Flags）]

接続で検出された TCP フラグ。

[合計パケット数（Total Packets）]

接続で送信されたパケットの総数：[イニシエータパケット] + [レスポンダパケット]。

[URL、URLカテゴリ、URLレピュテーション、URLレピュテーションスコア（URL, URL Category, URL Reputation, URL Reputation Score）]

セッション中に監視対象のホストによって要求されたURLと、関連付けられたカテゴリ、レピュテーション、およびレピュテーション スコア（利用できる場合）。

DNS ルックアップ要求フィルタリングの場合、カテゴリとレピュテーションは [DNSクエリ（DNS Query）] フィールドに表示される FQDN 用です。Web 要求ではなく DNS 要求に対してカテゴリ/レピュテーション ルックアップが実行されるため、URL フィールドは空白になります。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL証明書に基づいてトラフィックを識別します。したがって SSL アプリケーションの場合、この URL は証明書に含まれる一般名を表示します。

[ユーザー（User）]

イニシエータの IP アドレスに関連付けられたユーザー。

[VLAN]

イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

[Webアプリケーションのビジネスとの関連性（Web App Business Relevance）]

接続で検出された Web アプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出された Web アプリケーションのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

[Webアプリケーションのカテゴリおよびタグ（Web App Categories、Web App Tag）]

Web アプリケーションの機能を理解するのに役立つ、Web アプリケーションの特性を示す基準。

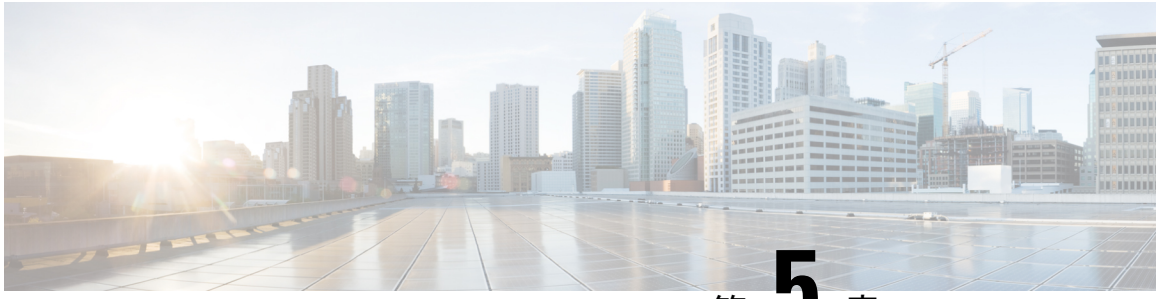
[Webアプリケーションのリスク（Web App Risk）]

接続で検出された Web アプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出された Web アプリケーションのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

[Webアプリケーション（Web Application）]

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。



第 5 章

Cisco ISA 3000 のアラーム

Cisco ISA 3000 デバイスのアラームシステムを設定して、望ましくない状況になったときに警告することができます。

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シビラティ（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。

アラームステータス	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。

アラームステータス	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	—

Syslog アラーム

デフォルトでは、アラームがトリガーされるとシステムは syslog メッセージを送信します。メッセージを送信しない場合は、syslog メッセージングを無効にすることができます。

syslog アラームを機能させるには、**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[ロギング設定（Logging Settings）]** で診断ロギングも有効にする必要があります。syslog サーバー、コンソールロギング、または内部バッファロギングを設定します。

診断ロギングの宛先を有効にしなければ、アラームシステムはどこにも syslog メッセージを送信しません。

SNMP トラップアラーム

必要に応じて、SNMP トラップを SNMP サーバーに送信するようにアラームを設定できます。SNMP トラップアラームが機能するには、SNMP を設定する必要があります。

SNMP を設定するには、Threat Defense API を使用します。[詳細オプション（More options）] ボタン（⋮）をクリックし、[API エクスプローラ（API Explorer）] を選択します。次に、SNMP リソースを探し、そのモデルのマニュアルを調べて、機能の設定方法を確認します。SNMP バージョン 2c または 3 を使用できます。バージョン 1 はサポートされていません。SNMP の設定の詳細については、最新バージョンの ASA ソフトウェア用の『*CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide*』にある SNMP に関する章を参照してください。このガイドは、https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html から入手できます。

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	シビラティ（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

ISA 3000 のアラームの設定

ISA 3000 のアラームを設定するには FlexConfig を使用します。ここでは、さまざまなタイプのアラームの設定方法について説明します。

アラーム入力コンタクトの設定

アラーム入力コンタクト（インターフェイス）を外部センサーに接続する場合、センサーからの入力に基づいてアラームを発行するようコンタクトを設定できます。実際には、デフォルトで、コンタクトはクローズ状態つまりコンタクトを流れる電流が停止すると syslog メッセージを送信するようになっています。デフォルトでは要件が満たされない場合にのみ、コンタクトを設定する必要があります。

アラームコンタクトには 1 および 2 の番号が付いているため、正しく設定するためにどのように物理ピンを接続するのかを理解する必要があります。コンタクトを個別に設定します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

ステップ 4 オブジェクトの名前を入力します。たとえば、**Enable_Alarm_Contact** と入力します。

ステップ 5 [テンプレート（Template）] エディタで、コンタクトの設定に必要なコマンドを入力します。

a) アラームコンタクトの説明を設定します。

alarm contact {**1** | **2**} **description** *string*

たとえば、コンタクト 1 の説明を「Door Open」に設定するには、次のように入力します。

```
alarm contact 1 description Door Open
```

b) アラームコンタクトの重大度を設定します。

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

1 つのコンタクトを設定する代わりに、**any** を指定してすべてのコンタクトの重大度を変更できます。重大度によって、コンタクトに関連付けられている LED の動作が制御されます。

- **major**：LED が赤色で点滅します。
- **minor**：LED が赤色で点灯します。これがデフォルトです。
- **none**：LED が消灯します。

たとえば、コンタクト 1 の重大度を [メジャー（Major）] に設定するには、次のように入力します。

```
alarm contact 1 severity major
```

c) アラームコンタクトのトリガーを設定します。

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

1 つのコンタクトを設定する代わりに、**any** を指定してすべてのコンタクトのトリガーを変更できます。トリガーは、アラート信号を発する電気条件を決定します。

- **open**：コンタクトの通常状態はクローズです。つまり、コンタクトに電流が流れています。コンタクトがオープンになる、つまり電流が停止するとアラートがトリガーされます。
- **closed**：コンタクトの通常状態はオープンです。つまり、コンタクトに電流は流れていません。コンタクトがクローズになる、つまり電流がコンタクトを流れ始めるとアラートがトリガーされます。これはデフォルトです。

たとえば、ドアセンサーをアラーム入力コンタクト 1 に接続して、通常状態ではアラームコンタクトに電流は流れていない（オープン）とします。ドアが開くとコンタクトはクローズになり、アラームコンタクトに電流が流れます。アラームトリガーをクローズに設定しているため、電流が流れ始めるとアラームはオフになります。

```
alarm contact 1 trigger closed
```

d) アラームコンタクトがトリガーされるときに実行するアクションを設定します。

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー（relay）]：アラーム出力リレーに通電します。これにより、ブザーやフラッシュ ライトになどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog]：syslog メッセージを送信します。このオプションは、デフォルトで有効です。
- [通知（notifies）]：SNMP トラップを送信します。

たとえば、アラーム入力コンタクト 1 のすべてのアクションを有効にするには、次のように入力します。

```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

ステップ 6 [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

これらすべてのコマンドでは、**no** 形式を使用して設定を無効化し、デフォルト設定に戻します。たとえば、テンプレートにこの手順で示したすべてのコマンド例が含まれている場合、ネゲートテンプレートは次のようになります。

```
no alarm contact 1 description Door Open
no alarm contact 1 severity major
no alarm contact 1 trigger closed
no alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 syslog
no alarm facility input-alarm 1 notifies
```

ステップ 7 [OK] をクリックしてオブジェクトを保存します。

ステップ 8 オブジェクトを FlexConfig ポリシーに追加します。

a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。
b) [グループリスト（Group List）] で [+] をクリックします。
c) Enable_Alarm_Contact オブジェクトを選択して、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 9 展開が完了したら、CLI コンソールまたは SSH セッションで、**show running-config** コマンドを使用し、実行中の設定が正しく変更されていることを確認します。外部センサーをテストして、アラームがトリガーされていることを確認します。

電源アラームの設定

ISA 3000 には、電源装置が 2 台搭載されています。デフォルトでは、システムはシングル電源モードで稼働しています。ただし、デュアルモードでシステムを稼働するよう設定できます。その場合、プライマリ電源が故障すると 2 つ目の電源が自動的に電力を供給します。デュアルモードを有効にすると、電源アラームが自動的に有効になって syslog アラートが送信されますが、アラートを無効にしたり、SNMP トラップまたはアラーム ハードウェア リレーを有効にすることもできます。

次の手順では、デュアルモードを有効にする方法と電源アラームを設定する方法について説明します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

ステップ 4 オブジェクトの名前を入力します。たとえば、**Enable_Power_Supply_Alarm** と入力します。

ステップ 5 [テンプレート（Template）]エディタで、電源アラームの設定に必要なコマンドを入力します。

a) デュアル電源モードを有効にします。

power-supply dual

次に例を示します。

```
power-supply dual
```

b) 電源アラームがトリガーされたときに実行するアクションを設定します。

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー（relay）]：アラーム出力リレーに通電します。これにより、ブザーやフラッシュ ライトになどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog]：syslog メッセージを送信します。このオプションは、デフォルトで有効です。
- [通知（notifies）]：SNMP トラップを送信します。
- [無効化（disable）]：電源アラームを無効にします。電源アラームに設定されたその他のアクションは動作しなくなります。

たとえば、電源アラームのすべてのアクションを有効にするには、次のように入力します。

```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

ステップ 6 [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

これらすべてのコマンドでは、**no** 形式を使用して設定を無効化し、デフォルト設定に戻します。たとえば、テンプレートにこの手順で示したすべてのコマンド例が含まれている場合、ネゲートテンプレートは次のようになります。

```
no power-supply dual
no alarm facility power-supply rps relay
no alarm facility power-supply rps syslog
no alarm facility power-supply rps notifies
```

ステップ 7 [OK] をクリックしてオブジェクトを保存します。

ステップ 8 オブジェクトを FlexConfig ポリシーに追加します。

a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。

b) [グループリスト（Group List）] で [+] をクリックします。

c) Enable_Power_Supply_Alarm オブジェクトを選択して、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 9 展開が完了したら、CLI コンソールまたは SSH セッションで、**show running-config** コマンドを使用し、実行中の設定が正しく変更されていることを確認します。

温度アラームの設定

デバイスの CPU カードの温度に基づいてアラームを設定できます。

プライマリ温度範囲とセカンダリ温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、およびSNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温を設定すると、プライマリ設定にデフォルト以外の値を設定している場合でも、対応するプライマリ設定はセカンダリの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

ステップ 4 オブジェクトの名前を入力します。たとえば、**Enable_Temperature_Alarm** と入力します。

ステップ 5 [テンプレート（Template）]エディタで、温度アラームの設定に必要なコマンドを入力します。

a) 許容温度範囲を設定します。

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

温度は摂氏で示されます。プライマリアラームの許容範囲は -40 ～ 92 で、これがデフォルト範囲でもあります。セカンダリアラームの許容範囲は、-35 ～ 85 です。低い値は、高い値より小さくする必要があります。

たとえば、セカンダリアラームの許容範囲内で、より制限された温度範囲の -20 ～ 80 を設定するには、次のようにセカンダリアラームを設定します。

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

b) 温度アラームがトリガーされたときに実行するアクションを設定します。

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

複数のアクションを設定できます。たとえば、デバイスを設定して、外部アラームをアクティブ化したり、syslog メッセージを送信したり、SNMP トラップを送信することもできます。

- [リレー（relay）]：アラーム出力リレーに通電します。これにより、ブザーやフラッシュ ライトになどに接続した外部アラームがアクティブ化されます。出力 LED も赤色になります。
- [syslog]：syslog メッセージを送信します。
- [通知（notifies）]：SNMP トラップを送信します。

たとえば、セカンダリ温度アラームのすべてのアクションを有効にするには、次のように入力します。

```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

ステップ 6 [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

次のすべてのコマンドでは、**no** 形式を使用してデフォルト設定に戻したり（プライマリアラームの場合）、設定を無効にします（セカンダリアラームの場合）。たとえば、テンプレートにこの手順で示したすべてのコマンド例が含まれている場合、ネゲートテンプレートは次のようになります。

```
no alarm facility temperature secondary low -20
no alarm facility temperature secondary high 80
no alarm facility temperature secondary relay
no alarm facility temperature secondary syslog
no alarm facility temperature secondary notifies
```

ステップ 7 [OK] をクリックしてオブジェクトを保存します。

ステップ 8 オブジェクトを FlexConfig ポリシーに追加します。

a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。
b) [グループリスト（Group List）] で [+] をクリックします。
c) Enable_Temperature_Alarm オブジェクトを選択して、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 9 展開が完了したら、CLI コンソールまたは SSH セッションで、**show running-config** コマンドを使用し、実行中の設定が正しく変更されていることを確認します。

アラームのモニタリング

ここでは、アラームのモニターおよび管理方法について説明します。

アラーム ステータスのモニタリング

CLI で次のコマンドを使用してアラームをモニターすることができます。

- **show alarm settings**

  使用可能な各アラームの現在の設定が表示されます。

- **show environment alarm-contact**

  入力アラームコンタクトの物理ステータスに関する情報が表示されます。

- **show facility-alarm relay**

  出力リレーをトリガーしたアラームに関する情報が表示されます。

- **show facility-alarm status[info |major |minor]**

  トリガーされたすべてのアラームに関する情報が表示されます。**major** ステータスまたは **minor** ステータスでフィルタリングすることで表示の絞り込みができます。**info** キーワードを使用すると、キーワードを使用しない場合と同じ出力になります。

アラームに関する Syslog メッセージのモニタリング

設定するアラームのタイプに応じて、次の Syslog メッセージが表示される場合があります。

デュアル電源アラーム

- %FTD-1-735005：Power Supply Unit Redundancy OK
- %FTD-1-735006：Power Supply Unit Redundancy Lost

温度アラーム

これらのアラームでは、*Celsius* は、デバイス上で検出された温度（摂氏単位）に置き換えられます。

- %FTD-6-806001：Primary alarm CPU temperature is High *Celsius*
- %FTD-6-806002：Primary alarm for CPU high temperature is cleared
- %FTD-6-806003：Primary alarm CPU temperature is Low *Celsius*
- %FTD-6-806004：Primary alarm for CPU Low temperature is cleared
- %FTD-6-806005：Secondary alarm CPU temperature is High *Celsius*
- %FTD-6-806006：Secondary alarm for CPU high temperature is cleared

- %FTD-6-806007：Secondary alarm CPU temperature is Low *Celsius*
- %FTD-6-806008：Secondary alarm for CPU Low temperature is cleared

アラーム入力コンタクトアラーム

これらのアラームでは、「*description*」は、設定したコンタクトの説明です。

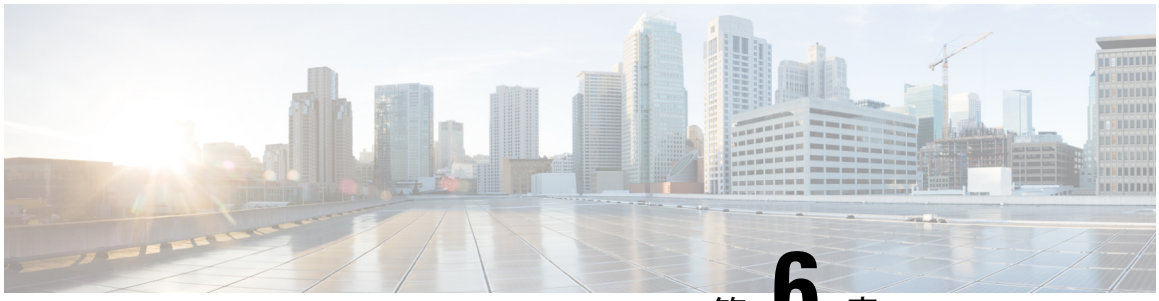
- %FTD-6-806009：Alarm asserted for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806010：Alarm cleared for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806011：Alarm asserted for ALARM_IN_2 *alarm_2_description*
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*

外部アラームをオフにする

アラーム出力にアタッチされる外部アラームを使用していて、アラームがトリガーされる場合、**clear facility-alarm output** コマンドを使用してデバイス CLI から外部アラームをオフにできます。このコマンドは、出力ピンの電源を切り、出力 LED もオフにします。

第 II 部

再利用可能なオブジェクト



第 6 章

オブジェクト

オブジェクトは、ポリシーまたはその他の設定内で使用する基準を定義した再利用可能なコンテナです。たとえば、ネットワーク オブジェクトは、ホスト アドレスとサブネット アドレスを定義します。

オブジェクトでは基準を定義することができ、同じ基準を異なるポリシーで簡単に再利用できるようになります。オブジェクトを更新すると、そのオブジェクトを使用するすべてのポリシーが自動的に更新されます。

オブジェクト タイプ

次のタイプのオブジェクトを作成できます。ほとんどの場合、ポリシーまたは設定によってオブジェクトを許可する場合、オブジェクトを使用する必要があります。

オブジェクト タイプ	主な用途	説明
セキュアクライアント プロファイル	リモート アクセス VPN	セキュアクライアントプロファイルは、セキュアクライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーがセキュアクライアントの設定および詳細設定からオプションを変更することを許可するかどうかを定義します。 クライアント プロファイルの設定およびアップロード（840 ページ）を参照してください。

オブジェクト タイプ	主な用途	説明
アプリケーション フィルタ	アクセス コントロール ルール	アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。 アプリケーション フィルタ オブジェクトの設定 （169 ページ）を参照してください。
証明書	アイデンティティ ポリシー リモート アクセス VPN SSL 復号ルール 管理 Web サーバ。	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。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。 証明書の設定 （183 ページ） を参照してください。
DNS グループ	管理インターフェイスとデータ インターフェイスの DNS 設定	DNS グループは、DNS サーバーおよび関連付けられているいくつかの属性のリストを定義します。www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバーが必要です。 「DNS グループの設定 （942 ページ）」を参照してください。
イベントリスト フィルタ	選択したログの宛先のシステムログ設定。	イベントリストフィルタは、syslog メッセージ用のカスタムフィルタリストを作成します。syslog サーバーまたは内部ログ バッファなど、特定のログの場所に送信されるメッセージを制限するには、これらを使用できます。 イベント リスト フィルタの設定 （932 ページ）を参照してください。

オブジェクト タイプ	主な用途	説明
位置情報（GeoLocation）	セキュリティ ポリシー	地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。 地理位置情報オブジェクトの設定（174ページ）を参照してください。
アイデンティティ ソース	アイデンティティ ポリシー リモート アクセス VPN Device Manager アクセス	アイデンティティ ソースは、ユーザー アカウントを定義するサーバーとデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。 アイデンティティ ソース（191ページ）を参照してください。
IKE ポリシー	VPN	インターネット キー エクスチェンジ（IKE）ポリシー オブジェクトは、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SAS）の自動的な確立に使用される IKE プロポーザルを定義します。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。 グローバル IKE ポリシーの設定（797ページ）を参照してください。
IPsec プロポーザル	VPN	IPsec プロポーザル オブジェクトは、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。IKEv1 と IKEv2 に対して、異なるオブジェクトがあります。 IPsec プロポーザルの設定（802 ページ）を参照してください。
ネットワーク	セキュリティ ポリシーおよびさまざまなデバイス設定	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。 ネットワーク オブジェクトとグループの設定（164ページ）を参照してください。

オブジェクト タイプ	主な用途	説明
ポート	セキュリティ ポリシー	トラフィックのプロトコル、ポート、またはICMPサービスを定義するポート グループおよびポート オブジェクト（総称してポート オブジェクトと呼ばれます）。 ポート オブジェクトとグループの設定（166ページ）を参照してください。
秘密キー	Smart CLI および FlexConfig ポリシー	秘密キー オブジェクトは、パスワードや、暗号化および非表示にするその他の認証文字列を定義します。 秘密キー オブジェクトの設定（1056ページ）を参照してください。
セキュリティ ゾーン	セキュリティ ポリシー	セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。 「セキュリティ ゾーンの設定（167ページ）」を参照してください。
SGT グループ	アクセス コントロール ポリシー	TrustSec セキュリティグループタグ（SGT）は、Cisco Identity Services Engine（ISE）で定義されたトラフィックのタグを定義します。これらのオブジェクトを作成するには ISE を設定する必要があります。その後、そのオブジェクトを、アクセス制御ルール内の送信元/宛先一致基準として使用できます。 「セキュリティグループタグ（SGT）グループの設定（176 ページ）」を参照してください。
SLA モニター	スタティック ルート	SLA モニターは、スタティックルートのモニタリングに使用するターゲット IP アドレスを定義します。ターゲット IP アドレスに到達できなくなったことをモニタが判断した場合、システムはバックアップ スタティック ルートをインストールできます。 「SLA モニター オブジェクトの設定（399 ページ）」を参照してください。

オブジェクト タイプ	主な用途	説明
SSL 暗号化	SSL 設定	SSL 暗号オブジェクトでは、Threat Defense への SSL 接続を確立するときに使用できるセキュリティレベル、TLS/DTLS プロトコルバージョン、および暗号化アルゴリズムの組み合わせを定義します。システム設定でこれらのオブジェクトを使用して、ボックスへの TLS/SSL 接続を行うユーザーのセキュリティ要件を定義します。 「TLS/SSL 暗号設定の設定 （967 ページ）」を参照してください。
Syslogサーバ	アクセス コントロール ルール 診断ロギング セキュリティ インテリジェンス ポリシー SSL 復号ルール 侵入ポリシー ファイル/マルウェアポリシー	syslog サーバーのオブジェクトはコネクション型メッセージまたは診断システム ログ（syslog）メッセージを受信できるサーバーを指定します。 Syslog サーバーの設定 （175 ページ）を参照してください。
URL	アクセス コントロール ルール セキュリティ インテリジェンス ポリシー	Web リクエストの URL または IP アドレスを定義する URL オブジェクトおよびグループ（総称して URLオブジェクトと呼ばれます）。 URL オブジェクトとグループの設定 （172 ページ）を参照してください。
Users	リモート アクセス VPN	リモート アクセス VPN で使用するユーザー アカウントをデバイスで直接作成できます。外部認証ソースの代わりに、またはそれに加えて、ローカル ユーザー アカウントを使用できます。 ローカル ユーザーの設定 （214 ページ） を参照してください。

オブジェクトの管理

オブジェクトは、[オブジェクト（Objects）]ページから直接設定することも、ポリシーの編集時に設定することもできます。いずれの方法でも同じく新規または更新されたオブジェクトが作成されるため、その時点で適した方法を使用します。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および管理する方法について説明します。

（注） ポリシーまたは設定を編集すると、プロパティにオブジェクトが必要な場合、すでに定義されているオブジェクトのリストが表示されるため、適切なオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合は、リストに表示される [新規オブジェクトの作成（Create New Object）] リンクをクリックします。

手順

ステップ 1 [オブジェクト（Objects）] を選択します。

[オブジェクト（Objects）]ページには、使用可能なオブジェクト タイプが一覧表示される目次があります。オブジェクト タイプを選択すると、既存オブジェクトのリストが表示され、新しいオブジェクトを作成できます。オブジェクトの内容とタイプも確認できます。

ステップ 2 目次からオブジェクト タイプを選択し、次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。オブジェクトの内容はタイプによって異なります。具体的な情報については、各オブジェクト タイプの設定トピックを参照してください。
- グループ オブジェクトを作成するには、[グループの追加（Add Group）]（）ボタンをクリックします。グループ オブジェクトには複数の項目が含まれます。
- オブジェクトを編集するには、そのオブジェクトの[編集（edit）]（）アイコンをクリックします。定義済みオブジェクトの内容は編集できません。
- オブジェクトを削除するには、そのオブジェクトの [削除（delete）]（）アイコンをクリックします。ポリシーや別のオブジェクトで現在使用されているオブジェクト、または定義済みのオブジェクトは削除できません。

ネットワーク オブジェクトとグループの設定

ホストまたはネットワークのアドレスを定義するには、ネットワーク グループとネットワーク オブジェクト（ネットワーク オブジェクトと総称される）を使用します。これらのオブジェクトは、トラフィックの一致条件を定義するためにセキュリティ ポリシーで使用するか、サーバーその他のリソースのアドレスを定義するために設定で使用できます。

ネットワーク オブジェクトは単一のホストまたはネットワーク アドレスを定義しますが、ネットワーク グループ オブジェクトは複数のアドレスを定義できます。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。アドレス プロパティの編集時に、オブジェクト リストに表示される [新しい

ネットワークの作成（Create New Network）] リンクをクリックして、ネットワーク オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [ネットワーク（Network）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）] ボタン（）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前を入力し、オプションでオブジェクトの説明を入力してオブジェクトの内容を定義します。

オブジェクトの内容またはスタンドアロン IP アドレスからオブジェクト名を簡単に識別できるように、名前に IP アドレスだけを使用しないことを推奨します。名前に IP アドレスを使用する場合は、host-192.168.1.2 や network-192.168.1.0 など、わかりやすいプレフィックスを付けてください。IP アドレスを名前として使用する場合は、縦線がプレフィックスとして追加されます（例：|192.168.1.2）。Device Manager ではオブジェクトセレクタに縦棒が表示されませんが、CLI で **show running-config** コマンドを使用して実行中の設定を調べると、この命名規則を確認できます。

ステップ 4 オブジェクトの内容を設定します。

ネットワーク オブジェクト

オブジェクトの [タイプ（Type）] を選択して、コンテンツを設定します。

- [ネットワーク（Network）]：次のいずれかの形式を使用してネットワーク アドレスを入力します。
  - サブネット マスクを含む IPv4 ネットワーク（10.100.10.0/24、10.100.10.0/255.255.255.0 など）。
  - プレフィックスを含む IPv6 ネットワーク（2001:DB8:0:CD30::/60 など）。
- [ホスト（Host）]：次のいずれかの形式を使用してホスト IP アドレスを入力します。
  - IPv4 ホスト アドレス（10.100.10.10 など）。
  - IPv6 ホスト アドレス（2001:DB8::0DB8:800:200C:417A または 2001:DB8:0:0:0DB8:800:200C:417A など）。

- [範囲（Range）]：ハイフンで区切られた開始アドレスと終了アドレスを備えたアドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。たとえば、192.168.1.10-192.168.1.250 または 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100 とします。
- [FQDN]：www.example.com などの単一の完全修飾ドメイン名を入力します。ワイルドカードを使用することはできません。また、[DNS解決（DNS Resolution）] を選択して、IPv4 アドレス、IPv6 アドレス、または Ipv4 アドレスと IPv6 アドレスの両方を FQDN と関連付けるかどうかも決定します。デフォルトは、IPv4 と IPv6 の両方です。これらのオブジェクトはアクセス制御ルールのみで使用できます。ルールでは、DNS ルックアップによって FQDN 用に取得された IP アドレスを照合します。

ネットワーク グループ

グループに追加するネットワークオブジェクトまたはグループを選択するには、[+] ボタンをクリックします。新しいオブジェクトを作成することもできます。

ステップ 5 [OK] をクリックして変更を保存します。

ポート オブジェクトとグループの設定

トラフィックのプロトコル、ポート、またはICMPサービスを定義するには、ポート グループとポート オブジェクト（まとめてポート オブジェクトと呼ぶ）を使用します。その後、トラフィックの一致基準を定義するためのセキュリティ ポリシーのオブジェクトを使用して、たとえばアクセス ルールを使用して特定の TCP ポートへのトラフィックを許可できます。

ポート オブジェクトは単一のプロトコル、TCP/UDP ポートまたはポート範囲、または ICMP サービスを定義しますが、ポート グループ オブジェクトは、複数のサービスを定義できます。

システムには、一般的なサービス向けの複数の事前定義されたオブジェクトが含まれています。これらのオブジェクトはポリシーで使用できます。ただし、システムで定義されたオブジェクトは、編集または削除ができません。

（注） ポート グループ オブジェクトを作成する場合、オブジェクトの組み合わせが有効であることを確認してください。たとえば、あるオブジェクトをアクセス ルールで送信元と宛先ポートの両方を指定するために使用する場合、そのオブジェクトに複数のプロトコルを組み合わせることはできません。すでに使用されているオブジェクトを編集する場合は注意してください。オブジェクトを使用するポリシーが無効（かつディセーブル）になる場合があります。

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [新規ポートの作成（Create New Port）] リンクをクリックすることで、サービスのプロパティを編集しながらポート オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [ポート（Ports）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）] ボタン（  ）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力し、オブジェクトの内容を定義します。

ポート オブジェクト

[プロトコル（Protocol）] を選択し、次のようにプロトコルを設定します。

- **TCP**、**UDP**：単一のポートまたはポート範囲の番号を入力します（たとえば80（HTTPの場合）または 1-65535（すべてのポートをカバー））。
- **ICMP**、**IPv6 ICMP**：ICMP の [タイプ（Type）] を選択し、オプションで [コード（Code）] を選択します。タイプをすべての ICMP メッセージに適用するには、[任意（Any）] を選択します。タイプとコードについての詳細は、次のページを参照してください。
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- [その他（Other）]：目的のプロトコルを選択します。

ポート グループ

[+] ボタンは、グループに追加するポート オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 4 [OK] をクリックして変更を保存します。

セキュリティ ゾーンの設定

セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

システムは初期設定時に次のゾーンを作成します。これらのゾーンを編集してインターフェイスを追加または削除したり、使用しなくなったゾーンを削除したりできます。

- **inside_zone**：内部インターフェイスが含まれます。内部インターフェイスがブリッジグループである場合、このゾーンには内部ブリッジ仮想インターフェイス（BVI）ではなく、すべてのブリッジ グループ メンバー インターフェイスが含まれます。このゾーンは、内部ネットワークを表します。
- **outside_zone**：外部インターフェイスが含まれます。このゾーンは、インターネットなどの制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターフェイスに接続するインターフェイスを**outside_zone**セキュリティ ゾーンに配置し、内部ネットワークに接続するすべてのインターフェイスを **inside_zone** セキュリティ ゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセス コントロール ルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセス ルールや他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。4 つの内部ネットワークがあり、1 つだけ他の 3 つとは異なる処理をしたい場合、1 つではなく 2 つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用できます。

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [新規セキュリティ ゾーンの作成（Create New Security Zone）] リンクをクリックすることで、セキュリティ ゾーンのプロパティを編集しながらセキュリティ ゾーンを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [セキュリティゾーン（Security Zones）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 ゾーンの [モード（Mode）] を選択します。

このモードはインターフェイスのモードに直接関係します。ゾーンには、1 つのタイプのインターフェイスを含めることができます。

- [ルーテッド（Routed）]：ルーテッドインターフェイスは、セキュリティポリシーを適用できる通過トラフィック用の通常のインターフェイスです。

- [パッシブ（Passive）]：パッシブインターフェイスは、デバイスを通過するトラフィックに影響を与えません。
- [インライン（Inline）]：インラインインターフェイスは、IPS 処理に使用されるインラインセットのメンバーです。

ステップ 5 [インターフェイス（Interfaces）]リストで、[+]をクリックし、ゾーンに追加するインターフェイスを選択します。

このリストは、現在ゾーンに含まれていないすべての名前付きインターフェイスを表示します。インターフェイスをゾーンに追加するには、インターフェイスを設定して名前を付ける必要があります。

すべての名前付きインターフェイスがすでにゾーンにある場合、リストは空になります。別のゾーンにインターフェイスを移動しようとする場合、最初に現在のゾーンから削除する必要があります。

（注） ゾーンにブリッジ グループ インターフェイス（BVI）を追加することはできません。代わりに、メンバーインターフェイスを追加します。メンバーを異なるゾーンに配置できます。

ステップ 6 [OK] をクリックして変更を保存します。

アプリケーション フィルタ オブジェクトの設定

アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーションフィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

アプリケーション フィルタ オブジェクトを使用せず、ポリシーのアプリケーションとアプリケーション フィルタを直接選択できます。ただし、同じアプリケーションまたはフィルタ グループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーションフィルタが含まれていて、これらは編集または削除できません。

（注） シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。[アプリケーション（Applications）]タブにアプリケーション基準を追加した後、[フィルタとして保存（Save As Filter）]リンクをクリックして、アクセス コントロール ルールを編集しながら、アプリケーション フィルタ オブジェクトも作成できます。

始める前に

フィルタを編集するときに、選択したアプリケーションが VDB の更新によって削除された場合は、アプリケーション名の後に「Deprecated（廃止）」が表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システム ソフトウェアのアップグレードがブロックされます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、目次から[アプリケーションフィルタ（Application Filters）]を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの[ごみ箱（trash can）]アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [アプリケーション（Applications）]リストで[追加＋（Add＋）]をクリックし、オブジェクトに追加するアプリケーションとフィルタを選択します。

最初のリストには、継続的にスクロールするリストでアプリケーションが表示されます。[フィルタの詳細設定（Advanced Filter）]をクリックすると、フィルタ オプションが表示され、アプリケーションを容易に選択できます。選択したら、[追加（Add）]をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

（注） 1 つのフィルタ条件内での複数の選択は OR 関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。

リスク

アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーションプロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル。
- [クライアントプロトコル（Client Protocol）]：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Webアプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も重要な機能を説明する一般分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは[SSLプロトコル（SSL Protocol）]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）] タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを

使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

ステップ 5 [OK] をクリックして変更を保存します。

URL オブジェクトとグループの設定

URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループ オブジェクトは複数の URL またはアドレスを定義できます。

URL オブジェクトを作成する場合は、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。
  - 文字列が URL の先頭にある。
  - 文字列がドットの後に続く。
  - 文字列の先頭にドットが含まれている。
  - 文字列が :// 文字の後に続く。

  たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。

（注） サーバーは再構成でき、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。

- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、http://example.com ではなく example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内

でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

次に、[オブジェクト（Objects）] ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクト リストに表示される [新規 URL の作成（Create New URL）] リンクをクリックすることで、URL のプロパティを編集しながら URL オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [URL] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）] ボタン（）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 オブジェクトの内容を定義します。

URL オブジェクト

URL または IP アドレスを [URL] ボックスに入力します。URL にはワイルドカードを使用できません。

URL グループ

[+] ボタンは、グループに追加する URL オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 5 [OK] をクリックして変更を保存します。

地理位置情報オブジェクトの設定

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。たとえば、地理的な場所を使用して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。

（注） 常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

次に、[オブジェクト（Objects）] ページで直接オブジェクトを作成および編集する方法について説明します。ネットワーク プロパティの編集時に、オブジェクト リストに表示される [新しい地理位置情報の作成（Create New Geolocation）] リンクをクリックして、地理位置情報オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [地理位置情報（Geolocation）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [大陸または国（Continents/Countries）] リストで [追加＋（Add＋）] をクリックして、オブジェクトに追加する大陸や国を選択します。

大陸を選択すると、大陸内のすべての国が選択されます。

ステップ 5 [OK] をクリックして変更を保存します。

Syslog サーバーの設定

syslog サーバーのオブジェクトはコネクション型メッセージまたは診断システム ログ（syslog）メッセージを受信できるサーバーを指定します。syslog サーバーにログ収集と分析のための設定がある場合は、オブジェクトを作成してそれらを定義し、関連ポリシーでこのオブジェクトを使用します。

以下のイベント タイプを syslog サーバに送信できます。

- 接続イベント。次のポリシーのタイプで syslog サーバ オブジェクトを構成します：アクセス制御ルールとデフォルト アクション、SSL 復号ルールとデフォルト アクション、セキュリティ インテリジェンス ポリシー。
- 侵入イベント。侵入ポリシーで syslog サーバ オブジェクトを構成します。
- 診断イベント。リモート syslog サーバーのロギングの設定（929 ページ）を参照してください。
- ファイル/マルウェアイベント。**[デバイス（Device）]**>**[システム設定（System Settings）]**>**[ロギング設定（Logging Settings）]** で syslog サーバーを設定します。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクト リストに表示される [Syslogサーバーの追加（Add Syslog Server）] リンクをクリックすることで、syslog サーバーのプロパティを編集しながら syslog サーバーを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [Syslogサーバー（Syslog Server）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 syslog サーバーのプロパティを設定します。

- [IPアドレス（IP Address）]：syslog サーバーの IP アドレスを入力します。
- [プロトコルタイプ（Protocol Type）]、[ポート番号（Port Number）]：プロトコルを選択して、syslog に使用するポート番号を入力します。デフォルトは UDP/514 です。[TCP] を選

択すると、システムはsyslogサーバーが利用できない場合を認識して、サーバーが再度利用可能になるまでイベントの送信を停止できます。デフォルトUDPポートは514、デフォルトTCPポートは1470です。デフォルトを変更する場合は、1025 ～ 65535の範囲のポートを使用してください。

（注） 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。

- [デバイスログのインターフェイス（Interface for Device Logs）]：診断syslogメッセージの送信に使用するインターフェイスを選択します。接続、侵入、ファイル、マルウェアの各イベントタイプでは、常に管理インターフェイスが使用されます。インターフェイスの選択によって、syslogメッセージに関連付けられるIPアドレスが決まります。次のオプションのいずれかを選択します。
  - [データインターフェイス（Data Interface）]：選択したデータ インターフェイスを診断syslogメッセージに使用します。サーバーがブリッジグループのメンバーインターフェイスを介してアクセスできる場合、代わりにブリッジ グループ インターフェイス（BVI）を選択します。パッシブ インターフェイスを選択することはできません。

    データインターフェイスで通信する場合、接続、侵入、ファイル、およびマルウェアの Syslog メッセージでは、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。前述のイベントタイプ用に選択したインターフェイスからsyslogサーバーにトラフィックを転送するための適切なルートが、ルーティングテーブルに存在する必要があることに注意してください。
  - [管理インターフェイス（Management Interface）]：すべてのタイプの syslog メッセージに管理インターフェイスを使用します。データインターフェイス経由でルーティングする場合、送信元IPアドレスが管理インターフェイスまたはゲートウェイインターフェイスで使用されます。

ステップ 4 [OK] をクリックして変更を保存します。

セキュリティグループタグ（SGT）グループの設定

セキュリティグループタグ（SGT）グループオブジェクトを使用して、Identity Services Engine（ISE）によって割り当てられたSGTに基づいて送信元アドレスまたは宛先アドレスを識別します。その後、トラフィックの一致基準を定義するためにアクセス制御ルールでオブジェクトを使用できます。

ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

アクセス制御のために SGT を使用する方法の詳細については、Trustsec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法 （631 ページ） を参照してください。

始める前に

SGT グループを作成する前に、SXP マッピングをサブスクライブして変更を展開するように ISE アイデンティティ ソースを設定する必要があります。その後、システムは ISE サーバーから SGT 情報を取得します。SGT をダウンロードした後にのみ、SGT グループを作成できます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [SGT グループ（SGT Groups）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

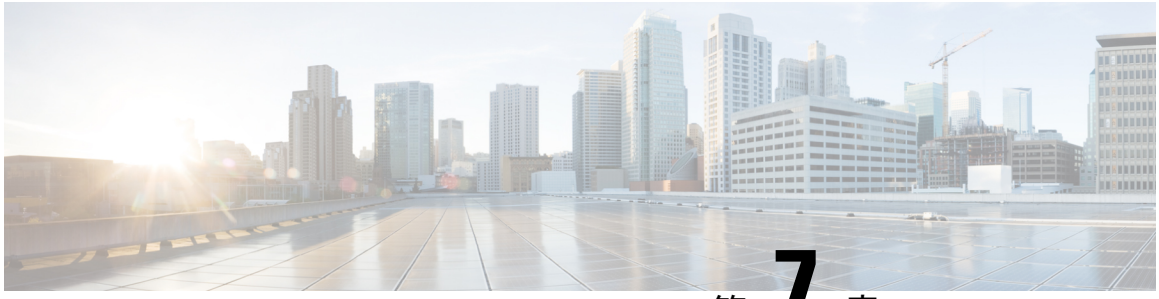
ステップ 4 [タグ（Tags）] で、[+] をクリックし、ダウンロードした SGT を選択してオブジェクトに含めます。

SGT を削除するには、タグ名の右横にある [x] をクリックします。

リストが空の場合、システムはSGTマッピングをダウンロードできませんでした。この場合、次のようになります。

- ISE アイデンティティ オブジェクトが SXP トピックをサブスクライブしていることを確認します。マッピングを取得するには、SXP をサブスクライブする必要があります。
- ISE で静的マッピングが定義されていることと、これらのマッピングをパブリッシュするように ISE が設定されていることを確認します。マッピングが存在しない場合は、単にダウンロードされるものはありません。ISE でのセキュリティ グループと SXP パブリッシングの設定 （634 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。



第 7 章

証明書

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。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。次のトピックでは、証明書の作成と管理の方法について説明します。

証明書について

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。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）に使用されます。

次のタイプの証明書を作成できます。

- 内部証明書：内部アイデンティティ証明書は、特定のシステムまたはホストの証明書です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名証明書を生成することもできます。何らかの理由で内部証明書が期限切れになるか無効になった場合は、次の CLISH CLI コマンドを使用して再生成できます。

```
> system support regenerate-security-keyring
  String  Certificate to be regenerated, default or fdm
```

- 内部証明書認証局（CA）証明書：内部 CA 証明書は、他の証明書の署名にシステムが使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。これらは OpenSSL ツールキットを使用して自分で生成することも、認証局から取得することもできます。自己署名内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。

- 信頼できる認証局（CA）証明書：信頼できる 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。

認証局（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。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。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、証明書要求の管理とデジタル証明書の発行を行います。詳細については、公開キー暗号化（180 ページ）を参照してください。

公開キー暗号化

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。

デジタル証明書および公開キー暗号化の詳細については、openssl.org、Wikipedia、またはその他のソースを参照してください。SSL/TLS 暗号化をしっかりと理解することで、デバイスへのセキュアな接続を確立できます。

各機能で使用される証明書タイプ

各機能に適したタイプの証明書を作成する必要があります。次の機能は、証明書が必要です。

アイデンティティ ポリシー（キャプティブ ポータル）：内部証明書

（オプション）キャプティブ ポータルはアイデンティティ ポリシーで使用されます。この証明書は、ユーザが自身を特定し、自分のユーザ名にデバイスの IP アドレスを関連付けることを目的としてデバイスを認証するときに承認する必要があります。証明書を提示しないと、デバイスは自動生成された証明書を使用します。

アイデンティティ レルム（アイデンティティ ポリシーおよびリモート アクセス VPN）：信頼できる CA 証明書

（オプション）ディレクトリ サーバに暗号化接続を使用する場合、ディレクトリ サーバの認証を行うためにこの証明書を承認する必要があります。ユーザは、アイデンティティ ポリシーおよびリモート アクセス VPN ポリシーから求められたときに認証する必要があります。ディレクトリ サーバに暗号化を使用しない場合、証明書は必要ありません。

管理 Web サーバ（管理アクセス システム設定）：内部証明書

（オプション）Device Manager は Web ベースのアプリケーションであり、Web サーバーで動作します。お使いのブラウザで有効として受け入れられる証明書をアップロードすると、Untrusted Authority の警告を受けるのを回避できます。

リモート アクセス VPN：内部証明書

（必須）内部証明書は、セキュアクライアントがデバイスへの接続を行うときにデバイス ID を確立する外部インターフェイスに使用します。クライアントはこの証明書を承認する必要があります。

サイト間 VPN：内部および信頼できる CA 証明書

サイト間 VPN 接続に証明書認証を使用する場合は、接続内のローカルピアの認証に使用される内部アイデンティティ証明書を選択する必要があります。これは VPN 接続の定義の一部ではありませんが、システムがピアを認証できるように、ローカルおよびリモートピアのアイデンティティ証明書に署名するために使用した信頼できる CA 証明書をアップロードする必要があります。

SSL 復号ポリシー：内部、内部証明書、および信頼できる CA 証明書および証明書グループ

（必須）SSL 復号ポリシーは、以下の目的のため証明書を使用します。

- 内部証明書は既知のキー復号ルールに使用されます。
- 内部 CA 証明書は、クライアントと 脅威に対する防御 デバイス間にセッションを作成するときに、再署名の復号ルールに使用されます。
- 信頼できる CA 証明書は、脅威に対する防御デバイスとサーバ間にセッションを作成するときに、再署名の復号ルールに間接的に使用されます。信頼できる CA 証明書は、サーバの証明書の署名機関を検証するために使用されます。 これらの証明書は、直接設定するか、ポリシー設定において証明書グループで設定できます。システムには、Cisco-Trusted-Authorities グループで収集された多数の信頼できる CA 証明書が含まれるため、追加の証明書をアップロードする必要はないことがあります。

例：OpenSSL を使用した内部証明書の生成

次の例では、OpenSSL コマンドを使用して内部サーバーの証明書を生成します。OpenSSL は openssl.org から取得できます。具体的な情報については、OpenSSL のマニュアルを参照してください。この例で使用するコマンドは変更される場合があり、この他にも利用できるオプションがある可能性もあります。

この手順は、脅威に対する防御にアップロードする証明書の取得方法について、1つの考え方を示すものです。

（注） 次に示す OpenSSL コマンドは一例にすぎません。セキュリティ要件に合わせてパラメータを調整してください。

手順

ステップ 1 キーを生成します。

```
openssl genrsa -out server.key 4096
```

ステップ 2 証明書署名要求（CSR）を生成します。

```
openssl req -new -key server.key -out server.csr
```

ステップ 3 キーと CSR を持つ自己署名証明書を生成します。

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Device Manager は暗号化キーをサポートしないため、自己署名証明書を生成するときはリターンキーを押してチャレンジパスワードをスキップしてください。

ステップ 4 内部証明書のオブジェクトを Device Manager で作成するときは、正しいフィールドにファイルをアップロードします。

ファイルの内容をコピーして貼り付けることもできます。サンプルコマンドは、次のファイルを作成します。

- server.crt：[サーバー証明書（Server Certificate）] フィールドにコンテンツをアップロードするか、貼り付けます。
- server.key：[証明書キー（Certificate Key）] フィールドにコンテンツをアップロードするか、貼り付けます。キーの生成時にパスワードを入力すると、次のコマンドを使用してそれを復号できます。出力は stdout に送信され、コピーできます。

  ```
  openssl rsa -in server.key -check
  ```

証明書の設定

Threat Defense PEM または DER 形式の X509 証明書をサポートします。OpenSSL を使用して必要に応じて証明書を生成、信頼できる認証局から取得、または自己署名証明書を作成します。

証明書の詳細については、証明書について （179 ページ）を参照してください。

各機能にどのタイプが使用されているかについては、各機能で使用される証明書タイプ （180 ページ）を参照してください。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。オブジェクト リストに表示されている [新規証明書の作成（Create New Certificate）] リンクをクリックし、証明書プロパティを編集しながら、証明書オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [証明書（Certificates）] を選択します。

システムには、そのまま、または置き換えて使用できる次の事前定義された証明書が付属します。

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

システムには、サードパーティ証明機関からの多数の信頼されたCAの証明書も含まれています。これらは再署名の復号アクションのために SSL 復号化ポリシーが使用します。Cisco-Trusted-Authorities グループにはこれらの証明書がすべて含まれており、このグループが SSL 復号ポリシーで使用されるデフォルトグループです。

定義済みの検索フィルタをクリックすると、リストを [システム定義（System-defined）] の証明書または [ユーザー定義（User-defined）] の証明書のみに制限できます。また、[脆弱キー（Weak Key）] フィルタを使用して、推奨される最小長よりも短いキーを持つ証明書を検索できます。それらの証明書を、より長いキーを持つ証明書に置き換えることをお勧めします。

ステップ 2 次のいずれかを実行します。

- 新しい証明書オブジェクトを作成するには、[+] メニューから証明書のタイプに適したコマンドを使用します。
- 新しい証明書グループを作成するには、 をクリックし、[証明書グループの追加（Add Certificate Group）] を選択します。
- 証明書やグループを表示または編集するには、証明書の編集アイコン（）または表示アイコン（）をクリックします。

- 参照されていない証明書やグループを削除するには、証明書のごみ箱アイコン（）をクリックします。

証明書の作成と編集の詳細については、次のトピックを参照してください。

- 内部および内部 CA 証明書のアップロード （184 ページ）
- 自己署名内部および内部 CA 証明書の生成 （186 ページ）
- 信頼できる CA 証明書のアップロード （188 ページ）
- 信頼できる CA 証明書グループの設定 （190 ページ）

内部および内部 CA 証明書のアップロード

内部アイデンティティ証明書は、特定のシステムまたはホストの証明書です。

内部 CA 証明書は、他の証明書の署名に使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。

この証明書は、OpenSSL ツールキットを使用して自分で生成するか、認証局から取得できます。その後、次の手順を使用してアップロードします。キー生成の例については、例：OpenSSL を使用した内部証明書の生成 （181 ページ）を参照してください。

自己署名内部アイデンティティ証明書および内部 CA 証明書を生成することもできます。自己署名内部 CA 証明書を設定する場合は、CA はデバイス自体で稼働します。自己署名証明書の作成の詳細については、自己署名内部および内部 CA 証明書の生成 （186 ページ）を参照してください。

これらの証明書を使用する機能の詳細については、各機能で使用される証明書タイプ （180 ページ）を参照してください。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [証明書（Certificates）] を選択します。

ステップ 2 次のいずれかを実行します。

- **[+] > [内部証明書の追加（Add Internal Certificate）]** をクリックし、次に [証明書とキーのアップロード（Upload Certificate and Key）] をクリックします。
- **[+] > [内部CA証明書の追加（Add Internal CA Certificate）]** をクリックし、次に [証明書とキーのアップロード（Upload Certificate and Key）] をクリックします。
- 証明書を編集または表示するには、情報アイコン（）をクリックします。ダイアログボックスには、証明書の件名、発行者、および有効な時間範囲が表示されます。[証明書

の置換（Replace Certificate）] をクリックして、新しい証明書とキーをアップロードします。ダイアログ ボックスで証明書とキーを貼り付けることもできます。

ステップ 3 [Name] に証明書の名前を入力します。

名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 4 [証明書のアップロード（Upload Certificate）]（編集する場合は、[証明書の置換（Replace Certificate）]）をクリックし、証明書ファイル（例：*.crt）を選択します。許可されるファイル拡張子は、.pem、.cert、.cer、.crt、および .der です。または、証明書に貼り付けます。

証明書は PEM または DER 形式の X509 証明書である必要があります。

貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

ステップ 5 [キーのアップロード（Upload Key）]（または編集時に、[キーの交換（Replace Key）]）をクリックし、証明書ファイル（例：*.key）を選択します。ファイル拡張子は .key である必要があります。または、証明書のキーに貼り付けます。

キーは暗号化できず、RSA キーである必要があります。

次に例を示します。

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

ステップ 6 [OK] をクリックします。

キーサイズが、生成された自己署名証明書で許可されている最小サイズよりも小さい場合、証明書が推奨の最小要件を満たしていないことを示す警告が表示されます。いずれにしても [続

行（Proceed）] をクリックして証明書をアップロードしますが、新しい強力な証明書を作成することをお勧めします。

自己署名内部および内部 CA 証明書の生成

内部アイデンティティ証明書は、特定のシステムまたはホストの証明書です。

内部 CA 証明書は、他の証明書の署名に使用できる証明書です。これらの証明書は、基本制約拡張と CA フラグに関して内部アイデンティティ証明書と異なります。これらは CA 証明書では有効ですが、アイデンティティ証明書では無効です。

ユーザは、自己署名内部アイデンティティと内部 CA 証明書を生成できます。つまり、証明書はデバイス自体によって署名されます。自己署名内部 CA 証明書を設定すると、CA がデバイス上で有効になります。システムは、証明書とキーの両方を生成します。

また、これらの証明書は、OpenSSL を使用して作成することも、信頼できる CA から取得してアップロードすることもできます。詳細については、内部および内部 CA 証明書のアップロード（184 ページ）を参照してください。

これらの証明書を使用する機能の詳細については、各機能で使用される証明書タイプ（180 ページ）を参照してください。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [証明書（Certificates）] を選択します。

ステップ 2 次のいずれかを実行します。

- **[+] > [内部証明書の追加（Add Internal Certificate）]** をクリックし、次に [自己署名証明書（Self-Signed Certificate）] をクリックする。
- **[+] > [内部CA証明書の追加（Add Internal CA Certificate）]** をクリックし、次に [自己署名証明書（Self-Signed Certificate）] をクリックする。

（注） 証明書を編集または表示するには、情報アイコン（ⓘ）をクリックします。ダイアログ ボックスには、証明書の件名、発行者、および有効な時間範囲が表示されます。[証明書の置換（Replace Certificate）] をクリックして、新しい証明書とキーをアップロードします。証明書を交換する際は、次の手順で説明されている自己署名の特性を設定し直すことはできません。代わりに、内部および内部 CA 証明書のアップロード（184 ページ）の説明に従って、新しい証明書を貼り付けるかアップロードする必要があります。残りの手順は、新しい自己署名証明書のみに適用されます。

ステップ 3 [Name] に証明書の名前を入力します。

名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 4 証明書の件名および発行者の情報については、次の少なくとも 1 つを設定します。

- **Country**（C）：証明書に含める 2 文字の ISO 3166 国コード。たとえば、米国の国コードは US です。ドロップダウン リストから国コードを選択します。
- **State or Province**（ST）：証明書に含める都道府県または州。
- **Locality or City**（L）：都市の名前など、証明書に含める地域。
- **Organization**（O）：証明書に含める組織または会社の名前。
- **Organizational Unit (Department)**（OU）：証明書に含める組織単位の名前（部門名など）。
- **Common Name**（CN）：証明書に含める X.500 共通名。これは、デバイスの名前、Web サイト、または他の文字列にできます。この要素は、通常は正常な接続のために必要です。たとえば、リモートアクセス VPN で使用する内部証明書に CN を含める必要があります。
- [キータイプ（Key Type）]：この証明書用に生成するキーのタイプ：RSA、ECDSA（楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA））、または EdDSA（エドワード曲線デジタル署名アルゴリズム）。
- [キーサイズ（Key Size）]：生成するキーのサイズ。一般に、キーが長いほど、安全性が高くなります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり、交換処理にも時間がかかります。許可されるサイズはキータイプによって異なります。
  - RSA キーは 2048、3072、または 4096 ビットです。
  - ECDSA キーは 256、384、または 521 ビットです。

    EdDSA キーは 256 ビットです。
- [有効期間（Validity Period）]：証明書が有効と見なされる期間。有効期限の設定に関係なく、デフォルトは本日から 825 日です。デフォルトに戻すには、[デフォルトの設定（Set default）] をクリックします。次のいずれかの方法を使用して、期間を設定できます。期限が切れる前に必ず証明書を交換してください。
  - [日付別（By Date）]：[期限日（Expiration Date）] をクリックして、証明書が有効と見なされる最終日を選択します。
  - [日数別（By Number of Days）]：証明書が有効と見なされる本日からの日数を入力します。数字を入力したら、[日付別（By Date）] をクリックして、計算された期限日を確認できます。

ステップ 5 [保存（Save）] をクリックします。

信頼できる CA 証明書のアップロード

信頼できる認証局（CA）の証明書は、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。

これらの証明書を使用する機能の詳細については、各機能で使用される証明書タイプ（180ページ）を参照してください。

外部の認証局から信頼できる CA 証明書を取得するか、自身の内部 CA を使用して（OpenSSL ツールを使用するなど）CA 証明書を作成します。その後、次の手順を使用して証明書をアップロードします。

始める前に

システムは 1 日に 1 回シスコに連絡して、新しいまたは更新された信頼できる CA 証明書があるかどうかを判断し、更新された証明書があればダウンロードします。毎日このジョブを実行することで、プレインストールされた証明書が最新の状態に保たれます。**show cert-update** コマンドを使用して、CLI でこの自動チェックを監視できます。**configure cert-update auto-update disable** コマンドを使用して毎日のジョブを無効にし、**configure cert-update run-now** コマンドを使用して更新を手動でダウンロードできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [証明書（Certificates）] を選択します。

ステップ 2 次のいずれかを実行します。

- **[+] > [信頼済みCAの証明書の追加（Add Trusted CA Certificate）]** をクリックします。
- 証明書を編集するには、その証明書の編集アイコン（  ）をクリックします。

ステップ 3 [Name] に証明書の名前を入力します。

名前は、設定時にオブジェクト名としてのみ使用され、証明書自体には含まれません。

ステップ 4 [証明書のアップロード（Upload Certificate）]（または、編集時は [証明書の置換（Replace Certificate）]）をクリックして、信頼できる CA 証明書ファイル（*.pem など）を選択します。許可されるファイル拡張子は、.pem、.cert、.cer、.crt、および .der です。または、信頼できる CA 証明書に貼り付けます。

証明書内のサーバ名は、サーバのホスト名または IP アドレスと一致している必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

証明書は PEM または DER 形式の X509 証明書である必要があります。

貼り付ける証明書は、BEGIN CERTIFICATE と END CERTIFICATE の行を含める必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

ステップ 5 この証明書が認証局によって発行されていない場合は、[CA証明書のチェックをスキップする（Skip CA Certificate Check）] を選択します。

信頼できるCA証明書としてローカルCA証明書をインストールする必要がある場合は、チェックをスキップしてください。

ステップ 6 [検証の使用（Validation Usage）] を設定して、証明書の使用を制限します。

一部の機能では、特定の証明書に対して接続を検証できるかどうかを選択できます。それらの機能が証明書を有効に使用できることを証明書で示す必要があります。そうしないと、接続が拒否されます。

これらのオプションに含まれていない機能は、明示的な使用許可なしでこの証明書に対して検証できます。たとえば、SSL復号ポリシー、およびDevice Manager をホストするWebサーバーは、[検証の使用（Validation Usage）] オプションを無視します。このフィールドでオプションを選択すると、**show running-config** コマンドを使用して表示される実行コンフィギュレーションに証明書がダウンロードされます。

これらのオプションの主な目的は、特定の証明書に対して検証できるため、VPN接続が確立されないようにすることです。

- [SSLサーバー（SSL Server）]：リモートSSLサーバーで証明書を検証します。ダイナミック DNS に使用されます。
- [SSL クライアント（SSL Client）]：着信リモートアクセス VPN 接続の証明書を検証します。
- [IPsec クライアント（IPsec Client）]：着信 IPsec サイト間 VPN 接続の証明書を検証します。
- [その他（Other）]：Snort検査エンジンで管理されない機能（LDAPSなど）を検証します。このオプションは、特定の機能に問題がある場合にのみ選択します。[その他（Other）]は他のすべてのオプションと相互に排他的です。他のオプションを選択する前に [その他（Other）] を選択解除し、[その他（Other）] を選択する前にすべてのオプションを選択解除する必要があります。

ステップ 7 [OK] をクリックします。

信頼できる CA 証明書グループの設定

SSL 復号ポリシー設定で外部の信頼できる CA 証明書グループを使用して、SSL 復号ポリシーが信頼する必要がある証明書を指定します。エンドユーザーが、証明書の発行者の証明書が信頼できる証明書に含まれていないサイトに接続しようとすると、証明書を信頼することを求めるメッセージが表示されます。そのため、信頼できるリストに証明書がないと、エンドユーザーの利便性は低下しますが、それ自体が接続を妨げることはありません（アクセス制御ルールを使用して実現することは可能）。

デフォルトグループは Cisco-Trusted-Authorities です。次の場合にのみ、独自のグループを作成する必要があります。

- デフォルトグループにない証明書を信頼する必要がある場合。作成後、SSL 復号ポリシー設定でデフォルトグループと新しいグループの両方を選択します。
- デフォルトグループよりも限定された証明書リストを信頼する必要がある場合。作成後、信頼できる証明書の完全なリスト（差分だけでなく）を持つグループを作成し、SSL 復号ポリシー設定で唯一のグループとして選択します。

始める前に

グループに追加するすべての信頼できる CA 証明書をアップロードします（システムにまだない場合）。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [証明書（Certificates）] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しい証明書グループを作成するには、 をクリックし、[証明書グループの追加（Add Certificate Group）] を選択します。
- 証明書グループを編集するには、そのグループの編集アイコン（）をクリックします。

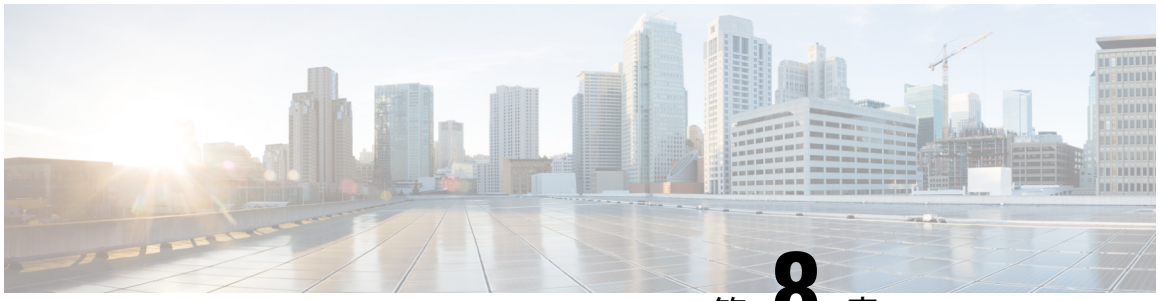
ステップ 3 証明書グループの [名前（Name）] を入力し、任意で説明を入力します。

ステップ 4 [+] をクリックし、証明書をグループに追加します。

グループに必要なすべての証明書を追加します。グループの作成時に [新規信頼CA証明書の作成（Create New Trusted CA Certificate）] をクリックして新しい証明書をアップロードできます。

グループ内の証明書が不要になった場合は、証明書の [X] アイコン（右横）をクリックします。

ステップ 5 [OK] をクリックします。



第 8 章

アイデンティティ ソース

アイデンティティ ソースは、ユーザー アカウントを定義するサーバーとデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

ここでは、アイデンティティ ソースの定義方法について説明します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。

アイデンティティ ソースについて

アイデンティティソースは、組織内のユーザーのユーザーアカウントを定義する AAA サーバーおよびデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。

[オブジェクト（Objects）] > [アイデンティティソース（Identity Sources）] ページを使用して、ソースを作成および管理します。アイデンティティ ソースを必要とするサービスを設定するときに、次のオブジェクトを使用します。

サポートされているアイデンティティソースとその使用方法は次のとおりです。

Active Directory（AD）アイデンティティレルム

Active Directory は、ユーザーアカウントおよび認証情報を提供します。Active Directory（AD）アイデンティティレルム （193 ページ）を参照してください。

このソースは、以下の目的で使用できます。

- リモートアクセス VPN（プライマリ アイデンティティ ソースとして）。AD は RADIUS サーバーと組み合わせて使用可能。

- アイデンティティポリシー（アクティブ認証用、およびパッシブ認証で使用されるユーザー アイデンティティ ソースとして）。

AD（Active Directory）レルムシーケンス

AD レルムシーケンスは、AD レルムオブジェクトの番号付きリストです。レルムシーケンスは、ネットワーク内で複数の AD ドメインを管理する場合に役立ちます。AD レルムシーケンスの設定 （198 ページ）を参照してください。

このソースは、以下の目的で使用できます。

- パッシブ認証で使用されるユーザー ID ソースとしての ID ポリシー。シーケンス内のレルムの順序によって、競合が発生しているまれな状況で、システムがユーザー ID を決定する方法が決まります。

Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）

ISE を使用している場合は、脅威に対する防御デバイスと ISE 展開を統合できます。Identity Services Engine（ISE） （205 ページ）を参照してください。

このソースは、以下の目的で使用できます。

- アイデンティティポリシー（ISE からユーザーアイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

RADIUS サーバー、RADIUS サーバーグループ

RADIUS サーバーを使用している場合は、それらを Device Manager で使用することもできます。それぞれのサーバーを個別のオブジェクトとして定義し、それらをサーバーグループ（特定グループ内のサーバーは互いのコピー）に入れる必要があります。サーバーグループを機能に割り当て、個々のサーバーは割り当てないでください。RADIUS サーバおよびグループ （200 ページ）を参照してください。

このソースは、以下の目的で使用できます。

- 認証、および許可、アカウンティングのアイデンティティソースとしてのリモートアクセス VPN。AD は RADIUS サーバーと組み合わせて使用できます。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザーアイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。
- Device Manager または 脅威に対する防御 CLI 管理ユーザーの外部認証。許可レベルが異なる複数の管理ユーザーをサポートできます。これらのユーザーは、デバイスの設定とモニタリングのためにシステムにログインできます。

SAML サーバー

セキュリティ アサーション マークアップ言語 2.0（SAML 2.0）は、当事者間、特に ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するためのオープン標準です。

このソースは、以下の目的で使用できます。

- シングルサインオン（SSO）認証ソースとしてのリモートアクセス VPN。
- Device Manager ユーザーの外部認証。許可レベルが異なる複数の管理ユーザーをサポートできます。これらのユーザーは、デバイスの設定とモニタリングのためにシステムにログインできます。

LocalIdentitySource

これはローカル ユーザー データベースです。これには Device Manager で定義したユーザーが含まれます。このデータベースのユーザーアカウントを管理するには、**[オブジェクト（Objects）]** > **[ユーザー（Users）]** を選択します。ローカル ユーザー （213 ページ）を参照してください。

（注） ローカル アイデンティティ ソース データベースには、CLI アクセス用に CLI で設定するユーザーは含まれません（**configure user add** コマンドを使用）。CLI ユーザーは、Device Manager で作成するユーザーとは完全に別のユーザーです。

このソースは、以下の目的で使用できます。

- リモートアクセス VPN（プライマリまたはフォールバック アイデンティティ ソースとして）。
- アイデンティティ ポリシー（リモート アクセス VPN ログインからユーザー アイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

Active Directory（AD）アイデンティティレルム

Microsoft Active Directory（AD）はユーザーアカウントを定義します。Active Directory ドメイン用に AD アイデンティティレルムを作成できます。ここでは、AD アイデンティティレルムの定義方法について説明します。

サポートされるディレクトリ サーバー

Windows Server 2012、2016、2019 で Microsoft Active Directory（AD）を使用できます。

サーバーの設定に関して次の点に注意してください。

- ユーザー グループまたはグループ内のユーザーに対してユーザー制御を実行する場合、ディレクトリ サーバーでユーザー グループを設定する必要があります。サーバーが基本的なオブジェクト階層でユーザーを整理している場合、システムはユーザー グループ制御を実行できません。
- ディレクトリ サーバーは、次の表に示すフィールド名を使用して、システムがそのフィールドのサーバーからユーザー メタデータを取得できるようにする必要があります。

メタデータ（Metadata）	Active Directory フィールド
LDAP ユーザ名	samaccountname
名	givenname
last name	sn
メール アドレス	メール アドレス userprincipalname（mail に値が設定されていない場合）
部署	部署 distinguishedname（department に値が設定されていない場合）
電話番号	telephonenumber

ユーザー数の制限

Device Manager はディレクトリサーバーから最大 50,000 人のユーザーに関する情報をダウンロードできます。

ディレクトリ サーバに 50,000 以上のユーザ アカウントが含まれる場合、アクセス ルールでユーザを選択するとき、またはユーザベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

この制限は、グループに関連付けられた名前にも適用されます。グループに 50,000 を超えるメンバーが含まれている場合は、ダウンロードした 50,000 個の名前だけをグループメンバーシップと照合できます。

ディレクトリ ベースの DN の決定

ディレクトリの各プロパティを設定する際、ユーザおよびグループに共通のベース識別名（DN）を指定する必要があります。ベースはディレクトリ サーバ内で定義され、ネットワークごとに異なります。アイデンティティ ポリシーが正しく機能するには、適切なベースを入力する必要があります。ベースが誤っていると、ユーザ名またはグループ名が特定されず、アイデンティティに基づくポリシーが機能しなくなります。

ヒント　正しいベースを取得するには、ディレクトリ サーバを担当する管理者に確認してください。

Active Directory の場合は、ドメイン管理者として Active Directory サーバにログインし、コマンドプロンプトで **dsquery** コマンドを次のように使用することで、正しいベースを判別できます。

ユーザ検索ベース

dsquery user コマンドを入力し、ベース識別名を調べる既知のユーザ名（一部または全部）を指定します。たとえば次のコマンドでは、部分名「John*」を使用して、「John」で始まるすべてのユーザに対する情報を返します。

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

ベース DN は「DC=csc-lab,DC=example,DC=com」となります。

グループ検索ベース

dsquery group コマンドを入力し、ベース識別名を調べたい既知のグループ名を指定します。たとえば次のコマンドでは、グループ名「Employees」を使用して識別名を返します。

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

グループのベース DN は「DC=csc-lab,DC=example,DC=com」となります。

ADSI Edit プログラムを使用して、Active Directory 構造を参照することもできます（**[スタート（Start）]** > **[ファイル名を指定して実行（Run）]** > **[adsiedit.msc]**）。ADSI Edit で、組織単位（OU）、グループ、ユーザなど任意のオブジェクトを右クリックし、[プロパティ（Properties）] を選択すると、識別名が表示されます。DC 値の文字列を、ベースとしてコピーします。

正しいベースであることを確認するには、次の手順を実行します。

1. ディレクトリ プロパティの [テスト接続（Test Connection）] ボタンをクリックし、接続を確認します。問題があった場合には修正して、ディレクトリ プロパティを保存します。
2. 変更をデバイスに適用します。
3. アクセス ルールを作成して、[ユーザ（Users）] タブを選択し、ディレクトリから既知のユーザおよびグループ名の追加を試みます。ディレクトリを含むレルム内の一致ユーザ名およびグループ名を入力すると、入力中にオートコンプリートによる候補が表示されます。ドロップダウンリストに候補が表示される場合は、システムがディレクトリに適切に照会できたことを意味します。入力した文字列がユーザ名またはグループ名として表示されることが確かであるにもかかわらず、候補が表示されない場合は、対応する検索ベースを修正する必要があります。

AD アイデンティティ レルムの設定

アイデンティティ レルムとは、認証サービスの提供に必要なディレクトリ サーバーとその他の属性のことです。ディレクトリ サーバーには、ネットワークへのアクセスを許可されているユーザーおよびユーザー グループについての情報が含まれます。

Active Directoryの場合、レルムはActive Directoryドメインに相当します。サポートする必要がある AD ドメインごとに個別のレルムを作成します。

レルムは次のポリシーで使用されます。

- アイデンティティ：レルムは、ユーザー アイデンティティ情報とグループ メンバーシップ情報を提供します。次いでそれらの情報をアクセス コントロール ルールで使用できます。システムは、毎日の最終時間（UTC）に、すべてのユーザーとグループに関する更新情報をダウンロードします。ディレクトリ サーバに管理インターフェイスから到達できる必要があります。
- リモート アクセス VPN：レルムは、接続が許可されているかどうかを判断する認証サービスを提供します。ディレクトリ サーバに RA VPN 外部インターフェイスから到達できる必要があります。
- アクセス制御、SSL 復号：レルム内のすべてのユーザーにルールを適用するため、ユーザーの基準でレルムを選択することができます。

ディレクトリ管理者に相談して、ディレクトリ サーバーのプロパティの設定に必要な値を取得します。

（注） ディレクトリ サーバーが接続済みネットワークに存在しない場合や、デフォルト ルートで使用できない場合には、サーバーのスタティック ルートを作成します。スタティック ルートを作成するには、**[デバイス（Device）]** > **[ルーティング（Routing）]** > **[表示設定（View Configuration）]** の順に選択します。 または、サーバーを定義するときに適切なインターフェイスを選択します。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。レルム プロパティの編集時に、オブジェクト リストに表示される [新しいアイデンティティ レルムの作成（Create New Identity Realm）] リンクをクリックして、アイデンティティ レルムを作成することもできます。

始める前に

ディレクトリサーバー、Threat Defense デバイス、およびクライアント間で、時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイムゾーンを使用できますが、たとえば、10 AM PST = 1 PM EST など、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から **[アイデンティティ ソース（Identity Sources）]** を選択します。

ステップ 2 次のいずれかを実行します。

- AD レルムを作成するには、**[+]** > **[AD]** をクリックします。
- 既存のレルムを編集するには、そのレルムの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 基本レルムのプロパティを設定します。

- [名前（Name）]：ディレクトリ レルムの名前。
- [タイプ（Type）]：ディレクトリ サーバのタイプ。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [ディレクトリユーザ名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN（Base DN）]：ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリ ツリー。例、cn=users,dc=example,dc=com。ベース DN の検索の詳細については、ディレクトリ ベースの DN の決定 （194 ページ）を参照してください。
- [ADプライマリドメイン（AD Primary Domain）]：デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。例、example.com。

ステップ 4 ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。
- [インターフェイス（Interface）]：AD サーバーに到達するためのインターフェイス。インターフェイスを選択しない場合、データ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検索されます。管理専用インターフェイスを使用する場合は、そのインターフェイスを具体的に選択する必要があります。管理専用ルーティングテーブルからルートルックアップを使用することはできません。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。
- [暗号化（Encryption）]：ユーザおよびグループの情報のダウンロードに暗号化された接続を使用するには、希望の方法（[STARTTLS] または [LDAPS]）を選択します。デフォルト

では [なし（None）] になっており、ユーザおよびグループの情報がクリア テキストでダウンロードされます。

- [STARTTLS] では、暗号化方式をネゴシエートし、ディレクトリ サーバでサポートされる最も強力な方式を使用します。ポート 389 を使用します。このオプションは、リモート アクセス VPN にレルムを使用する場合はサポートされません。
- [LDAPS] では、LDAP over SSL が必要です。ポート 636 を使用します。

- [信頼できるCA証明書（Trusted CA Certificate）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリ サーバ間の信頼できる接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で ad.example.com を使用すると接続が失敗します。

ステップ 5 レルムの複数のサーバーがある場合は、[別の設定の追加（Add Another Configuration）] をクリックし、追加サーバーごとのプロパティを入力します。

最大 10 の AD サーバーをレルムに追加できます。これらのサーバーは互いに複製である必要があり、同じ AD ドメインをサポートする必要があります。

各サーバーエントリは適宜折りたたんだり展開することができます。セクションには、ホスト名または IP アドレスとポートラベルが付けられます。

ステップ 6 [テスト（Test）]ボタンをクリックして、システムがサーバーに接続できることを確認します。

システムは別個のプロセスおよびインターフェイスを使用してサーバにアクセスします。このため、アイデンティティ ポリシーでは接続に成功してリモート アクセス VPN では失敗するなど、ある使用方法では接続が成功しても、別の方法では失敗したことを示すエラーが表示される場合があります。サーバーに到達できない場合は、正しい IP アドレスとホスト名を指定していること、DNS サーバーに当該ホスト名のエントリなどが設定されていることを確認します。サーバーにスタティック ルートを設定する必要があるかもしれません。詳細については、ディレクトリ サーバー接続のトラブルシューティング （199 ページ）を参照してください。

ステップ 7 [OK] をクリックします。

AD レルムシーケンスの設定

パッシブ ID ルールで AD レルムシーケンスを使用すると、システムが複数の AD サーバーでユーザーの照合を試みることができるようになります。レルムシーケンスで、各 AD サーバーが別個のレルムまたはドメイン（engineering.example.com や marketing.example.com など）を管理する AD レルムの番号付きリストを設定します。

レルムシーケンスは、複数の AD ドメインをサポートしていて、異なるドメインのユーザーが Threat Defense デバイスを介してトラフィックを送信する可能性がある場合にのみ役立ちます。

レルムは、受動的に認証されるユーザーセッションの ID を検索するために使用されます。レルムの順序は、まれに競合が発生した場合に、ID の競合を解決するために使用されます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- AD レルムシーケンスを作成するには、**[+]**>**[AD レルムシーケンス（AD Realm Sequence）]** をクリックします。
- AD レルムシーケンスを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 レルムシーケンスのプロパティを設定します。

- [名前（Name）]：オブジェクトの名前。
- [説明（Description）]：（オプション）オブジェクトの説明。
- [AD レルム（AD Realms）]：[+] をクリックして、AD レルムオブジェクトをシーケンスに追加します。レルムを追加したら、目的の順序になるように、レルムをクリックしてドラッグアンドドロップします。

ステップ 4 [OK] をクリック

パッシブ ID ルールで AD レルムシーケンスを選択できるようになりました。

ディレクトリ サーバー接続のトラブルシューティング

システムは、機能に応じて異なるプロセスを使用して、ディレクトリ サーバーと通信します。そのため、アイデンティティ ポリシー用の接続は機能しますが、リモート アクセス VPN 用の接続は失敗します。

これらのプロセスでは、さまざまなインターフェイスを使用してディレクトリ サーバと通信します。次のインターフェイスからの接続を確認する必要があります。

- 管理インターフェイス（アイデンティティ ポリシーの場合）
- データ インターフェイス（リモート アクセス VPN（外部インターフェイス）の場合）

アイデンティティ レルムを設定する場合、[テスト（Test）] ボタンを使用して接続が機能することを確認します。障害メッセージによって、接続上の問題がある機能が示されます。次に、

認証属性およびルーティング/インターフェイス設定に基づいて、発生する可能性がある一般的な問題を示します。

ディレクトリユーザーの認証の問題。

ユーザー名またはパスワードが原因でシステムがディレクトリ サーバーにログインできない問題の場合、名前とパスワードが正しく、ディレクトリ サーバーで有効なことを確認します。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

また、システムはユーザー名とパスワードの情報から ldap-login-dn と ldap-login-password も生成します。たとえば、Administrator@example.com は cn=administrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザーは、共通名の「users」フォルダの下で設定する必要があります。

ディレクトリ サーバーにはデータ インターフェイスを介してアクセスできます。

ディレクトリ サーバーがデータ インターフェイス（GigabitEthernet インターフェイスなど）に直接接続されているネットワークまたは直接接続されたネットワークからルーティング可能なネットワーク上にある場合、仮想管理インターフェイスとディレクトリ サーバーの間にルートがあることを確認する必要があります。

- **data-interfaces** を管理ゲートウェイとして使用するには、ルーティングを成功させる必要があります。
- 管理インターフェイス上に明示的なゲートウェイがある場合、そのゲートウェイ ルータにディレクトリ サーバーへのルートが存在している必要があります。
- 直接接続されたネットワークとディレクトリ サーバーをホストするネットワークの間にルータがある場合、ディレクトリ サーバーのスタティック ルートを設定します（**[デバイス（Device）] > [ルーティング（Routing）]**）。
- データ インターフェイスの IP アドレスとサブネットマスクが正しいことを確認します。

ディレクトリ サーバーは外部ネットワークにあります。

ディレクトリ サーバーが外部（アップリンク）インターフェイスの反対側のネットワークにある場合、サイト間 VPN 接続を設定する必要がある場合があります。詳細な手順については、リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方法 （892 ページ）を参照してください。

RADIUS サーバおよびグループ

RADIUS サーバーを使用して、リモートアクセス VPN 接続、および Device Manager と脅威に対する防御 CLI 管理ユーザーの認証および認可を行うことができます。たとえば、Cisco Identity

Services Engine（ISE）とその RADIUS サーバーも使用する場合は、Device Manager でそのサーバーを使用できます。

RADIUS サーバを使用するように機能を設定する場合は、個別のサーバではなく RADIUS グループを選択します。RADIUS グループは、相互にコピーである RADIUS サーバの集合です。グループに複数のサーバがある場合は、それらは、1 つのサーバが使用できなくなった場合に冗長性を提供する一連のバックアップ サーバを形成します。ただし、サーバが 1 つしかない場合でも、機能の RADIUS サポートを設定するには、メンバーが 1 つのグループを作成する必要があります。

ここでは、サポートされている機能で使用できるように RADIUS サーバおよびグループを設定する方法について説明します。

RADIUS サーバーの設定

RADIUS サーバーは、AAA（認証、認可、アカウンティング）サービスを提供します。RADIUS サーバーを使用してユーザーを認証および認可すると、これらのサーバーを Device Manager と一緒に使用できます。

RADIUS サーバーごとにオブジェクトを作成した後、重複サーバーの各グループを含む RADIUS サーバーグループを作成します。

始める前に

RA VPN のリダイレクト ACL を設定する場合は、スマート CLI を使用して、サーバーオブジェクトを作成または編集する前に拡張 ACL を作成する必要があります。オブジェクトの編集中に ACL を作成することはできません。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティ ソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+]** > **[RADIUSサーバー（RADIUS Server）]** をクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 次のプロパティを設定します。

- [名前（Name）]：オブジェクトの名前。 サーバーで設定されているものと一致している必要はありません。

- [サーバー名またはIPアドレス（Server Name or IP Address）]：サーバーの完全修飾ホスト名（FQDN）またはIPアドレス。たとえば、radius.example.com または 10.100.10.10 とします。
- [認証ポート（Authentication Port）]：RADIUS 認証および承認が行われるポートです。デフォルトは 1812 です。
- [タイムアウト（Timeout）]：次のサーバーに要求を送信する前にサーバーからの応答を待機する時間の長さ（1 ～ 300 秒）。デフォルトは 10 秒です。認証トークンの入力を求めるなどのために、このサーバーをリモートアクセス VPN のセカンダリ認証ソースとして使用している場合は、このタイムアウトを少なくとも 60 秒に増やします。この間に、ユーザーはトークンを取得して入力できます。
- [サーバー秘密キー（Server Secret Key）]：（オプション）脅威に対する防御 デバイスと RADIUS サーバー間でデータを暗号化するために使用される共有秘密キー。キーは、大文字と小文字が区別される最大 64 文字の英数字文字列です。スペースは使用できません。キーは、英数字または下線で開始する必要があります。特殊文字 $ & - _ . + @ を使用できます。文字列は、RADIUS サーバーで設定された文字列と一致している必要があります。秘密キーを設定していない場合、接続は暗号化されません。

ステップ 4 （オプション）リモートアクセス VPN の認可変更設定のためにサーバーを使用している場合は、[RA VPNのみ（RA VPN Only）] リンクをクリックし、次のオプションを設定できます。

- [ACLのリダイレクト（Redirect ACL）]：RA VPN リダイレクト ACL を使用する拡張 ACL を選択します。**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** ページのスマート CLI 拡張アクセスリストオブジェクトを使用して、拡張 ACL を作成します。

  リダイレクト ACL の目的は、Cisco Identity Services Engine（ISE）がクライアントポスチャを評価できるように、初期トラフィックを ISE に送信することです。ACL は、ISE に HTTPS トラフィックを送信しますが、ISE 宛てのトラフィックや、名前解決のために DNS サーバーに送信されるトラフィックは送信しません。例については、Threat Defense デバイスでの認可変更の設定 （870 ページ）を参照してください。
- [RADIUSサーバーに接続するために使用されるインターフェイス（Interface Used to Connect to RADIUS Server）]：サーバーと通信するときに使用するインターフェイス。[ルートルックアップ経由で解決する（Resolve via Route Lookup）] を選択した場合、システムは常にデータルーティングテーブルを使用して使用するインターフェイスを決定します。[インターフェイスを手動で選択する（Manually Choose Interface）] を選択すると、システムは常に選択されたインターフェイスを使用します。管理専用インターフェイスを使用する場合は、そのインターフェイスを具体的に選択する必要があります。管理専用ルーティングテーブルにルートルックアップを使用することはできません。

  認可変更を設定する場合、システムがインターフェイスで CoA リスナーを適切に有効にできるように、特定のインターフェイスを選択する必要があります。

  Device Manager 管理アクセスにもこのサーバーを使用する場合、このインターフェイスは無視されます。管理アクセスの試行は、常に管理 IP アドレスを介して認証されます。

ステップ 5 （任意。オブジェクトを編集する場合のみ）[テスト（Test）]をクリックして、システムがサーバーに接続できるかどうか確認します。

ユーザー名とパスワードの入力を求められます。テストでは、サーバーを接続できるかどうか、接続できる場合はユーザー名が認証されるかどうかを確認します。

ステップ 6 [OK] をクリックします。

RADIUS サーバー グループの設定

RADIUS サーバーグループには、1 つまたは複数の RADIUS サーバーオブジェクトが含まれています。グループ内のサーバーは、相互にコピーされる必要があります。グループ内のサーバーでバックアップサーバーのチェーンが形成されるため、最初のサーバーが利用できなった場合、システムはリスト上の次のサーバーを試すことができます。

ある機能に RADIUS サポートを設定する場合、サーバーグループを選択する必要があります。したがって、RADIUS サーバーが 1 台しかなくても、それを含むサーバーグループを作成する必要があります。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+]** > **[RADIUSサーバーグループ（RADIUS Server Group）]** をクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（ ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（ ）をクリックします。

ステップ 3 次のプロパティを設定します。

- [名前（Name）]：オブジェクトの名前。 サーバーで設定されているものと一致している必要はありません。
- [デッドタイム（Dead Time）]：失敗したサーバーは、すべてのサーバーが失敗した後にのみ再アクティブ化されます。デッドタイムは、最後のサーバーが失敗した後にすべてのサーバーを再アクティブ化するまで待機する時間の長さ（0 ～ 1440分）です。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。
- [最大失敗試行回数（Maximum Failed Attempts）]：次のサーバーを試行する前に、グループ内の RADIUS サーバーに送信された AAA トランザクションの失敗数（応答がなかった

要求の数）。1～5を指定できます。デフォルトは3です。最大失敗試行回数を超えると、システムはそのサーバーを故障としてマークします。

特定の機能について、ローカルデータベースを使用するフォールバック方式を設定していて、グループ内のすべてのサーバーが応答に失敗した場合、そのグループは非応答と見なされ、フォールバック方式が試行されます。サーバー グループはデッド タイムの間、非応答とマークされたままになるため、その期間内に追加の AAA 要求でサーバー グループへの接続は試行されず、フォールバック方式がすぐに使用されます。

- ダイナミック認証（RA VPNの場合のみ）、ポート：RADIUS サーバー グループ向けの RADIUS ダイナミック認証または認可変更（CoA）サービスを有効にすると、グループは CoA 通知用に登録され、Cisco Identity Services Engine（ISE）からの指定した CoA ポリシー更新用ポートをリッスンします。デフォルトのリスニングポートは 1700 ですが、1024 ～ 65535 の範囲で別のポートを指定することができます。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。
- [RADIUSサーバーをサポートするレルム（Realm that Supports the RADIUS Server）]：AD サーバーを使用してユーザーを認証するように RADIUS サーバーが設定されている場合は、この RADIUS サーバーと組み合わせて使用される AD サーバーを指定する AD レルムを選択します。レルムが存在していない場合は、リストの下部にある [新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックして作成します。
- [RADIUSサーバーリスト（RADIUS Server list）]：グループのサーバーを定義する RADIUS サーバー オブジェクトを最大 16 個選択します。優先順にこれらのオブジェクトを追加します。リストの最初のサーバーが、非応答になるまで使用されます。オブジェクトを追加した後に、ドラッグアンドドロップで並び替えることができます。必要なオブジェクトがまだない場合は、[新規RADIUSサーバーの作成（Create New RADIUS Server）] をクリックしてすぐに追加します。

  [テスト（Test）] リンクをクリックして、システムがサーバーに接続できることを確認することもできます。ユーザー名とパスワードの入力を求められます。テストでは、サーバーを接続できるかどうか、接続できる場合はユーザー名が認証されるかどうかを確認します。

ステップ 4 （オプション）[すべてのサーバーをテスト（Test All Servers）] ボタンをクリックして、グループ内の各サーバーへの接続を確認します。

ユーザー名とパスワードの入力を求められます。システムは、各サーバーに接続できるかどうか、各サーバーでユーザー名が認証されるかどうかを確認します。

ステップ 5 [OK] をクリックします。

RADIUS サーバーおよびグループのトラブルシューティング

次に、外部認証が機能しない場合に確認する項目を示します。

- RADIUS サーバーの [テスト（Test）] ボタンとサーバーグループオブジェクトを使用して、デバイスからサーバーに通信できることを確認します。テストする前に、必ずオブジェクトを保存してください。テストが失敗した場合：
  - テストは、サーバーに設定されたインターフェイスを無視し、常に管理インターフェイスを使用することを理解しておいてください。RADIUS 認証プロキシが管理 IP アドレスからの要求に応答するように設定されていない場合、テストは失敗することが予想されます。
  - テスト中に正しいユーザー名/パスワードの組み合わせを入力していることを確認します。正しくない場合は、ログイン情報が不正であるというメッセージが表示されます。
  - 秘密鍵、ポート、およびサーバーの IP アドレスを確認します。ホスト名を使用している場合は、DNS が管理インターフェイス用に設定されていることを確認します。秘密鍵がデバイス設定ではなく RADIUS サーバーで変更された可能性を考えます。
  - テストが引き続き失敗する場合は、RADIUS サーバーへのスタティックルートを設定する必要があります。CLI コンソールまたは SSH セッションからサーバーに ping を試行して、到達できるかどうか確認します。
- 外部認証が機能していたのに機能しなくなった場合は、すべてのサーバーがデッドタイムになっている可能性を考えます。ローカル認証へのフォールバックを設定する場合、グループ内のすべての RADIUS サーバーが失敗したときに、システムが最初のサーバーを再試行する前に待機する時間（分単位）がデッドタイムです。デッドタイム中は、ローカル認証が使用されるため、指定したユーザーのユーザー名とパスワードがローカルのユーザー名/パスワードになります。デフォルトは 10 分ですが、1440 分までの範囲で設定できます。
- HTTPS 外部認証が一部のユーザーでしか機能しない場合は、各ユーザーアカウントの RADIUS サーバーで定義されている cisco-av-pair 属性を評価します。この属性の設定が正しくない可能性があります。属性が欠落しているか不正であると、そのユーザーアカウントのすべての HTTS アクセスがブロックされます。
- SSH 外部認証が一部のユーザーでしか機能しない場合は、各ユーザーアカウントの RADIUS サーバーで定義されている Service-Type 属性を評価します。この属性の設定が正しくない可能性があります。属性が欠落しているか不正であると、そのユーザーアカウントのすべての SSH アクセスがブロックされます。

Identity Services Engine（ISE）

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を 脅威に対する防御 デバイスと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザーに関するユーザー認識データを提供します。ただし、脅威に対する防御 では、AD との組み合わせでのみユーザーアイデンティティ認

識にISEを使用できます。さまざまな監視ダッシュボードおよびイベントでユーザー情報を表示できるだけでなく、アクセス制御およびSSL復号ポリシーでユーザーアイデンティティを一致基準として使用できます。

Cisco ISE/ISE-PIC の詳細については、『*Cisco Identity Services Engine Administrator Guide*』（https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html）および『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*』（https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html）を参照してください。

ISE に関する注意事項と制限事項

- ファイアウォールシステムでは、システムがデバイス認証をユーザーと関連付けないため、Active Directory認証とともに802.1xデバイス認証を使用することはできません。802.1xアクティブログインを使用する場合は、802.1xアクティブログインのみをレポートするようにISEを設定します（デバイスとユーザーの両方）。この設定により、デバイスログインは一度だけシステムにレポートされます。
- ISE/ISE-PIC は、ISE ゲストサービスユーザーのアクティビティをレポートしません。
- ISE/ISE-PIC サーバーとデバイスの時刻を同期させます。そうしないと、システムが予期しない間隔でユーザーのタイムアウトを実行する可能性があります。
- 多数のユーザー グループをモニターするように ISE/ISE-PIC を設定した場合、システムはメモリ制限のためにグループに基づいてユーザーマッピングをドロップすることがあります。その結果、レルムまたはユーザー条件を使用するルールが想定どおりに実行されない可能性があります。
- システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、『*Cisco Secure Firewall Compatibility Guide*』（https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html）を参照してください。
- ご使用のバージョンの ISE が IPv6 をサポートしていることを確認できないかぎり、ISE サーバーの IPv4 アドレスを使用してください。

Identity Services Engine の設定

Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）をパッシブ アイデンティティ ソースとして使用するには、ISE Platform Exchange Grid（pxGrid）サーバへの接続を設定する必要があります。

始める前に

- ISEからpxGridサーバおよびMNTサーバの証明書をエクスポートします。たとえば、ISE PIC 2.2 では、**[証明書（Certificates）] > [証明書の管理（Certificate Management）] > [システム証明書（System Certificates）]** ページにあります。MNT（モニタリングおよびトラブルシューティング ノード）は、証明書リストの [使用者（Used By）] 列に [管理者

（Admin）] として表示されます。これらは、**[オブジェクト（Objects）] > [証明書（Certificates）]** ページで信頼できる CA 証明書としてアップロードするか、次の手順でアップロードできます。これらのノードは、同じ証明書を使用することがあります。

- AD アイデンティティ レルムを設定する必要もあります。システムは、AD からユーザのリストを取得し、ISE から user-to-IP アドレス マッピングに関する情報を取得します。
- 静的セキュリティ グループ タグ マッピングの有無にかかわらず、アクセス制御にセキュリティグループタグ（SGT）を使用し、SXP トピックをリッスンする場合は、ISE で SXP とこれらのマッピングも設定する必要があります。ISE でのセキュリティ グループと SXP パブリッシングの設定 （634 ページ）を参照してください。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アイデンティティソース（Identity Sources）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+] > [Identity Services Engine]** をクリックします。最大で 1 つの ISE オブジェクトを作成できます。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 次のプロパティを設定します。

- [名前（Name）]：オブジェクトの名前。
- [ステータス（Status）]：クリックしてオブジェクトを有効または無効にします。無効にすると、アイデンティティ ルールで ISE をアイデンティティ ソースとして使用できません。
- [説明（Description）]：（オプション）オブジェクトの説明。
- [プライマリ ノードホスト名/IP アドレス（Primary Node Hostname/IP Address）]：プライマリ pxGrid ISE サーバのホスト名または IP アドレス。ISE バージョンが IPv6 をサポートしていることを確認しない限り、IPv6 アドレスを指定しないでください。
- [セカンダリ ノードのホスト名/IP アドレス（Secondary Node Hostname/IP Address）]：ハイアベイラビリティ向けにセカンダリ ISE サーバーを設定している場合、[セカンダリ ノードのホスト名/IP アドレスの追加（Add Secondary Node Hostname/IP Address）] をクリックし、セカンダリ pxGrid ISE サーバーのホスト名または IP アドレスを入力します。
- [pxGrid サーバ CA 証明書（pxGrid Server CA Certificate）]：pxGrid フレームワークの信頼できる認証局の証明書。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

- [MNTサーバCA証明書（MNT Server CA Certificate）]：一括ダウンロードを実行する場合に使用するISE証明書の信頼できる認証局の証明書。これは、MNT（モニタリングおよびトラブルシューティング）サーバーが分かれていない場合、pxGridサーバー証明書と同じものにできます。展開にプライマリとセカンダリのMNTノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- [サーバ証明書（Server Certificate）]：ISEへの接続時または一括ダウンロードの実行時に脅威に対する防御 デバイスがISEに提供する必要がある内部アイデンティティ証明書。
- [登録（Subscribe To）]：登録する必要があるISE pxGridトピックを選択します。トピックを登録すると、そのトピックに関連するデータがダウンロードされます。
  - [セッション ディレクトリ トピック（Session Directory Topic）]：ユーザーセッションのSGTマッピングを含む、ユーザーセッションに関する情報を取得するかどうか。このオプションは、デフォルトで有効です。セキュリティポリシーで使用するためや、監視ダッシュボードで表示するためにパッシブユーザーIDを取得する場合は、このオプションを選択する必要があります。
  - [SXPトピック（SXP Topic）]：SGTからIPアドレスへの静的マッピングを取得するかどうか。セキュリティグループタグ（SGT）に基づくアクセス制御ルールを作成する場合は、このトピックを選択します。
- [ISEネットワークフィルタ（ISE Network Filters）]：ISEがシステムに報告するデータを制限するように設定できる任意のフィルタ。ネットワーク フィルタを指定すると、ISEはフィルタ内のネットワークからのみデータを報告します。[+]をクリックして、ネットワークを識別するネットワーク オブジェクトを選択し、[OK]をクリックします。オブジェクトを作成する必要がある場合は、[新しいネットワークの作成（Create New Network）]をクリックします。IPv4ネットワーク オブジェクトのみを設定します。

ステップ4 [テスト（Test）]ボタンをクリックして、システムがISEサーバに接続できることを確認します。

テストが失敗した場合は、[ログの表示（See Logs）]リンクをクリックして、詳細なエラーメッセージを確認します。たとえば、次のメッセージはシステムが必要なポートでサーバに接続できなかったことを示しています。問題はホストへのルートが存在しないことである可能性があります。つまり、ISEサーバが予期されたポートを使用していないか、接続を妨げるアクセス制御ルールが存在します。

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

ステップ5 [OK]をクリックしてオブジェクトを保存します。

次のタスク

ISEを設定したら、アイデンティティポリシーを有効にして、パッシブ認証ルールを設定し、その設定を展開します。その後、ISE/ISE PICに移動して、デバイスをサブスクライバとして

許可する必要があります。サブスクライバを自動的に許可するよう ISE/ISE PIC を設定している場合、サブスクリプションを手動で許可する必要はありません。

ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング

ISE/ISE-PIC 接続

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE を脅威に対する防御デバイスに正常に統合するには、ISE の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- ISE サーバーと脅威に対する防御デバイスの間の接続を確立するには、ISE のクライアントを手動で承認する必要があります。

  または、『*Cisco Identity Services Engine* 管理者ガイド』の「ユーザーおよび外部 ID ソースの管理」の章にある説明に従って、ISE で [新しいアカウントの自動承認（Automatically approve new accounts）] を有効にできます。
- 脅威に対する防御デバイス（サーバー）証明書には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、他の拡張キー使用値を含むことはできません。clientAuth 拡張キーの使用が設定されている場合は、キーの使用も設定されていないか、デジタル署名キー使用値が設定されている必要があります。Device Manager を使用して作成できる自己署名アイデンティティ証明書は、これらの要件を満たしています。
- ISE サーバーの時間は、脅威に対する防御デバイスの時間と同期する必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザーのタイムアウトが実行される可能性があります。

ISE/ISE-PIC ユーザーデータ

ISE または ISE-PIC によって報告されるユーザー データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザーのアクティビティを検出すると、サーバーからそれらに関する情報を取得します。ISE ユーザーによるアクティビティは、アクセス制御ルールで処理されず、システムがユーザーダウンロードでそのユーザーに関する情報を正常に取得するまでダッシュボードに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザーに対するユーザー制御は実行できません。
- システムは、ISE ゲストサービスユーザーのユーザーデータを受信しません。

SAML サーバー

セキュリティ アサーション マークアップ言語 2.0（SAML 2.0）サーバーを設定して、リモートアクセス VPN 接続およびデバイスマネージャユーザーのシングルサインオン（SSO）認証ソースとして使用することができます。SAML は、当事者間、特に ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するためのオープン標準です。

SAML サーバーの設定

セキュリティ アサーション マークアップ言語 2.0（SAML 2.0）サーバーを設定して、リモートアクセス VPN 接続およびデバイスマネージャユーザーのシングルサインオン（SSO）認証ソースとして使用することができます。たとえば、Duo Access Gateway（DAG）は SAML サーバーです。

SAML サーバーを認証方法として使用する場合、SAML サーバーはアイデンティティ プロバイダー（IdP）として機能し、Threat Defense デバイスはサービスプロバイダー（SP）として機能します。

RA VPN の場合、SAML サーバーをプライマリ認証ソースとして使用できますが、セカンダリ認証ソースを設定したり、フォールバック ソースを設定したりすることはできません。

デバイスマネージャのログインでは、SAML サーバーをサポートするように設定している場合、SAML サーバーを使用するときに Common Access Card（CAC）をログインに使用できます。

始める前に

SAML サーバー アイデンティティ プロバイダーから次の情報を取得します。可能であれば、簡単にアップロードできるように XML ファイルでユーザーから情報をダウンロードします。

- エンティティ ID URL（SAML サーバーメタデータを提供）
- サインイン URL
- サインアウト URL
- アイデンティティ プロバイダー証明書

手順

ステップ 1 [SAMLサーバー（SAML Servers）] ページに移動するには、次のいずれかを実行します。

- [オブジェクト（Objects）] を選択し、目次から [アイデンティティソース（Identity Sources）] を選択します。

- **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[SAMLサーバー（SAML Servers）]** を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、**[+]** > **[SAMLサーバー（SAML Server）]** をクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 次のプロパティを設定します。

- [名前（Name）]：オブジェクトの名前。
- [説明（Description）]：（オプション）オブジェクトの説明。
- [アイデンティティ プロバイダー（IDP）エンティティID URL（Identity Provider (IDP) Entity ID URL）]：SAML 発行元が要求に応答する方法を記述したメタデータ XML を提供するページの URL。これは、一部の SAML サーバー製品ではエンティティ ID と呼ばれ、他の製品ではメタデータ URL と呼ばれます。この URL は、プロトコル（https://）を含めて 4 ～ 256 文字である必要があります。たとえば、https://191.168.2.21/dag/saml2/idp/metadata.php のようになります。

  （注） SAML サーバーから XML ファイルで情報をダウンロードした場合は、[XML ファイルから読み込む（Populate from XML file）] をクリックし、ファイルを選択します。このフィールドと [サインインURL（Sign-In URL）] と [アイデンティティプロバイダー証明書（Identity Provider Certificate）] は、XML ファイルから読み込むことができます。

- [サインインURL（Sign-In URL）]：アイデンティティ プロバイダー SAML サーバーにサインインするための URL。この URL は、プロトコルを含めて 4 ー 500 文字である必要があります。http:// と https:// の両方を使用できます。たとえば、https://191.168.2.21/dag/saml2/idp/SSOService.php のようになります。
- [サインアウトURL（Sign-Out URL）]：アイデンティティ プロバイダー SAML サーバーからサインアウトするための URL。この URL は、プロトコルを含めて 4 ー 500 文字である必要があります。http:// と https:// の両方を使用できます。たとえば、https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php のようになります。
- [サービスプロバイダー証明書（Service Provider Certificate）]：Threat Defense デバイスに使用する内部証明書。認定済みのサードパーティによって署名された証明書がすでにアップロードされていると理想的であり、ここでそれを選択できます。組み込みの DefaultInternalCertificate を使用することや、ここで [新しい内部証明書の作成（Create New Internal Certificate）] をクリックして署名済みの証明書をアップロードすることもできます。SAML サーバー アイデンティティ プロバイダーはこの証明書を信頼する必要があるため、証明書を SAML サーバーにアップロードする必要がある場合があります。証明書

をアップロードする方法や、その他の方法でサービスプロバイダーとの信頼関係を有効にする方法については、SAML サーバーのマニュアルを参照してください。

- [アイデンティティ プロバイダー証明書（Identity Provider Certificate）]：SAML サーバー アイデンティティ プロバイダーの信頼できる CA 証明書。この証明書は SAML サーバーからダウンロードします。まだアップロードしていない場合は、ここで [新しい信頼できるCA証明書の作成（Create New Trusted CA Certificate）] をクリックしてアップロードしてください。
- [要求の署名（Request Signature）]：ログイン要求の署名時に使用する暗号化アルゴリズム。暗号化を無効にする場合は、[なし（None）] を選択します。それ以外の場合は、[SHA1]、[SHA256]、[SHA384]、または [SHA512] のいずれか（後のものほど強力）を選択してください。
- [要求タイムアウト（Request Timeout）]：SAML アサーションには有効な期間があります。ユーザーは、有効な期間内にシングルサインオン要求を完了する必要があります。この期間を変更するために、秒単位でタイムアウトを設定できます。アサーションの NotOnOrAfter 条件よりも長いタイムアウトを設定すると、タイムアウトは無視され、NotOnOrAfter が使用されます。指定できる範囲は 1 ～ 7200 秒です。デフォルトは 300 秒です。
- [このSAMLアイデンティティ プロバイダー（IDP）は内部ネットワーク上にある（This SAML identity provider（IDP）is on an internal network）]：SAML サーバーが、保護されたネットワークへの内部ネットワーク（外部ネットワークではなく）上で動作しているかどうか。
- [ログイン時のIDP再認証の要求（Request IDP re-authentication at login）]：SAML サーバーに以前の認証セッションを再利用させるのではなく、ログインごとにユーザーが再認証されるようにするには、このオプションを選択します。このオプションは、デフォルトで有効です。

ステップ 4 [ユーザーロール（User Roles）] をクリックし、外部ユーザーの RBAC 許可ロールを設定します。

- [デフォルトユーザーロール（Default User Role）]：このページの設定で決定できない場合にユーザーに割り当てる許可ロール。
- [グループメンバー属性（Group Member Attribute）]：ユーザーの RBAC 許可ロールを定義する SAML サーバーのユーザー属性。
- [ロールマッピング（Role Mapping）]：ロールごとに、ロールに対応する SAML ユーザー レコードのグループメンバー属性に表示される文字列を入力します。
  - [管理者（Administrator）]：アプリケーションのすべての側面に対する完全な読み取り/書き込みアクセス権を持つユーザー。
  - [暗号管理者（Cryptographic Admin）]：証明書、復号ポリシー、秘密キーなどの暗号化関連機能を設定できるユーザー。他の機能への読み取り専用アクセス。
  - [監査管理者（Audit Admin）]：ユーザーのログイン履歴と監査ログを表示し、監査関連のアクションを実行できるユーザー。設定機能への読み取り専用アクセス。

- [読み取り/書き込み（Read-Write）]：読み取り専用ユーザーが実行できることをすべて実行でき、設定を編集および展開することもできるユーザー。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、他の Device Manager ユーザーセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- [読み取り専用（Read-Only）]：ダッシュボードおよび設定を表示できますが、変更することはできないユーザー。変更しようとすると、権限がないことを示すエラーメッセージが表示されます。

ステップ 5 [OK] をクリック

次のタスク

通信を暗号化するために [署名の要求（Request Signature）] を有効にした場合は、デバイスマネージャ情報を SAML サーバーにアップロードする必要があります。ID ソースのリストから、サーバーの [ダウンロード（Download）]（）ボタンをクリックし、XML ファイルを保存します。次に、SAML サーバーにログインし、情報をアップロードします。詳細については、SAML プロバイダーのマニュアルを参照してください。

デバイスマネージャのログインにサーバーを使用しているのに機能しない場合は、SAML サーバーの設定を確認します。

- SAML IdP にログインし、デバイスマネージャの SAML 応答コンシューマが正しく設定されていることを確認します。次の値である必要があります：https://<FDM_URL>/api/fdm/latest/fdm/token
- SAML サーバーオブジェクトで署名が有効になっている場合は、デバイスマネージャのパブリック証明書が SAML アプリケーションにアップロードされ、暗号化が有効になっていることを確認します。デバイスマネージャの XML ファイルをアップロードすると、証明書が SAML サーバーに追加されます。FDM API を使用してデバイスマネージャ証明書を取得することもできます：https://<FDM_URL>/saml/metadata

ローカル ユーザー

ローカル ユーザー データベース（LocalIdentitySource）には Device Manager で定義したユーザーが含まれます。

ローカル定義ユーザーは、次の目的で使用できます。

- リモートアクセス VPN（プライマリまたはフォールバック アイデンティティ ソースとして）。
- 管理アクセス（Device Manager ユーザーのプライマリまたはセカンダリソースとして）。

管理者ユーザーはシステム定義のローカルユーザーです。ただし、管理者ユーザーはリモートアクセス VPN にログインできません。追加のローカル管理者ユーザーは作成できません。

管理アクセスの外部認証を定義すると、デバイスにログインしている外部ユーザーがローカルユーザーのリストに表示されます。

- アイデンティティポリシー（間接的）（リモートアクセス VPN ログインからユーザーアイデンティティを収集するためのパッシブ アイデンティティ ソースとして）。

ここでは、ローカルユーザーの設定方法について説明します。

ローカル ユーザーの設定

リモート アクセス VPN で使用するユーザー アカウントをデバイスで直接作成できます。外部認証ソースの代わりに、またはそれに加えて、ローカルユーザーアカウントを使用できます。

リモート アクセス VPN のフォールバック認証方式としてローカル ユーザ データベースを使用する場合、必ず外部データベースの名前と同じユーザ名/パスワードをローカル データベースで設定します。そうしなければ、フォールバック メカニズムは効果を発揮しません。

ここで定義されたユーザは、デバイス CLI にログインできません。

手順

ステップ 1 **[オブジェクト（Objects）] > [ユーザ（Users）]** を選択します。

リストに、次のようなユーザ名とサービス タイプが表示されます。

- MGMT：Device Manager にログインできる管理ユーザー向け。管理者ユーザが常に定義されており、削除することはできません。また、追加の MGMT ユーザを設定することもできません。ただし、管理アクセス用の外部認証を定義すると、デバイスにログインする外部ユーザが MGMT ユーザとしてローカル ユーザ リストに表示されます。
- RA VPN：デバイスに設定されたリモート アクセス VPN にログインできるユーザー向け。プライマリ ソースまたはセカンダリ（フォールバック）ソースのローカル データベースも選択する必要があります。

ステップ 2 次のいずれかを実行します。

- ユーザを追加するには、[+] をクリックします。
- ユーザーを編集するには、そのユーザーの [編集（edit）] アイコン（  ）をクリックします。

特定のユーザー アカウントが必要なくなったら、そのユーザーの [削除（delete）] アイコン（  ）をクリックします。

ステップ 3 ユーザ プロパティを設定します。

名前とパスワードには、印刷可能ASCII英数字または特殊文字（スペースと疑問符を除く）を使用できます。印刷可能文字は ASCII コード 33 ～ 126 です。

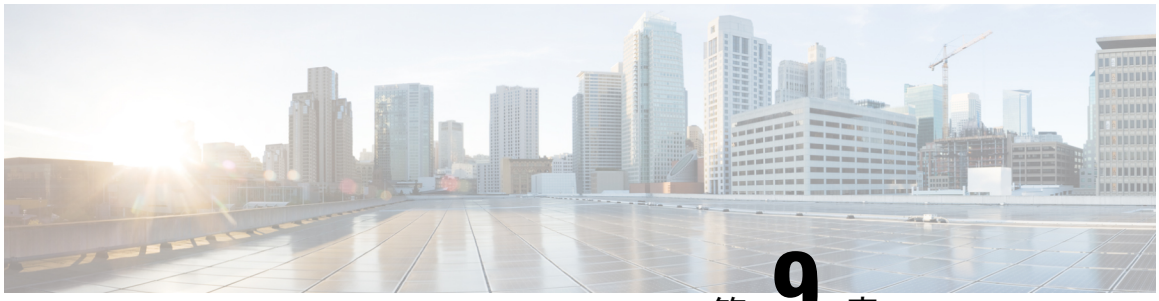
- [名前（Name）]：リモート アクセス VPN にログインするためのユーザ名。名前には 4 ～ 64 文字を使用できますが、スペースは使用できません（例：johndoe）。
- [パスワード（Password）]、[パスワードの確認（Confirm Password）]：アカウントのパスワードを入力します。パスワードの長さは、8～16文字にする必要があります。同じ文字を連続して使用することはできません。数字、大文字、小文字、および特殊文字をそれぞれ 1 文字以上使用する必要もあります。

（注） ユーザは、自分のパスワードを変更できません。ユーザにパスワードを通知します。パスワードを変更する必要がある場合は、ユーザアカウントを編集する必要があります。また、外部 MGMT ユーザのパスワードは更新しないでください。パスワードは外部 AAA サーバによって制御されています。

ステップ 4 [OK] をクリックします。

第 III 部

基本



第 9 章

Firepower 4100/9300 上の論理デバイス

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。

シャーシインターフェイスを設定し、論理デバイスを追加し、Secure Firewall シャーシマネージャ または FXOS の CLI を使用して Firepower 4100/9300 シャーシ上のデバイスにインターフェイスを割り当てる必要があります。これらのタスクは、Device Manager では実行できません。

この章では、基本的なインターフェイスの設定、および 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。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。

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 シャーシマネージャ によって、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、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

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（脅威に対する防御Management Center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。アプリケーションと管理によっては、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（219 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。

- Eventing： Management Center デバイスを使用した 脅威に対する防御 のセカンダリ管理インターフェイスとして使用します。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 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。Device Manager および CDO はクラスタリングをサポートしていません。

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。

Firepower 9300 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 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-48 をモジュール 1、SM-40 をモジュール 2 、SM-56 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。
- 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、各シャーシには SM-40、SM-48、および SM-56 があります。SM-40 モジュール間、SM-48 モジュール間、および SM-56 モジュール間にハイアベイラビリティペアを作成できます。
- ASA および Threat Defense 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 Threat Defense をインストールすることができます。
- ASA または Threat Defense 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 Threat Defense 6.3 を、モジュール 2 に Threat Defense 6.4 を、モジュール 3 に Threat Defense 6.5 をインストールできます。

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。

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

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。
- 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。
  - 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。
- 詳細については、ハイ アベイラビリティのシステム要件（243 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、EtherChannel を追加して、インターフェイス プロパティを編集できます。

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 [インターフェイス（Interfaces）] を選択して、[インターフェイス（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、**無効なスライダ**（  ）をクリックします。これで、**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、**有効なスライダ**（  ）をクリックして、**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。

（注） QSFPH40G-CUxMの場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。

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。

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。

各メンバーインターフェイスが LACP 更新を送受信するように、Firepower 4100/9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。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。

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。

論理デバイスの設定

スタンドアロン論理デバイスまたはハイ アベイラビリティのペアを Firepower 4100/9300 シャーシ に追加します。

Device Manager のスタンドアロン Threat Defense を追加します。

Device Manager はネイティブインスタンスで使用できます。コンテナインスタンスはサポートされていません。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。

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 にします。
- 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、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。
- 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
  - DNS サーバの IP アドレス
  - Threat Defense ホスト名とドメイン名

手順

セキュリティポリシーの設定を始めるには、Device Manager のコンフィギュレーション 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

Threat Defense 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

ハイ アベイラビリティのシステム要件 （243 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（フェールオーバー） （233 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。

Threat Defense 論理デバイスのインターフェイスの変更

脅威に対する防御論理デバイスでは、インターフェイスの割り当てや割り当て解除を行うことができます。その後、Device Manager でインターフェイス設定を同期できます。

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、脅威に対する防御の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティ ルール、VPN、DHCP サーバなど、脅威に対する防御の設定における多くの場所で直接参照されている可能性があります。セキュリティゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつDevice Managerでの同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

古いインターフェイスを削除する前に、あるインターフェイスから別のインターフェイスに設定を移行できます。

始める前に

- 物理インターフェイスの設定 （224 ページ）およびEtherChannel（ポート チャネル）の追加 （224 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。

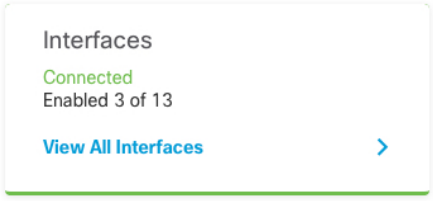
- ハイアベイラビリティのため、Device Manager で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にスタンバイユニットでインターフェイスを変更してから、アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイス モニタリングに影響を及ぼさないことに注意してください。

手順

ステップ 1 Device Manager でインターフェイスを同期して移行します。

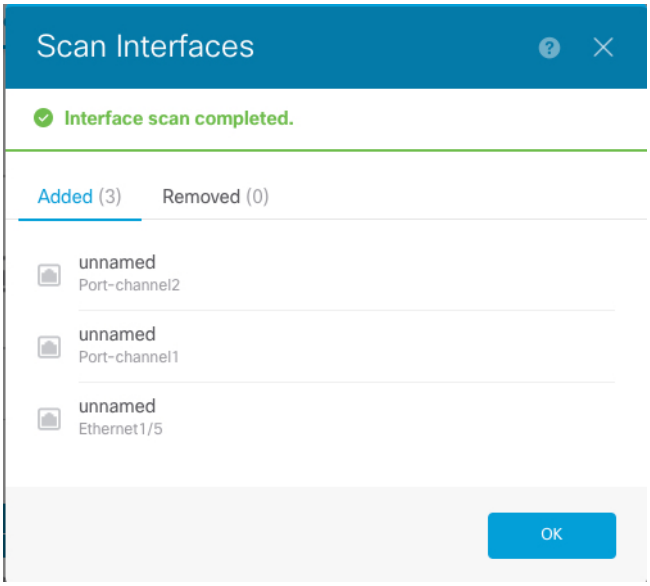
a) Device Manager にログインします。

b) [デバイス（Device）] をクリックしてから、**[インターフェイス（Interfaces）]** サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。



c) [インターフェイス（Interfaces）] アイコンをクリックします。

d) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



e) 新しいインターフェイスに名前、IP アドレスなどを設定します。

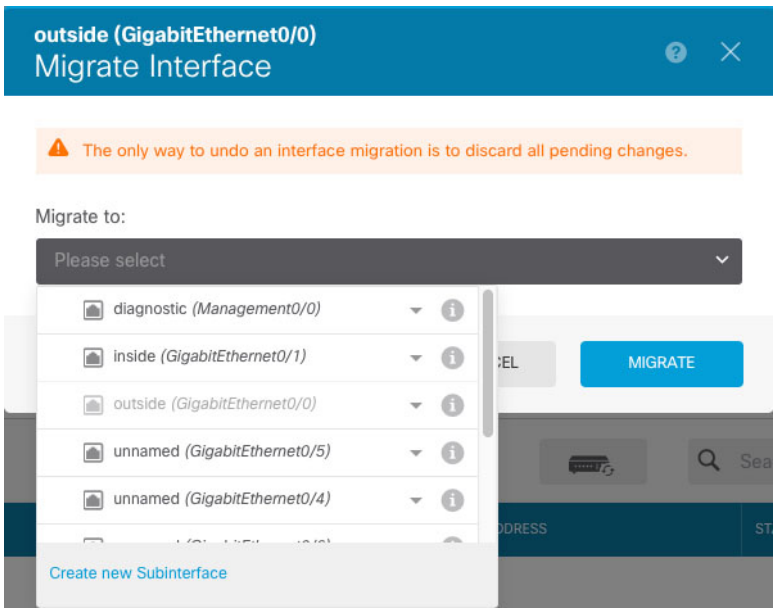
削除するインターフェイスの既存のIPアドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、古いインターフェイスをダミーの名前とIPアドレスで再設定する必要があります。

f) 古いインターフェイスを新しいインターフェイスに置き換えるには、古いインターフェイスの [置換（Replace）] アイコンをクリックします。

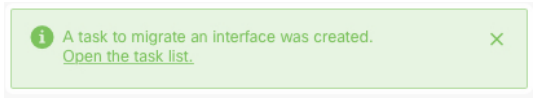
[置換（Replace）] アイコン

このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに置き換えられます。

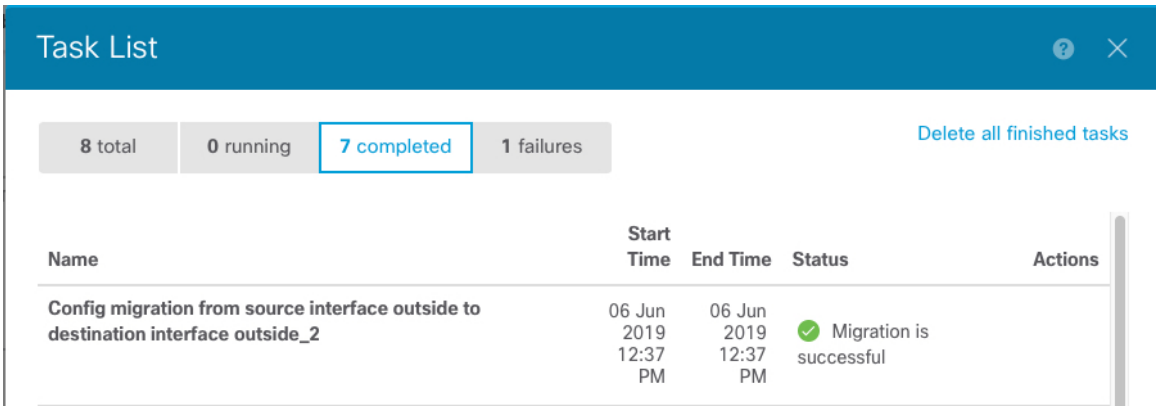
g) [交換用インターフェイス（Replacement Interface）]：ドロップダウン リストから新しいインターフェイスを選択します。



h) [インターフェイス（Interfaces）] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。

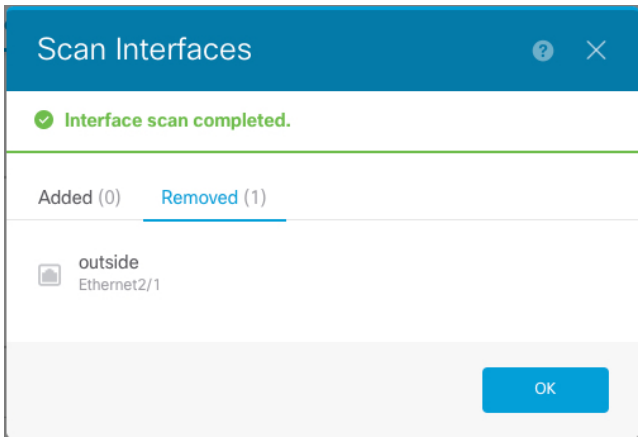


i) [タスクリスト（Task List）] を調べて、移行が成功したことを確認します。



ステップ 2 Device Manager でインターフェイスを再度同期します。

図 *6 : Device Manager* によるインターフェイスのスキャン



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 ftd *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 ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

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。

- Threat Defense ：「**exit**」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。

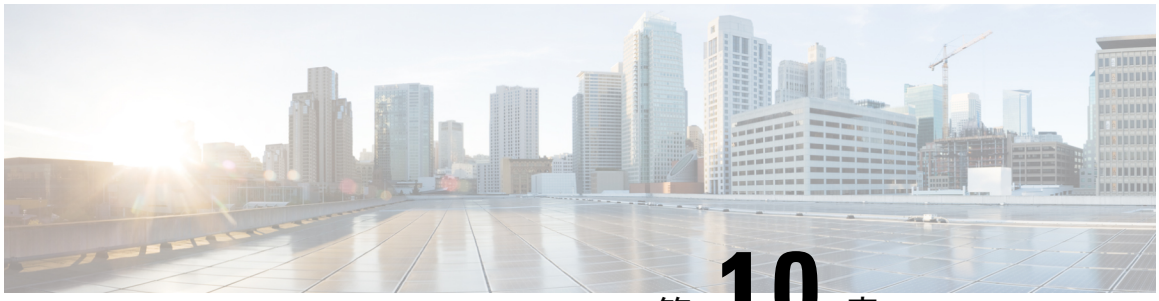
telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

Firepower 4100/9300 論理デバイスの履歴

機能	バージョン	詳細
Firepower 4100/9300 での Device Manager のサポート	6.5.0	Firepower 4100/9300 の 脅威に対する防御 論理デバイスで Device Manager を使用できるようになりました。Device Manager はマルチインスタンス機能をサポートしていません。ネイティブインスタンスのみがサポートされています。 （注） FXOS 2.7.1 が必要です。



第 10 章

ハイ アベイラビリティ（フェールオーバー）

ここでは、アクティブ/スタンバイ フェールオーバーを設定および管理して、Threat Defense システムのハイ アベイラビリティを実現する方法について説明します。

ハイ アベイラビリティ（フェールオーバー）について

ハイ アベイラビリティまたはフェールオーバー セットアップは、プライマリ デバイスの障害時にセカンダリ デバイスで引き継ぐことができるように、2つのデバイスを結合します。これにより、デバイスの障害時にネットワーク運用を維持できます。

ハイアベイラビリティを設定するには、同じ脅威に対する防御デバイスが2台、専用のフェールオーバーリンク（オプションで、ステートリンク）で相互に接続されている必要があります。2台の装置はフェールオーバーリンクを介して常に通信し、各装置の動作状態を判断して、展開された設定の変更を同期します。システムでは、フェールオーバーが発生したときにユーザー接続が維持されるように、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。

この装置はアクティブ/スタンバイペアを形成します。1台の装置がアクティブ装置となり、トラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを通過させることはありませんが、アクティブ装置の設定やその他の状態情報を同期しています。

アクティブ装置（ハードウェア、インターフェイス、ソフトウェアおよび環境ステータス）の状態は、特定のフェールオーバー条件に一致しているかどうかを確認するためにモニターされ

ます。これらの条件が満たされると、アクティブ装置がスタンバイ装置にフェールオーバーし、スタンバイ装置がアクティブになります。

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 Threat Defense デバイス 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。

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。

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 *4*: 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。
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。

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 リンクは 2 つの装置の間の専用接続です。ステートフル フェールオーバー リンクも専用接続ですが、1 つのフェールオーバー リンクをフェールオーバー リンクとステート リンクが組み合わされたものとして使用することも、個別の専用ステート リンクを作成することもできます。フェールオーバー リンクだけを使用する場合は、ステートフルな情報もそのリンクを経由し、ステートフル フェールオーバー機能は失われません。

デフォルトでは、フェールオーバー リンクおよびステートフル フェールオーバー リンク上の通信はプレーン テキスト（暗号化されない）です。IPsec 暗号キーを設定することにより、通信を暗号化してセキュリティを強化できます。

ここでは、これらのインターフェイスについて詳しく説明するとともに、最良の結果を得るためのデバイスの配線方法に関する推奨事項を示します。

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、設定の変更を同期します。

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 ステータス
- MAC アドレス交換
- 設定の複製と同期化
- システムデータベースの更新。これには、VDB やルールは含まれますが、地理位置情報データベースやセキュリティ インテリジェンス データベースは含まれません。各システムは、地理位置情報の更新やセキュリティインテリジェンスの更新を個別にダウンロードします。更新スケジュールを作成する場合は、これらの同期が維持されます。ただし、アクティブデバイスで地理位置情報やセキュリティ インテリジェンスを手動更新する場合は、スタンバイデバイスでも更新する必要があります。

（注） イベント、レポート、および監査ログデータは同期されません。イベントビューアとダッシュボードには、特定の装置に関連するデータのみが表示されます。また、展開履歴、タスク履歴、およびその他の監査ログイベントも同期されません。

ステートフル フェールオーバー リンク

システムは、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。

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 リンクの両方に単一のリンクを使用することは、インターフェイスを節約する最善の方法です。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。

フェールオーバー リンクとステート リンクのインターフェイス

使用されていないものの有効になっているデータインターフェイス（物理またはEtherChannel）を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）。フェールオーバーに管理インターフェイス、サブインターフェイス、VLANインターフェイス、あるいはスイッチポートを使用することはできません。

脅威に対する防御デバイスは、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。

フェールオーバーリンクとステートリンクのサイジングについては、次のガイドラインを参照してください。

- 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。
- 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。

フェールオーバーまたはステート リンクとしてEtherChannelインターフェイスを使用している場合、高可用性を確立する前に、両方のデバイスで同じ ID とメンバー インターフェイスを備えた同じ EtherChannel が存在していることを確認する必要があります。EtherChannel の不一致がある場合は、HA を無効にして、セカンダリユニットの設定を修正する必要があります。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。

フェールオーバーおよびステートフル フェールオーバー インターフェイスの接続

未使用のデータ物理インターフェイスは、フェールオーバーリンクやオプションの専用ステート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やサブインターフェイスを持つインターフェイスは選択できません。フェールオーバーおよびステートフル フェールオーバー リンク インターフェイスは、通常のネットワーキング インターフェイスとして設定されません。フェールオーバー通信用にのみ存在し、通過トラフィックや管理アクセスに使用することはできません。

設定がデバイス間で同期されるため、リンクの両端に同じポート番号を選択する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで GigabitEthernet 1/3 を使用します。

次のいずれかの方法で、フェールオーバーリンクおよび専用ステートリンク（使用する場合）を接続します。

- 脅威に対する防御 デバイス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）に他の装置のないスイッチを使用する。専用ステートリンクの要件は同じですが、フェールオーバーリンクとは異なるネットワークセグメントに存在する必要があります。

（注） スイッチを使用する利点は、装置のいずれかのインターフェイスがダウンした場合、障害が発生したインターフェイスのトラブルシューティングが容易であることです。直接ケーブル接続を使用する場合、1 つのインターフェイスに障害が発生すると、リンクが両方のピアでダウンし、どのデバイスで障害が発生しているのかを判別することが困難になります。

- 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。脅威に対する防御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ので、クロス ケーブルまたはストレート ケーブルのどちらでも使用できます。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。

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、脅威に対する防御デバイスはデータ 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

2 つの 脅威に対する防御 デバイス間のフェールオーバーとデータ インターフェイスの両方を接続するために1つのスイッチまたは一連のスイッチを使用している場合、スイッチまたはスイッチ間リンクがダウンしていると、両方の 脅威に対する防御 デバイス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 2 つの接続方式は推奨**しません**。

図 *7*：単一のスイッチを使用した接続：非推奨

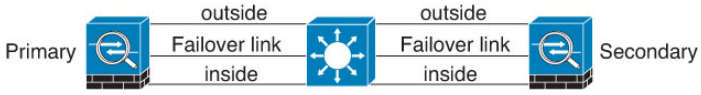
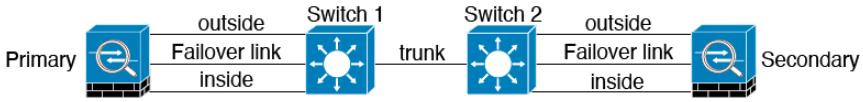


図 *8*：*2* つのスイッチを使用した接続：非推奨



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 *9*：異なるスイッチを使用した接続

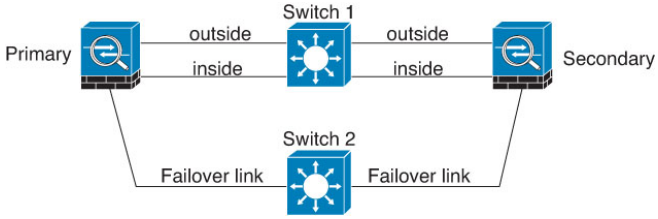
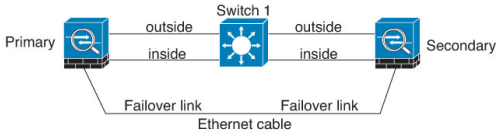


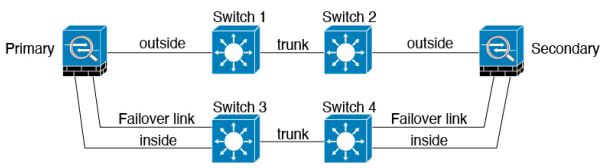
図 *10*：ケーブルを使用した接続



シナリオ 3：推奨

脅威に対する防御 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 *11*：セキュア スイッチを使用した接続



ステートフル フェールオーバーがユーザー接続に与える影響

アクティブ装置は、接続状態情報をスタンバイ装置と共有します。これは、スタンバイ装置がユーザーに影響を与えずに特定のタイプの接続を維持できることを意味します。

ただし、ステートフルフェールオーバーをサポートしないタイプの接続もあります。これらの接続については、フェールオーバーが発生した場合、ユーザーが接続を再確立する必要があります。多くの場合、これは、接続で使用されているプロトコルの動作に基づいて自動的に実行されます。

ここでは、ステートフルフェールオーバーに関してサポートされる機能またはサポートされない機能について説明します。

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 Threat Defense デバイスに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および HTTP 接続状態を含む状態。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。
- 厳密な TCP 強制を含む、Snort の接続状態、インスペクション結果、およびピンホール情報。
- 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。
- 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。
- アクセス コントロール ポリシーの判断：フェールオーバー時には、トラフィックの照合（URL、URL カテゴリ、地理位置情報など）、侵入検知、マルウェア、ファイル タイプに関する判断が保持されます。ただし、フェールオーバーの時点で評価される接続には、次のような注意事項があります。
  - AVC：App-ID 判定は複製されますが、検出状態は複製されません。フェールオーバーが発生する前に、App-ID 判定が完了および同期されていれば、正常に同期は行われます。
  - 侵入検知状態：フェールオーバーの際、フロー中にピックアップが発生すると、新しいインスペクションは完了しますが、古い状態は失われます。
  - ファイル マルウェア ブロッキング：ファイルの処分は、フェールオーバー前にできるようになる必要があります。
  - ファイル タイプ検出とブロッキング：ファイル タイプは、フェールオーバー前に特定される必要があります。元のアクティブ デバイスでファイルを特定している間にフェールオーバーが発生すると、ファイル タイプの同期は失われます。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。
- アイデンティティ ポリシーからのパッシブなユーザ識別の判断（キャプティブ ポータルを介したアクティブ認証を通じて収集されたもの以外）。
- セキュリティ インテリジェンス判断。
- 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。
- すべての接続から、確立された接続だけがスタンバイ ASA に複製されます。

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 Threat Defense デバイスに渡されません。

- GRE や IP-in-IP などのプレーンテキストトンネル内のセッション。トンネル内のセッションは複製されず、新しいアクティブ ノードは、既存のインスペクションの判定を再利用して、正しいポリシー ルールを照合することができません。
- 復号された TLS/SSL 接続：復号状態は同期されず、アクティブユニットに障害が発生すると、復号された接続がリセットされます。新しいアクティブユニットへの新しい接続を確立する必要があります。復号されていない接続（つまり、TLS/SSL[復号しない（Do Not Decrypt）] ルールアクションに一致する）は影響を受けず、正しく複製されます。
- マルチキャスト ルーティング。

スタンバイ装置で許可される設定の変更とアクション

ハイ アベイラビリティ モードで運用している場合は、アクティブ装置にのみ設定の変更を加えます。設定を展開すると、新しい変更はスタンバイ装置にも送信されます。

ただし、一部のプロパティはスタンバイ装置固有です。スタンバイ装置では次の設定を変更できます。

- 管理 IP アドレスとゲートウェイ。
- （CLI のみ）管理者ユーザーアカウントや他のローカルユーザーアカウントのパスワード。この変更を行うことができるのは CLI のみで、Device Manager で行うことはできません。すべてのローカルユーザーは、両方のユニットで個別にパスワードを変更する必要があります。

さらに、スタンバイデバイスでは次のアクションを実行できます。

- HA の一時停止、再開、リセット、解除などのハイ アベイラビリティ アクションと、アクティブ モードとスタンバイ モードの切り替え。
- ダッシュボードとイベントデータはデバイスごとに一意であり、同期されません。これには、イベントビューアのカスタムビューが含まれます。
- 監査ログ情報はデバイスごとに一意です。
- スマートライセンスの登録。ただし、アクティブ装置でオプションのライセンスを有効または無効にする必要があります。このアクションはスタンバイ装置と同期され、適切なライセンスが要求または解放されます。
- バックアップ（ただし復元ではない）。バックアップを復元するには装置で HA を解除する必要があります。バックアップに HA 設定が含まれている場合、装置は HA グループに再び参加します。
- ソフトウェアアップグレードのインストール。

- トラブルシューティングログの生成。
- 地理位置情報データベースまたはセキュリティ インテリジェンス データベースの手動更新。これらのデータベースは、装置間で同期されません。更新スケジュールを作成する場合、装置は独立して一貫性を維持できます。
- **[モニタリング（Monitoring）]** > **[セッション（Sessions）]** ページからアクティブな Device Manager のユーザーセッションを表示したり、セッションを削除できます。

ハイ アベイラビリティのシステム要件

ここでは、ハイ アベイラビリティ設定に2台のデバイスを実装する前に満たさなくてはならない要件について説明します。

HA のハードウェア要件

高可用性設定で2つのデバイスを結び付けるには、次のハードウェア要件を満たす必要があります。

- デバイスはまったく同じハードウェア モデルである必要があります。

  Firepower 9300 の場合、ハイ アベイラビリティ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 がある場合、SM-36 モジュール間と SM-44 モジュール間に高可用性ペアを作成できます。

- デバイスは同じ数の同じタイプのインターフェイスを備えている必要があります。

  Firepower 4100/9300 シャーシの場合、HA を有効にする前に、すべてのインターフェイスを FXOS で同様に事前設定する必要があります。HA を有効にした後に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。

- デバイスには同じモジュールが取り付けられている必要があります。たとえば、一方にオプションのネットワーク インターフェイス モジュールがある場合は、もう一方のデバイスに同じモジュールを取り付ける必要があります。
- 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 Firepower 9300 シャーシで別の論理デバイス間の HA を設定することはできません。

HA のソフトウェア要件

高可用性設定で2つのデバイスを結び付けるには、次のソフトウェア要件を満たす必要があります。

- デバイスは、まったく同じバージョンのソフトウェア（つまり、1 番目のメジャー番号、2 番目のマイナー番号、および 3 番目のメンテナンス番号が同じ）を実行する必要があり

ます。バージョンは、Device Manager の [デバイス（Devices]） ページで確認できます。また、CLI で **show version** コマンドを使用して確認することもできます。異なるバージョンを実行するデバイスでも参加できますが、設定がスタンバイ装置にインポートされず、装置を同じソフトウェアバージョンにアップグレードしないとフェールオーバーは機能しません。

- 両方のデバイスがローカルマネージャモードになっている必要があります。つまり、Device Manager を使用して設定されている必要があります。両方のシステムで Device Manager にログインできる場合は、それらがローカルマネージャモードになっています。CLI で **show managers** コマンドを使用して確認することもできます。
- 各デバイスの初期セットアップ ウィザードを完了する必要があります。
- 各デバイスに固有の管理 IP アドレスが必要です。管理インターフェイスの設定は、デバイス間で同期されません。
- デバイスの NTP 設定が同じである必要があります。
- DHCP を使用してアドレスを取得するようにインターフェイスを設定することはできません。つまり、すべてのインターフェイスに静的 IP アドレスが必要です。
- クラウドサービスの場合は、両方のデバイスを同じリージョンに登録する必要があります。そうしないと、どちらのデバイスも登録できなくなります。複数のクラウドサービスの登録を組み合わせることはできません。
- ハイ アベイラビリティを設定する前に、保留中の変更を展開する必要があります。

HA のライセンス要件

高可用性を設定する前に、装置が同じ状態（両方とも Essentials ライセンスに登録されているか両方とも評価モードになっている）である必要があります。デバイスが登録されている場合は、それらを異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態（両方有効または両方無効）である必要があります。ただし、装置ごとに異なるオプション ライセンスを有効にすることは可能です。両方のユニットを登録する場合は、デバイスに対して同じシスコ クラウドサービスのリージョンを選択する必要があります。

デバイスが登録されている場合は、スマートライセンスまたはパーマネントライセンス予約（PLR）のいずれかと同じモードを使用する必要があります。

運用時には、ハイ アベイラビリティ ペアの装置に同じライセンスが必要です。アクティブ装置で行ったライセンスの変更は、展開時にスタンバイ装置で繰り返されます。

ハイ アベイラビリティ構成には、2 つのスマート ライセンス資格（ペアを構成するデバイスごとに 1 つ）が必要です。各デバイスに適用するためにアカウントに十分なライセンスがあることを確認する必要があります。ライセンスが不足している場合は、一方のデバイスが準拠状態でも、もう一方のデバイスが非準拠になる可能性があります。

たとえば、アクティブデバイスに Essentials ライセンスと IPS が割り当てられており、スタンバイデバイスに Essentials ライセンスのみが割り当てられている場合、スタンバイ装置は Cisco

Smart Software Manager と通信してアカウントから利用可能な IPS を取得します。スマート ライセンス アカウントに購入済みの十分な権限付与が含まれていない場合は、正しい数のライセンスが購入されるまで、アカウントがコンプライアンス適用外（そのため、アクティブ デバイスにコンプライアンスが適用されていてもスタンバイ デバイスはコンプライアンス適用外）になります。

（注） 輸出規制対象の機能の設定が異なるアカウントにデバイスを登録した場合、または1つの装置が登録済みで、もう 1 つが評価モードにある HA ペアを作成しようすると、HA の参加が失敗する可能性があります。輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワーク セグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置で HA を手動で中断する必要があります。

ハイ アベイラビリティのガイドライン

モデルのサポート

- Firepower 9300：Firepower 9300 で HA を設定することができます。ただし、同じ Firepower 9300 シャーシで別の論理デバイス間の HA を設定することはできません。
- Firepower 1010：
  - 高可用性を使用する場合は、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。高可用性は、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 高可用性 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、高可用性 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。
  - 高可用性ペアのシャーシの場合、スタンバイユニットの「アクティブ」LEDはオレンジ色です。
- （Firepower 1000 シリーズ、Firepower 2100）：デバイスが HA で展開されており、それらのデバイスで何百ものインターフェイスが設定されている場合、フェールオーバー時間の遅延（秒単位）が増加する可能性があります。

- Threat Defense Virtual：HA 設定は、Microsoft Azure クラウドまたは Amazon Web Services（AWS）クラウドの Threat Defense Virtual ではサポートされていません。

その他のガイドライン

- 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。
- アクティブ装置で展開ジョブを実行すると、アクティブ装置の設定がスタンバイ装置に同期されます。ただし、一部の変更は、変更を展開するまでスタンバイ装置で同期されなくても、保留中の変更に表示されません。次のいずれかを変更すると、変更は非表示になり、スタンバイ装置で設定する前に展開ジョブを実行する必要があります。変更をすぐに適用する必要がある場合は、保留中の変更に表示されている他の変更を行う必要があります。非表示となる変更には、ルール、ジオデータベース、セキュリティインテリジェンスまたはVDB更新のスケジュール、バックアップのスケジュール、NTP、管理接続用HTTPプロキシ、ライセンス権限付与、クラウドサービスオプション、URLフィルタリングオプションの編集が含まれます。
- プライマリ装置とセカンダリ装置の両方でバックアップを実行する必要があります。バックアップを復元するには、まず HA を解除する必要があります。両方のユニットで同じバックアップを復元しないでください（両方のユニットがアクティブになってしまうため）。代わりに、まず、アクティブにする装置でバックアップを復元し、その後に、別のユニットで同等のバックアップを復元してください。
- さまざまなアイデンティティソースの [テスト（Test）] ボタンは、アクティブ装置でのみ機能します。スタンバイデバイスのアイデンティティソース接続をテストする必要がある場合は、まず、モードを切り替えてスタンバイピアをアクティブピアにする必要があります。
- ハイアベイラビリティ設定を作成または解除すると、設定の変更が展開されたときに両方のデバイスで Snort 検査プロセスが再開されます。これにより、プロセスが完全に再開されるまでに通過トラフィックの中断が発生する可能性があります。
- ハイ アベイラビリティの初期設定時に、セカンダリ上のセキュリティ インテリジェンスおよび地理位置情報データベースのバージョンがプライマリ上のバージョンと異なる場合、データベースを更新するジョブはセカンダリ装置でスケジュールされます。これらのジョブは、次の展開時にアクティブ装置から実行されます。HA結合に失敗した場合でも、これらのジョブはそのまま残り、次の展開時に実行されます。
- 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。

- ハイ アベイラビリティ ペアに接続されているスイッチでポート 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上の問題が発生する可能性があります。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するときに、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るために発生します。
- アクティブ/スタンバイ ハイ アベイラビリティと VPN IPsec トンネルの場合、VPN トンネル経由でSNMPを使用してアクティブ装置とスタンバイ装置の両方をモニターすることはできません。スタンバイ装置にはアクティブ VPN トンネルがなく、ネットワーク管理システム（NMS）宛ての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。

ハイ アベイラビリティの設定

ハイアベイラビリティのセットアップを使用して、デバイスで障害が発生している場合でもネットワーク接続を確保します。アクティブ/スタンバイ ハイ アベイラビリティを使用して、2 台のデバイスがリンクされます。そのため、アクティブデバイスが故障した場合、スタンバイデバイスが引き継ぎ、ユーザーは接続の問題をほとんど感じません。

次の手順で、アクティブ/スタンバイ ハイ アベイラビリティ（HA）ペアをセットアップするエンドツーエンドプロセスについて説明します。

手順

ステップ 1 2 台の装置でのハイ アベイラビリティの準備 （248 ページ）。

ステップ 2 ハイ アベイラビリティ用のプライマリ装置の設定 （250 ページ）。

ステップ 3 ハイ アベイラビリティ用のセカンダリ装置の設定 （253 ページ）。

ステップ 4 ヘルスモニタリングのフェールオーバー基準の設定 （255 ページ）。

基準には、ピアモニタリングとインターフェイスモニタリングが含まれます。すべてのフェールオーバー基準にはデフォルト設定がありますが、デフォルト設定を調べて、それらがネットワークで機能していることを確認する必要があります。

- ピア装置のヘルス モニタリング フェールオーバー基準の設定 （255 ページ）。
- インターフェイスのヘルス モニタリング フェールオーバー基準の設定 （257 ページ）。

  インターフェイステストの詳細については、システムがインターフェイスヘルスをテストする方法 （259 ページ）を参照してください。

ステップ 5 （オプション。ただし推奨。）スタンバイ IP および MAC アドレスの設定 （260 ページ）。

ステップ 6 （任意）ハイ アベイラビリティ設定の確認 （262 ページ）。

2 台の装置でのハイ アベイラビリティの準備

高可用性を正常に設定するには、多くのことを事前に正しく準備する必要があります。

手順

ステップ 1 デバイスがHA のハードウェア要件 （243 ページ）に説明されている要件を満たしていることを確認します。

ステップ 2 単一のフェールオーバー リンクを使用するのか、別のフェールオーバー リンクとステートフル フェールオーバー リンクを使用するのかを決め、使用するポートを特定します。

各リンクのそれぞれのデバイスで同じポート番号を使用する必要があります。たとえば、フェールオーバー リンクの場合は両方のデバイスで GigabitEthernet 1/3 を使用します。使用する内容を把握しておくことで、誤ってその他の目的で使用することがなくなります。詳細については、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 （236 ページ）を参照してください。

ステップ 3 デバイスをインストールしてネットワークに接続し、各デバイスで初期セットアップ ウィザードを完了します。

a) フェールオーバー リンクとデータ リンクの中断の回避 （238 ページ）で推奨のネットワーク設計を確認します。

b) インターフェイスの接続 （12 ページ）の説明に従い、少なくとも外部インターフェイスだけは接続します。

その他のインターフェイスも接続できますが、特定のサブネットへの接続には各デバイスで同じポートを使用する必要があります。各デバイスでは同じ設定が共有されるため、デバイスは同じ方法でネットワークに接続する必要があります。

（注） セットアップ ウィザードでは、管理インターフェイスと内部インターフェイスの IP アドレスを変更できません。そのため、プライマリ デバイス上のそれらのインターフェイスのいずれかをネットワークに接続する場合、セカンダリ デバイスのインターフェイスは接続しないでください。接続すると IP アドレスの競合が発生します。ワークステーションをそれらのインターフェイスのいずれかに直接接続し、DHCP を介してアドレスを取得できるため、Device Manager に接続して、デバイスを設定できます。

c) 各デバイスで初期セットアップ ウィザードを完了します。外部インターフェイスの静的IP アドレスを指定していることを確認します。さらに、同じNTP サーバを設定します。詳細については、セットアップウィザードを使用した初期設定の完了 （24 ページ）を参照してください。

各装置で同じライセンスと Cisco Success Network オプションを選択します。たとえば、それぞれに評価モードを選択したり、デバイスを登録したりします。

d) セカンダリ デバイスで、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** を選択して一意の IP アドレスを設定し、必要に応じてゲートウェイを変更します。また、ニーズに合わせて DHCP サーバの設定を無効化または変更します。

e) セカンダリ デバイスで、**[デバイス（Device）]** > **[インターフェイス（Interface）]** を選択し、内部インターフェイスを編集します。IP アドレスを削除するか、または変更します。また、同じネットワーク上に 2 つの DHCP サーバは定義できないため、インターフェイスに定義されている DHCP サーバを削除します。

f) 設定をセカンダリ デバイスに展開します。

g) ネットワーク トポロジに基づいて必要な場合は、プライマリ デバイスにログインして、管理アドレス、ゲートウェイ、DHCP サーバの設定、および内部インターフェイスの IP アドレスを変更します。変更を加えた場合は、設定を展開します。

h) 内部インターフェイス、または管理インターフェイス（別の管理ネットワークを使用する場合）を接続していない場合は、ここでそれらのインターフェイスをスイッチに接続できます。

ステップ 4 デバイスのソフトウェア バージョンが完全に同じである（つまり、同じメジャー（1 番）、マイナー（2 番）、メンテナンス（3 番）の番号が付いている）ことを確認します。バージョンは、Device Manager の [デバイス（Devices）] ページで確認できます。また、CLI で **show version** コマンドを使用して確認することもできます。

同じソフトウェア バージョンが実行されていない場合は、Cisco.com から推奨のソフトウェア バージョンを取得して、各デバイスにインストールします。詳細は、のアップグレードThreat Defense （976 ページ）を参照してください。

ステップ 5 接続して、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 リンクを設定します。

a) （フェールオーバー リンクとデータ リンクの中断の回避（238 ページ）で選択した）推奨のネットワーク設計に従い、適切に各デバイスのフェールオーバーインターフェイスをスイッチに接続するか、デバイス間で直接接続します。

b) 別のステートリンクを使用している場合は、各デバイスのステートフルフェールオーバーインターフェイスも適切に接続します。

c) 次に各デバイスにログインして、**[デバイス（Device）]** > **[インターフェイス（Interface）]** にアクセスします。各インターフェイスを編集し、インターフェイス名や IP アドレスが設定されていないことを確認します。

名前付きのインターフェイスが設定されている場合、その名前を削除する前に、セキュリティ ゾーンからそれらのインターフェイスを削除して、その他の設定を削除する必要がある場合があります。名前の削除に失敗した場合は、エラー メッセージを調べて、加える必要があるその他の変更を確認します。

ステップ 6 プライマリ デバイスで、残りのデータ インターフェイスを接続してデバイスを設定します。

a) **[デバイス（Device）]** > **[インターフェイス（Interface）]** を選択し、トラフィックの通過に使用される各インターフェイスを編集し、プライマリ静的 IP アドレスを設定します。

b) セキュリティ ゾーンにインターフェイスを追加し、接続されたネットワーク上のトラフィックの処理に必要な基本的なポリシーを設定します。設定例については、ベストプラクティ

ス：Threat Defense の使用例 （49 ページ）にリストされているトピックを参照してください。

c) 設定を展開します。

ステップ 7 HA のソフトウェア要件 （243 ページ）で説明されているすべての要件を満たしていることを確認します。

ステップ 8 一貫性のあるライセンス（登録済みまたは評価モード）を保有していることを確認します。詳細については、HA のライセンス要件 （244 ページ）を参照してください。

ステップ 9 セカンダリ デバイスで、残りのデータ インターフェイスをプライマリ デバイスの同等のインターフェイスと同じネットワークに接続します。インターフェイスは設定しないでください。

ステップ 10 各デバイスで **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** を選択し、設定が同じであることを確認します。

これで、プライマリ デバイスでハイ アベイラビリティを設定する準備が整いました。

ハイ アベイラビリティ用のプライマリ装置の設定

アクティブ/スタンバイ ハイ アベイラビリティ ペアをセットアップするには、まず、プライマリデバイスを設定する必要があります。プライマリ デバイスは、通常の状況下でアクティブにする予定の装置です。セカンダリ デバイスは、プライマリ装置が使用できなくなるまでスタンバイ モードのままです。

プライマリにするデバイスを選択し、そのデバイス上の Device Manager にログインして次の手順に従います。

（注） いったんハイアベイラビリティペアを確立すると、この手順で説明する設定を編集するにはペアを破棄する必要があります。

始める前に

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 リンク用に設定するインターフェイスに名前が付いていないことを確認します。名前が付いている場合は、セキュリティゾーンオブジェクトを含め、それらを使用するポリシーからインターフェイスを削除してインターフェイスを編集し、名前を削除する必要があります。また、インターフェイスはパッシブモードではなくルーテッドモードにする必要もあります。これらのインターフェイスは、HA 設定での使用専用にする必要があります。他のプロセスに使用することはできません。

保留中の変更がある場合は、それらを展開してから HA を設定する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側で、[ハイアベイラビリティ（High Availability）] グループの横にある [設定（Configure）] をクリックします。

デバイスで初めて HA を設定する場合、グループは次のように表示されます。

ステップ 3 [ハイアベイラビリティ（High Availability）] ページで、[プライマリデバイス（Primary Device）] ボックスをクリックします。

セカンダリデバイスがすでに設定されていて、その設定をクリップボードにコピーした場合は、[クリップボードから貼り付け（Paste from Clipboard）] ボタンをクリックすると設定を貼り付けることができます。これにより、適切な値でフィールドが更新され、後で確認できます。

ステップ 4 [フェールオーバーリンク（Failover Link）] プロパティを設定します。

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、設定の変更を同期します。詳細については、フェールオーバー リンク （236 ページ）を参照してください。

- [物理インターフェイス（Physical Interface）] フェールオーバーリンクとして使用するセカンダリデバイスに接続したインターフェイスを選択します。名前が付いていないインターフェイスにする必要があります。

  フェールオーバーまたはステートリンクとして EtherChannel インターフェイスを使用している場合、高可用性を確立する前に、両方のデバイスで同じ ID とメンバー インターフェイスを備えた同じ EtherChannel が存在していることを確認する必要があります。EtherChannel の不一致がある場合は、HA を無効にして、セカンダリユニットの設定を修正する必要があります。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。

- [タイプ（Type）]：インターフェイスに IPv4 アドレスまたは IPv6 アドレスを使用するかどうか選択します。設定できるアドレスタイプは 1 つのみです。

- [プライマリ IP（Primary IP）]：このデバイス上のインターフェイスの IP アドレスを入力します。たとえば、192.168.10.1 と入力します。IPv6 アドレスの場合、標準表記にプレフィックス長を含める必要があります（2001:a0a:b00::a0a:b70/64 など）。

- [セカンダリ IP（Secondary IP）]：セカンダリ デバイス上のインターフェイスについて、リンクのもう一方の端に設定する必要がある IP アドレスを入力します。このアドレスはプライマリアドレスと同じサブネット上に存在し、プライマリアドレスとは異なるアドレスである必要があります（192.168.10.2 または 2001:a0a:b00::a0a:b71/64 など）。

- [ネットマスク（Netmask）]（IPv4 のみ）：プライマリ/セカンダリ IP アドレスのサブネット マスクを入力します。

ステップ 5 [ステートフル フェールオーバー リンク（Stateful Failover Link）] プロパティを設定します。

システムは、ステートリンクを使用して接続状態の情報をスタンバイデバイスに渡します。この情報は、フェールオーバーが発生したときにスタンバイ装置が既存の接続を維持するために役立ちます。フェールオーバーリンクと同じリンクを使用するか、別のリンクを設定することができます。

- [フェールオーバーリンクと同じインターフェイスを使用する（Use the Same Interface as the Failover Link）]：フェールオーバー通信およびステートフル フェールオーバー通信に単一のリンクを使用する場合は、このオプションを選択します。このオプションを選択する場合は、次の手順に進みます。
- [物理インターフェイス（Physical Interface）]：別のステートフル フェールオーバー リンクを使用する場合は、ステートフル フェールオーバー リンクとして使用するセカンダリ デバイスに接続したインターフェイスを選択します。名前が付いていないインターフェイスにする必要があります。次のプロパティを設定します。
  - [タイプ（Type）]：インターフェイスに IPv4 アドレスまたは IPv6 アドレスを使用するかどうか選択します。設定できるアドレスタイプは 1 つのみです。
  - [プライマリIP（Primary IP）]：このデバイス上のインターフェイスの IP アドレスを入力します。アドレスは、フェールオーバー リンクに使用されるものとは別のサブネット上にある必要があります。たとえば、192.168.11.1 と入力します。IPv6 アドレスの場合、標準表記にプレフィックス長を含める必要があります（2001:a0a:b00:a::a0a:b70/64 など）。
  - [セカンダリIP（Secondary IP）]：セカンダリ デバイス上のインターフェイスについて、リンクのもう一方の端に設定する必要がある IP アドレスを入力します。このアドレスはプライマリアドレスと同じサブネット上に存在し、プライマリアドレスとは異なるアドレスである必要があります（192.168.11.2 または 2001:a0a:b00:a::a0a:b71/64 など）。
  - [ネットマスク（Netmask）]（IPv4 のみ）：プライマリ/セカンダリ IP アドレスのサブネット マスクを入力します。

ステップ 6 （オプション）ペアの 2 台の装置間での通信を暗号化する場合は、[IPsec暗号キー（IPsec Encryption Key）] 文字列を入力します。

セカンダリノードでまったく同じキーを設定する必要があるため、入力した文字列をメモしてください。

キーを入力しなければ、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 リンクでのすべての通信はプレーンテキストで実行されます。インターフェイス間をケーブルで直接接続していない場合、これによってセキュリティの問題が発生することがあります。

（注） 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。

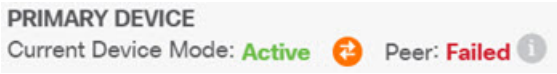
ステップ7 [HAの有効化（Activate HA）] をクリックします。

システムは、すぐにデバイスに設定を展開します。展開ジョブを開始する必要はありません。設定が保存され、展開が進行中であるというメッセージが表示されない場合は、ページ上部にスクロールして、エラーメッセージを確認します。

設定はクリップボードにもコピーされます。コピーを使用すると、簡単にセカンダリ装置を設定できます。セキュリティを強化するため、暗号キーはクリップボードのコピーには含まれません。

設定が完了すると、実行する必要がある次の手順を説明するメッセージが表示されます。情報を確認したら、[了解（Got It）] をクリックします。

この時点で、[ハイアベイラビリティ（High Availability）] ページが表示され、デバイスステータスが [ネゴシエーション中（Negotiating）] になっている必要があります。ステータスはピアの設定前でも [アクティブ（Active）] に変わります。設定するまで [故障（Failed）] と表示されます。



これで、セカンダリ装置を設定できるようになりました。ハイ アベイラビリティ用のセカンダリ装置の設定 （253 ページ） を参照してください。

（注） 選択したインターフェイスは直接設定されません。ただし、CLIに **show interface** と入力すると、インターフェイスが特定のIPアドレスを使用していることが表示されます。インターフェイスには「failover-link」という名前が付いています。別のステート リンクを設定する場合は「stateful-failover-link」になります。

ハイ アベイラビリティ用のセカンダリ装置の設定

プライマリデバイスをアクティブ/スタンバイ ハイ アベイラビリティ向けに設定した後、セカンダリデバイスを設定する必要があります。そのデバイス上の Device Manager にログインして、次の手順に従います。

（注） まだそのように設定していない場合は、プライマリデバイスからクリップボードにハイアベイラビリティ設定をコピーします。手動でデータを入力するより、コピーと貼り付けを使用してセカンダリデバイスを設定するほうがはるかに簡単です。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側で、[ハイアベイラビリティ（High Availability）] グループの横にある [設定（Configure）] をクリックします。

デバイスで初めて HA を設定する場合、グループは次のように表示されます。

ステップ 3 [ハイアベイラビリティ（High Availability）] ページで、[セカンダリデバイス（Secondary Device）] ボックスをクリックします。

ステップ 4 次のいずれかを実行します。

- [簡単な方法（Easy method）] : [クリップボードから貼り付け（Paste from Clipboard）] ボタンをクリックして設定に貼り付け、[OK] をクリックします。これにより、適切な値でフィールドが更新され、後で確認できます。
- [手動の方法（Manual method）] : 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 リンクを直接設定します。プライマリデバイスに入力したのとまったく同じ設定をセカンダリデバイスに入力します。

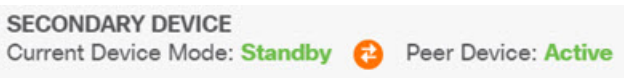
ステップ 5 プライマリデバイスで [IPSec暗号キー（IPSec Encryption Key）] を設定した場合、まったく同じキーをセカンダリデバイスに入力します。

ステップ 6 [HA の有効化（Activate HA）] をクリックします。

システムは、すぐにデバイスに設定を展開します。展開ジョブを開始する必要はありません。設定が保存され、展開が進行中であるというメッセージが表示されない場合は、ページ上部にスクロールして、エラーメッセージを確認します。

設定が完了すると、HA が設定されたことを示すメッセージが表示されます。[了解（Got It）] をクリックして、メッセージを閉じます。

この時点で、[ハイアベイラビリティ（High Availability）] ページが表示され、デバイスステータスにこれがセカンダリデバイスであることが示されている必要があります。プライマリデバイスとの結合が成功した場合、デバイスはプライマリと同期して、最終的にはスタンバイモードになります。ピアがアクティブになります。



（注） 選択したインターフェイスは直接設定されません。ただし、CLI に **show interface** と入力すると、インターフェイスが特定の IP アドレスを使用していることが表示されます。インターフェイスには「failover-link」という名前が付いています。別のステート リンクを設定する場合は「stateful-failover-link」になります。

ヘルスモニタリングのフェールオーバー基準の設定

ハイアベイラビリティ設定の装置は、全体的な健全性とインターフェイスの健全性をモニターします。

フェールオーバー基準により、ピアに障害が発生したかどうかを判断するヘルスモニタリングメトリックが定義されます。アクティブピアが基準に違反した装置である場合、スタンバイ装置へのフェールオーバーがトリガーされます。スタンバイピアが基準に違反した装置である場合、スタンバイピアは障害が発生した装置としてマークされ、フェールオーバーに使用できなくなります。

アクティブデバイスでのみフェールオーバー基準を設定できます。

次の表に、フェールオーバー トリガー イベントと、関連する障害検出のタイミングを示します。

表 *5*: フェールオーバー基準に基づくフェールオーバー時間

フェールオーバー トリガー イベント	最小	デフォルト	最大数
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ装置のインターフェイスの物理リンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ装置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

ここでは、フェールオーバー ヘルス モニタリング基準をカスタマイズする方法と、システムがインターフェイスをテストする方法について説明します。

ピア装置のヘルス モニタリング フェールオーバー基準の設定

ハイアベイラビリティ設定の各ピアは、helloメッセージを使用してフェールオーバーリンクをモニターすることによって相手装置の状態を判断します。装置が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い場合、装置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にLANTESTメッセージを送信し、ピアが応答するかどうか検証します。デバイスが行うアクションは、相手装置からの応答によって異なります。

- デバイスがフェールオーバーリンクで応答を受信した場合は、フェールオーバーを行いません。
- デバイス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。
- デバイス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。

hello メッセージのポーリング時間および保留時間を設定できます。

手順

ステップ 1 アクティブデバイスで、[デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

フェールオーバー条件は、[ハイアベイラビリティ（High Availability）] ページの右側の列に表示されます。

ステップ 3 [ピアのタイミング設定（Peer Timing Configuration）] を定義します。

これらの設定では、アクティブデバイスがスタンバイデバイスにフェールオーバーできる早さを決定します。ポーリング間隔が短いほど、デバイスは短時間で障害を検出し、フェールオーバーをトリガーできます。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。ほとんどの場合、デフォルト設定が適切です。

1 回のポーリング期間中に装置がフェールオーバー インターフェイスで hello パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

- [ポーリング時間（Poll Time）] : hello メッセージ間の間隔。1 ～ 15 秒または 200 ～ 999 ミリ秒を入力します。デフォルト値は 1 秒です。
- [保留時間（Hold Time）] : 装置が、フェールオーバー リンクで hello メッセージを受信する間隔。この時間を経過すると、ピア装置で障害が発生したと見なされます。保留時間は、ポーリング時間の 3 倍以上にする必要があります。1 ～ 45 秒または 800 ～ 999 ミリ秒を入力します。デフォルトは 15 秒です。

ステップ 4 [保存（Save）] をクリックします。

インターフェイスのヘルス モニタリング フェールオーバー基準の設定

デバイスモデルに応じて、最大211のインターフェイスをモニターできます。重要なインターフェイスをモニタする必要があります。たとえば、重要なネットワーク間のスループットを保証するインターフェイスなどです。スタンバイ IP アドレスを設定する場合、さらにインターフェイスを常にアップ状態にする必要がある場合にのみインターフェイスをモニタします。

装置が、2回のポーリング期間中にモニター対象のインターフェイス上でhelloメッセージを受信しない場合、インターフェイステストを実行します。1つのインターフェイスに対するすべてのインターフェイステストがすべて失敗したが、相手装置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、そのインターフェイスは故障していると見なされます。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われます。相手装置のインターフェイスもすべてのネットワークテストに失敗した場合、両方のインターフェイスが「Unknown」状態になり、フェールオーバー制限に向けてのカウントは行いません。

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。故障したデバイスは、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。

show monitor-interface コマンドを使用して、CLI または CLI コンソールからインターフェイスの HA ステータスをモニターできます。詳細については、HA モニター対象インターフェイスのステータスのモニタリング （278 ページ）を参照してください。

（注） インターフェイスの1つがダウンした場合、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスがダウンしていることを装置が検出すると、インターフェイスの保留時間を待たずにすぐにフェールオーバーが発生します（1インターフェイスのデフォルトしきい値を維持している場合）。インターフェイスの保留時間が有効であるのは、装置が自身のステータスを OK と見なしているときだけです（ピアから hello パケットを受信していなくても）。

始める前に

デフォルトでは、すべての名前付き物理インターフェイスが HA モニタリングに選択されています。したがって、重要ではない物理インターフェイスのモニタリングを無効にする必要があります。サブインターフェイスまたはブリッジグループでは、手動でモニタリングを有効にする必要があります。

インターフェイス モニタリングを完全に無効にしてインターフェイスの故障によるフェールオーバーを防止するには、単純に、HA モニタリングが有効になっているインターフェイスがないことを確認します。

手順

ステップ 1 アクティブデバイスで、[デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

フェールオーバー条件は、[ハイアベイラビリティ（High Availability）] ページの右側の列に表示されます。

ステップ 3 [インターフェイス障害しきい値（Interface Failure Threshold）] を定義します。

故障したインターフェイスの数がしきい値を満たすと、装置は自身を故障としてマークします。装置がアクティブ装置の場合、スタンバイ装置にフェールオーバーします。装置がスタンバイ装置の場合、自身を故障としてマークすることによって、アクティブ装置はその装置をフェールオーバーに利用できると見なさなくなります。

この条件を設定する場合、モニターするインターフェイスの数を考慮します。たとえば、2 つのインターフェイスでのみモニタリングを有効ににすると、10 個のインターフェイスのしきい値に到達することはありません。インターフェイスのプロパティを編集するときに [詳細オプション（Advanced Options）] タブの [HAモニタリングの有効化（Enable for HA Monitoring）] オプションを選択することで、インターフェイスのモニタリングを設定します。

デフォルトでは、1 つのモニター対象インターフェイスが故障すると、装置は自身を故障としてマークします。

次の [フェールオーバー条件（Failover Criteria）] オプションのいずれかを選択して、インターフェイス障害のしきい値を設定できます。

- [故障したインターフェイスの数を超える（Number of failed interfaces exceeds）]：インターフェイスの生の数字を入力します。デフォルトは 1 です。実際には、最大値はデバイスモデルに依存して変わりますが、211 以上を入力することはできません。この条件を使用すると、デバイスサポートよりも大きい数を入力すると展開エラーが発生します。より小さい数を試すか、代わりにパーセンテージを使用します。
- [故障インターフェイスのパーセンテージを超える（Percentage of failed interfaces exceeds）]：1 ～ 100 の数値を入力します。たとえば、50% と入力して 10 個のインターフェイスをモニターする場合、5 個のインターフェイスが故障するとデバイスは自身を故障としてマークします。

ステップ 4 [インターフェイスタイミング設定（Interface Timing Configuration）] を定義します。

これらの設定では、インターフェイスで障害が発生したかどうかをアクティブデバイスが判断できる早さを決定します。ポーリング間隔が短いほど、デバイスは短時間でインターフェイス障害を検出できます。ただし、検出が早いほど、実際には健全な状態でもビジー状態のインターフェイスが障害発生とマークされ、必要以上に頻繁にフェールオーバーが生じる可能性があります。ほとんどの場合、デフォルト設定が適切です。

インターフェイスリンクがダウンしていると、インターフェイスのテストは実行されません。また、故障したインターフェイスの数が設定されたインターフェイスフェールオーバーしきい値に合致するかまたはそれを超過すると、スタンバイ装置は 1 回のインターフェイスポーリング期間でアクティブになります。

- [ポーリング時間（Poll Time）]：hello パケットがデータ インターフェイスで送信される頻度。1 ～ 15 秒または 500 ～ 999 ミリ秒を入力します。デフォルトは 5 秒です。

- [保留時間（Hold Time）]：保留時間によって、helloパケットを受信できなかったときからインターフェイスが故障とマークされるまでの時間が決まります。5 ～ 75 秒を入力します。ポーリング時間の 5 倍に満たない保持時間は入力できません。

ステップ 5 [Save] をクリックします。

ステップ 6 モニターする各インターフェイスの HA モニタリングを有効にします。

a) **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** を選択します。

インターフェイスをモニターしている場合、[HAのモニター（Monitor for HA）]列は [有効（Enabled）] になります。

b) モニタリングステータスを変更するインターフェイスの編集アイコン（）をクリックします。

フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスは編集できません。インターフェイス モニタリングはそれらに適用されません。

c) [詳細オプション（Advanced Options）] タブをクリックします。

d) 必要に応じて、[HAモニタリングの有効化（Enable for HA Monitoring）] チェックボックスを選択または選択解除します。

e) [OK] をクリック

ステップ 7 （オプション。ただし推奨。）モニタ対象インターフェイスのスタンバイ IP アドレスおよび MAC アドレスを設定します。スタンバイ IP および MAC アドレスの設定 （260 ページ） を参照してください。

システムがインターフェイスヘルスをテストする方法

システムは、ユーザーがハイ アベイラビリティ ヘルスをモニターしているインターフェイスを継続的にテストします。インターフェイスのテストに使用されるアドレスは、ユーザーが設定するアドレスタイプに基づきます。

- インターフェイスに IPv4 アドレスと IPv6 アドレスの両方が設定されている場合、デバイスは IPv4 アドレスを使用してヘルスモニタ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、デバイスは ARP ではなく IPv6 ネイバー探索を使用してヘルスモニタ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、デバイスは IPv6 全ノードアドレス（FE02::1）を使用します。

システムは、各装置で次のテストを実行します。

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、装置はそれに障害が発生していると見なします。ステータスがアップの場合は、装置がネットワーク アクティビティ テストを実行します。
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。このテストの目的は、LANTEST メッセージを使用してネットワーク トラフィックを生成

し、障害が発生しているユニット（いずれか 1 つ）を特定することです。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。ユニットがテスト中にパケットを受信したらすぐに（最大 5 秒）、そのインターフェイスは動作可能と見なされます。いずれか一方の装置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なかった装置が故障していると見なされます。いずれの装置もトラフィックを受信しなかった場合、装置は ARP テストを開始します。

3. ARPテスト：取得したエントリの最後の2つの装置ARPキャッシュの読み取り。装置は、ネットワークトラフィックを発生させるために、1 回に 1 つずつ、これらのデバイスに ARP 要求を送信します。各要求後、装置は最大 5 秒間受信したトラフィックをすべてカウントします。トラフィックが受信されれば、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。トラフィックが受信されなければ、ARP 要求が次のデバイスに送信されます。リストの最後まで来てもトラフィックが受信されない場合は、ping テストが実行されます。

4. ブロードキャスト ping テスト：このテストでは、ブロードキャスト ping 要求が送信されます。装置は、最大 5 秒間、すべての受信パケット数をカウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなければ、ARPテストからやり直します。

スタンバイ IP および MAC アドレスの設定

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。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。

1. プライマリ装置に障害が発生すると、セカンダリ装置はプライマリ ユニットの 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。

2. 現在スタンバイになっている装置が、スタンバイの 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。

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。しかし、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 アドレスは手動で設定できます。

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。Threat Defense デバイス 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。

手順

ステップ 1 **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** を選択します。

少なくとも、HA をモニターしているインターフェイスのスタンバイ IP アドレスと MAC アドレスを設定する必要があります。インターフェイスをモニターしている場合、[HAのモニター（Monitor for HA）] 列は [有効（Enabled）] になります。

ステップ 2 スタンバイアドレスを設定するインターフェイスの編集アイコン（  ）をクリックします。

フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスは編集できません。ハイアベイラビリティを設定する場合、これらのインターフェイスの IP アドレスを設定します。

ステップ 3 [IPv4アドレス（IPv4 Address）] タブおよび [IPv6アドレス（IPv6 Address）] タブでスタンバイ IP アドレスを設定します。

スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。使用している IP バージョンごとにスタンバイアドレスを設定します。

ステップ 4 [詳細オプション（Advance Options）] タブをクリックして、MAC アドレスを設定します。

デフォルトでは、システムはインターフェイスのネットワークインターフェイス カード（NIC）に焼き込まれた MAC アドレスを使用します。したがって、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 MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MACアドレス（MAC Address）]：H.H.H 形式の Media Access Control アドレス。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。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。
- [スタンバイMACアドレス（Standby MAC Address）]：高可用性で使用します。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 5 [OK] をクリックします。

ハイ アベイラビリティ設定の確認

ハイ アベイラビリティの設定が完了したら、両方のデバイスが「動作中」でアクティブ/スタンバイ モードであることが、デバイスのステータスに示されていることを確認します。

次の手順を使用して、ハイ アベイラビリティの設定が機能していることを確認できます。

手順

ステップ 1 FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

設定済みの各インターフェイスに接続されている、少なくとも 1 つのワークステーションからシステムへの接続をテストします。

ステップ 2 次のいずれかを実行して、モードを切り替え、アクティブ装置をスタンバイ装置にします。

- Device Manager で、**[デバイス（Device）]** > **[ハイアベイラビリティ（High Availability）]** ページの歯車メニューから [モードの切り替え（Switch Mode）] を選択します。
- アクティブ装置の CLI で、**no failover active** を入力します。

ステップ 3 接続テストを繰り返して、ハイ アベイラビリティ ペア内のその他の装置からも同じ接続を確立できることを確認します。

テストが失敗する場合は、他の装置の同等インターフェイスと同じネットワークにその装置のインターフェイスを接続していることを確認します。

HA ステータスは [ハイアベイラビリティ（High Availability）] ページから確認できます。CLI または装置の CLI コンソールを使用し、**show failover** コマンドを入力して、フェールオーバー ステータスを確認することもできます。また、**show interface** コマンドを使用して、失敗した接続テストで使用されたインターフェイスのインターフェイス設定を確認できます。

これらの操作で問題を特定できない場合は、他の手順を実行することができます。ハイ アベイラビリティ（フェールオーバー）のトラブルシューティング（280 ページ）を参照してください。

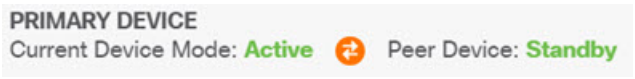
ステップ 4 完了したら、モードを切り替えて、元々アクティブだった装置をアクティブ ステータスに戻します。

ハイ アベイラビリティの管理

ハイ アベイラビリティ ペアを管理するには、[デバイス概要（Device Summary）] ページの [ハイアベイラビリティ（High Availability）] リンクをクリックします。

[ハイアベイラビリティ（High Availability）] ページには次のものがあります。

- [ロールおよびモードステータス（Role and Mode Status）]：左側のステータスエリアには、デバイスがグループ内のプライマリ デバイスかセカンダリ デバイスかが示されます。モードには、このデバイスがアクティブかスタンバイかや、HA が一時停止されているかデバイスがピアデバイスの参加を待っているかが示されます。また、ピアデバイスのステータス（アクティブ、スタンバイ、一時停止、または障害）も示されます。たとえば、現在ログインしているデバイスがプライマリデバイスであり、アクティブデバイスでもある場合、セカンダリデバイスが正常で、必要に応じてフェールオーバーできる状態であれば、ステータスは次のように表示されます。ピアの間のアイコンをクリックすると、デバイス間の設定同期ステータスに関する情報を取得できます。

- [直近の失敗理由（Last Failure Reason）]：高可用性（HA）の設定が何らかの理由で失敗した場合（アクティブデバイスが使用不可になり、スタンバイデバイスにフェールオーバーするなど）、直近の失敗の理由がロールとモードのステータスの下に表示されます。このメッセージは、フェールオーバー履歴から取得されます。
- [フェールオーバー履歴（Failover History）] リンク：このリンクをクリックすると、ペアに含まれるデバイスのステータスの詳細な履歴を確認できます。CLI コンソールが開き、**show failover history details** コマンドが実行されます。
- [展開履歴（Deployment History）] リンク：このリンクをクリックすると、イベントがフィルタリングされて展開ジョブだけが表示された監査ログに移動します。
- 歯車ボタン：このボタンをクリックすると、デバイス上でアクションが実行されます。
  - [HAの一時停止（Suspend HA）]/[HAの再開（Resume HA）]：HA を一時停止すると、HA 設定を削除しなくても、デバイスがハイアベイラビリティ ペアとして機能しなくなります。その後、デバイスで HA を再開（つまり再有効化）することができます。詳細は、ハイ アベイラビリティの中断または再開 （264 ページ）を参照してください。

- [HAの解除（Break HA）]：HA を解除すると、両方のデバイスからハイ アベイラビリティ設定が削除され、それらがスタンドアロン デバイスに戻ります。詳細は、ハイ アベイラビリティの破棄 （266 ページ）を参照してください。
- [モードの切り替え（Switch Mode）]：モードを切り替えることにより、アクションを実行するデバイスに応じて、強制的にアクティブデバイスをスタンバイにしたりスタンバイデバイスをアクティブにすることができます。詳細は、アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー） （267 ページ）を参照してください。

- [ハイアベイラビリティ設定（High Availability Configuration）]：このパネルには、フェールオーバー ペアの設定が表示されます。[クリップボードにコピー（Copy to Clipboard）] ボタンをクリックすると情報をクリップボードにロードできます。そこから、セカンダリ デバイスの設定に貼り付けることができます。情報を記録するために別のファイルにコピーすることもできます。この情報には、IPsec 暗号キーを定義したかどうかは示されません。

（注） HA のインターフェイス設定は、インターフェイスのページ（**[デバイス（Device）]>[インターフェイス（Interfaces）]**）に反映されません。HA 設定で使用しているインターフェイスは編集できません。

- [フェールオーバー基準（Failover Criteria）]：このパネルには、「アクティブ装置に障害が発生したためにスタンバイ装置がアクティブ装置になる必要がある」かどうかを評価する際に使用される健全性の基準を決定する設定が含まれます。これらの基準を調整して、ネットワークで必要なフェールオーバーパフォーマンスを実現してください。詳細は、ヘルスモニタリングのフェールオーバー基準の設定 （255 ページ）を参照してください。

ここでは、ハイ アベイラビリティ設定に関連するさまざまな管理タスクについて説明します。

ハイ アベイラビリティの中断または再開

ハイ アベイラビリティ ペアの 1 つのユニットを中断できます。これは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイ ユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。
- スタンバイデバイスのソフトウェアアップグレードをインストール中のフェールオーバーを防ぎたい場合。

ハイ アベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイ アベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムで HA を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバー ペアとして再び機能します。

アクティブ装置からハイ アベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。

ユニットが中断状態の場合にのみ、ユニットを再開できます。ユニットは、ピア ユニットとアクティブ/スタンバイ ステータスをネゴシエートします。

（注） 必要に応じて、CLI から **configure high-availability suspend** コマンドを入力して HA を中断できます。HA を再開するには、**configure high-availability resume** を入力します。

始める前に

Device Manager を使用してハイアベイラビリティを中断した場合、装置をリロードした場合でも、再開するまで中断のままになります。ただし、CLI を使用して中断した場合は一時的な状態なので、リロード時に装置のハイ アベイラビリティの設定が自動的に再開され、ピアとアクティブ/スタンバイ状態がネゴシエートされます。

スタンバイ装置のハイ アベイラビリティを中断する場合は、展開ジョブがアクティブな装置で実行中かどうかを確認してください。展開ジョブの進行中にモードを切り替えると、ジョブが失敗し、設定の変更は失われます。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

ステップ 3 歯車アイコン（⚙）から適切なコマンドを選択します。

- [HAの中断（Suspend HA）]：アクションの確認を求められます。メッセージを読んで、[OK] をクリックします。HA ステータスにデバイスが中断モードであることが表示されます。

- [HAの再開（Resume HA）]：アクションの確認を求められます。メッセージを読んで、[OK]をクリックします。HAステータスは、装置がピアとネゴシエートした後に正常（アクティブまたはスタンバイ）に戻ります。

ハイ アベイラビリティの破棄

2台のデバイスをハイ アベイラビリティ ペアとして稼働させない場合は、HA設定を破棄できます。HAを破棄すると、各デバイスはスタンドアロンデバイスになります。これらの設定は、次のように変更されます。

- アクティブデバイスは破棄される前と変わらずすべての設定を維持し、HA設定が削除されます。
- スタンバイデバイスではHA設定だけでなくすべてのインターフェイス設定が削除されます。すべての物理インターフェイスは無効になりますが、サブインターフェイスは無効になりません。管理インターフェイスはアクティブなままであるため、デバイスにログインして再設定することができます。

（注） または、（APIエクスプローラから）BreakHAStatus APIリソースを使用し、**interfaceOption**属性を使用して、スタンバイIPアドレスを使用してスタンバイデバイスのインターフェイスを再設定するようシステムに指示することもできます。この結果が必要な場合は、APIを使用する必要があります。Device Manager は常にインターフェイスを無効にします。システムはIPアドレスを再設定しますが、そうでない場合にはすべてのインターフェイスオプションが再設定されないため、中断後に変更が展開されるまでトラフィックが期待どおりに動作しない可能性があることに注意してください。

破棄が装置にどのように影響するのかは、破棄を実行するときの各装置の状態によって変わります。

- 装置が健全なアクティブ/スタンバイ状態である場合、アクティブ装置からHAを破棄します。これにより、HAペアの両方のデバイスからHA設定が削除されます。スタンバイ装置でのみHAを破棄する場合は、スタンバイ装置にログインしてHAを中断した後にHAを破棄できます。
- スタンバイ装置が中断状態または障害状態になっている場合、アクティブ装置からHAを破棄するとアクティブ装置からのみHA設定が削除されます。スタンバイ装置にログインして、スタンバイ装置のHAも破棄する必要があります。
- ピアがHAをネゴシエーションしていたり設定を同期している場合、HAを破棄することはできません。ネゴシエーションまたは同期が完了するか、タイムアウトになるまで待ち

ます。システムがこの状態でスタックしていると思われる場合は、HAを中断してからHAを破棄することができます。

（注） Device Manager を使用する場合、**configure high-availability disable** コマンドを使用して CLI から HA を破棄することはできません。

始める前に

理想的な結果を得るために、デバイスを健全なアクティブ/スタンバイ状態にして、アクティブデバイスからこの操作を実行します。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

ステップ 3 歯車アイコン（⚙）から、[HAの破棄（Break HA）] を選択します。

ステップ 4 確認メッセージを読み、オプションを選択してインターフェイスを無効にするかどうかを決定し、[OK] をクリックします。

スタンバイ装置からHAを破棄する場合は、インターフェイスを無効にするオプションを選択する必要があります。

システムはすぐに、このデバイスとピアデバイスの両方で変更を展開します（可能な場合）。各デバイスで展開が完了して、各デバイスが依存しなくなるまで数分かかることがあります。

アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー）

機能しているハイアベイラビリティペア（つまり、1つのピアがアクティブで、もう1つがスタンバイ）のアクティブ/スタンバイ モードを切り替えることができます。たとえば、ソフトウェアアップグレードをインストールしている場合は、アクティブな装置をスタンバイに切り替えて、アップグレードがユーザートラフィックに影響を及ぼさないようにできます。

モードはアクティブまたはスタンバイ装置から切り替えることができますが、ピア装置はその他の装置の観点から機能している必要があります。中断中の装置がある場合、モードを切り替えることはできません（最初に HA を再開する必要があります）。そうしないと、失敗します。

（注） 必要に応じて、CLIからアクティブモードとスタンバイモードを切り替えることができます。スタンバイ装置から、**failover active**コマンドを入力します。アクティブ装置から、**no failover active** コマンドを入力します。

始める前に

モードを切り替える前に、アクティブな装置で展開ジョブが進行中でないことを確認します。展開ジョブの完了を待ってから、モードを切り替えます。

アクティブな装置に保留中の展開していない変更がある場合は、モードを切り替える前に展開します。そうしないと、新しいアクティブな装置から展開ジョブを実行した場合に変更内容が失われます。

手順

ステップ 1 [デバイス（Device）] をクリックします。

ステップ 2 デバイスの概要の右側に表示される [ハイアベイラビリティ（High Availability）] リンクをクリックします。

ステップ 3 歯車アイコンから（⚙）から、[モードの切り替え（Switch Mode）] を選択します。

ステップ 4 確認メッセージを読んで、[OK] をクリックします。

強制的にフェールオーバーが行われ、アクティブな装置がスタンバイになり、スタンバイ装置が新しいアクティブな装置になります。

フェールオーバー後の未展開の設定変更の保持

ハイ アベイラビリティ ペアの装置の設定を変更する場合は、アクティブ装置で設定を編集します。その後、変更を展開すると、アクティブ装置とスタンバイ装置の両方が新しい設定で更新されます。アクティブ装置がプライマリデバイスであるかセカンダリデバイスであるかは関係ありません。

ただし、未展開の変更は装置間で同期されません。未展開の変更は、変更を行った装置でのみ利用できます。

そのため、未展開の変更があるときにフェールオーバーが発生すると、その変更は新しいアクティブ装置で利用できません。ただし、現在のスタンバイになっている装置では、変更が保持されています。

未展開の変更を取得するには、モードを切り替えてフェールオーバーを強制的に実行し、そのもう一方の装置をアクティブステータスに戻す必要があります。新しくアクティブになった装置にログインすると、未展開の変更が利用可能になり、それらを展開できます。[ハイアベイ

ラビリティ（High Availability）] 設定の歯車メニュー（⚙）から [モードの切り替え（Switch Modes）] コマンドを使用します。

次の点に注意してください。

- スタンバイ装置上に未展開の変更があるときにアクティブ装置から変更を展開すると、スタンバイ装置上の未展開の変更が削除されます。そのため、それらを取得できなくなります。
- スタンバイ装置がハイアベイラビリティペアに参加すると、そのスタンバイ装置上の未展開の変更が削除されます。装置がペアに参加または再参加するたびに、設定が同期されます。
- 未展開の変更を持つ装置に致命的な障害が発生し、その装置を置き換えたり再イメージ化する必要があった場合は、未展開の変更が完全に失われます。

ハイ アベイラビリティ モードでのライセンスと登録の変更

ハイ アベイラビリティ ペアの装置は、ライセンスと登録ステータスが同じである必要があります。変更するには、次の手順に従います。

- アクティブ装置でオプションのライセンスを有効または無効にします。その後、設定を展開すると、スタンバイ装置が必要なライセンスを要求（または解放）します。ライセンスを有効にする際は、Cisco Smart Software Manager アカウントで十分な数のライセンスが使用可能であることを確認する必要があります。これを確認しないと、一方の装置が準拠、もう一方の装置が非準拠になる可能性があります。
- 装置を個別に登録または登録解除します。正しく機能させるには、両方の装置を評価モードにするか、両方の装置を登録する必要があります。装置を異なる Cisco Smart Software Manager アカウントに登録できますが、それらのアカウントは、エクスポート制御機能設定が同じ状態（両方有効または両方無効）である必要があります。装置の登録ステータスに一貫性がない場合は、設定の変更を展開できません。

HA IPsec 暗号キーまたは HA 設定の編集

フェールオーバー基準を変更するには、アクティブ装置にログインし、変更を加えて、それらを展開します。

ただし、フェールオーバーリンクで使用されるIPsec暗号キーを変更したり、フェールオーバーまたはステートフル フェールオーバー リンクのインターフェイスやIPアドレスを変更する必要がある場合は、まず HA 設定を解除する必要があります。その後、新しい暗号キーまたはフェールオーバー/ステートフル フェールオーバー リンク設定を使用してプライマリおよびセカンダリ装置を再設定できます。

障害のある装置の正常な装置としてのマーキング

ハイ アベイラビリティ設定の装置は、定期的なヘルス モニタリングによって、障害が発生した装置としてマーキングされる場合があります。この装置が正常である場合は、ヘルスモニタリング要件を再度満たすと正常なステータスに戻ります。正常なデバイスが、頻繁に、障害が発生したデバイスとしてマーキングされる場合は、ピアタイムアウトの値を増やしたり、重要性の低い特定のインターフェイスのモニタリングを停止したり、インターフェイスのモニタリングタイムアウトを変更することができます。

CLI から **failover reset** コマンドを入力することにより、障害が発生した装置を強制的に正常な装置として表示させることができます。このコマンドは、アクティブ装置から入力することをお勧めします。それにより、スタンバイ装置のステータスがリセットされます。**show failover** コマンドまたは **show failover state** コマンドを使用することにより、装置のフェールオーバーステータスを表示できます。

障害が発生した装置を障害のない状態に復元しても、その装置は自動的にはアクティブになりません。復元された装置は、（強制または通常の）フェールオーバーによってアクティブになるまではスタンバイ状態のままです。

デバイスステータスをリセットしても、障害が発生したデバイスとしてマーキングされる原因となった問題は解決されません。問題に対処しなかったり、モニタリングタイムアウトを緩和したりすると、そのデバイスは、障害が発生したデバイスとして再びマーキングされます。

ハイアベイラビリティ Threat Defense のアップグレード

ハイアベイラビリティデバイスをアップグレードするには、この手順を使用します。一度に1つずつアップグレードしてください。中断を最小限に抑えるため、スタンバイは常にアップグレードします。つまり、現在のスタンバイをアップグレードし、ロールを切り替えてから、新しいスタンバイをアップグレードします。FXOS を更新する必要がある場合は、どちらかのシャーシで Threat Defense をアップグレードする前に、両方のシャーシで更新してください。その場合も、常にスタンバイをアップグレードします。

⚠

注意 一方のユニットのアップグレード中にもう一方のユニットで設定変更を行ったり展開したりしないでください。また、異なるバージョンのペアに設定変更を展開しないでください。システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。失敗した（または進行中）のメジャーおよびメンテナンスアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。問題が解消されない場合は、Cisco TAC にお問い合わせください。

アップグレード中に発生する可能性のあるこれらの問題およびその他の問題の詳細については、ハイアベイラビリティ Threat Defense のアップグレードのトラブルシューティング （273 ページ）を参照してください。

始める前に

事前アップグレードのチェックリストを完了します。正常に展開され、通信が確立されていることを確認します。

ヒント　アップグレード前のチェックリストには、計画（Cisco Secure Firewall Threat Defense リリースノートを読むことから開始）、バックアップの作成、アップグレードパッケージの取得、および関連するアップグレード（Firepower 4100/9300 の FXOS など）の実行が含まれます。また、必要な構成変更のチェック、準備状況のチェック、ディスク容量のチェック、実行中のタスクとスケジュールされたタスクの両方のチェックも含まれます。アップグレード手順の詳細については、アップグレード前のチェックリストを含め、お使いのバージョンの『Device Manager 用 Cisco Secure Firewall Threat Defense アップグレードガイド』を参照してください。

手順

ステップ 1　スタンバイユニットにログインします。

ステップ 2　[デバイス（Device）] を選択し、[更新（Updates）] パネルの [設定の表示（View Configuration）] をクリックします。
[システムアップグレード（System Upgrade）] パネルには、現在実行中のソフトウェアバージョン、およびすでにアップロードされたアップグレードパッケージが表示されます。

ステップ 3　アップグレードパッケージをアップロードします。

アップロードできるパッケージは 1 つだけです。新しいパッケージをアップロードすると、古いパッケージが置き換えられます。ターゲットバージョンとデバイスモデルに適したパッケージがあることを確認してください。[参照（Browse）] または **[ファイルの置き換え（Replace File）]** をクリックしてアップロードを開始します。

アップロードが完了すると、確認ダイアログボックスが表示されます。[OK] をクリックする前に、必要に応じて [すぐにアップグレードを実行（Run Upgrade Immediately）] を選択して、ロールバックオプションを選択し、今すぐアップグレードします。今すぐアップグレードする場合は、アップグレード前のチェックリストをできるだけ多く完了することが特に重要です（次のステップを参照）。

ステップ 4　準備状況チェックを含む、アップグレード前の最終チェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。準備状況チェックを手動で実行しない場合、アップグレードの開始時に実行されます。準備状況チェックに失敗すると、アップグレードはキャンセルされます。詳細については、アップグレード準備状況チェックの実行（978 ページ）を参照してください。

ステップ 5　**[今すぐアップグレード（Upgrade Now）]** をクリックしてアップグレードを開始します。

a)　ロールバックオプションを選択します。

[アップグレードに失敗すると自動的にキャンセルされ、前のバージョンにロールバックする（Automatically cancel on upgrade failure and roll back to the previous version）] を選択できます。オプションを有効にすると、メジャーまたはメンテナンスアップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。失敗したアップグレードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。

b) [続行（Continue）] をクリックして、アップグレードしてデバイスを再起動します。

自動的にログオフされ、デバイスが再起動するまでアップグレードを監視できるステータスページに移動します。また、このページには、進行中のインストールをキャンセルするオプションが含まれています。自動ロールバックを無効にしてアップグレードが失敗した場合は、アップグレードを手動でキャンセルするか、再試行できます。

アップグレード中にトラフィックがドロップされます。ISA 3000 の場合にのみ、電源障害に対するハードウェアバイパスを設定すると、トラフィックはアップグレード中にドロップされますが、デバイスのアップグレード後の再起動完了時に検査なしでトラフィックが渡されます。

ステップ 6 可能なときに再度ログインし、アップグレードが成功したことを確認します。

[デバイスの概要（Device Summary）]ページには、現在実行中のソフトウェアバージョンとハイアベイラビリティのステータスが表示されます。成功を確認する「とともに」ハイアベイラビリティが再開されるまで、続行しないでください。アップグレードが成功した後もハイアベイラビリティが一時停止されたままになる場合は、ハイアベイラビリティ Threat Defense のアップグレードのトラブルシューティング （273 ページ）を参照してください。

ステップ 7 2 つ目のユニットをアップグレードします。

a) ロールを切り替えてこのデバイスをアクティブにします。**[デバイス（Device）]** > **[ハイアベイラビリティ（High Availability）]** を選択し、歯車メニュー（⚙）から [モードの切り替え（Switch Mode）] を選択してください。ユニットのステータスがアクティブに変わるのを待ち、トラフィックが正常に送信されていることを確認します。ログアウトします。

b) アップグレードします。前の手順を繰り返して新しいスタンバイにログインして、パッケージをアップロードし、デバイスをアップグレードして、進行状況をモニターし、成功を確認してください。

ステップ 8 デバイスのロールを調べます。

特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

ステップ 9 アクティブユニットにログインします。

ステップ 10 アップグレード後のタスクを完了します。

a) システムデータベースを更新します。侵入ルール、VDB、GeoDB の自動更新が設定されていない場合は、ここで更新します。

b) アップグレード後に必要な構成変更が他にもあれば、実行します。

c) 展開します。

ハイアベイラビリティ Threat Defense のアップグレードのトラブルシューティング

一般的なアップグレードのトラブルシューティング

以下の問題は、スタンドアロンまたはハイアベイラビリティペアのデバイスをアップグレードするときに発生する可能性があります。

アップグレードパッケージのエラー。

適切なアップグレードパッケージを見つけるには、使用しているモデルを シスコ サポートおよびダウンロード サイト で選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。

バージョン 6.2.1 以降のアップグレードパッケージは署名されており、ファイル名の最後は .sh.REL.tar です。署名付きのアップグレードパッケージは解凍しないでください。アップグレードパッケージの名前を変更したり、電子メールで転送したりしないでください。

アップグレード中にデバイスにまったく到達できない。

デバイスは、アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止します。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。

アップグレード中にデバイスが非アクティブまたは無反応に見える。

進行中のメジャーおよびメンテナンスアップグレードは手動でキャンセルできます。Threat Defense のアップグレードのキャンセルまたは再試行（980 ページ）を参照してください。デバイスが応答しない場合、またはアップグレードをキャンセルできない場合は、Cisco TAC にお問い合わせください。

⚠

注意 システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウン「しない」でください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

アップグレードは成功したが、システムが予期どおりに機能しない。

まず、キャッシュされた情報が更新されていることを確認します。単にブラウザウィンドウを更新して再度ログインするのではなく、URL から「余分な」パスを削除し、ホームページに再接続します（たとえば、http://threat-defense.example.com/）。

引き続き問題が発生し、以前のメジャーリリースまたはメンテナンスリリースに戻す必要がある場合は、復元できる場合があります。Threat Defense の復元（980 ページ）を参照してください。復元できない場合は、イメージを再作成する必要があります。

アップグレードが失敗する。

メジャーアップグレードまたはメンテナンスアップグレードを開始する場合は、[アップグレードに失敗すると自動的にキャンセルされる...（Automatically cancel on upgrade failure...）]（自動キャンセル）オプションを使用して、次のように、アップグレードが失敗した場合の動作を選択します。

- [自動キャンセルが有効（Auto-cancel enabled）]（デフォルト）：アップグレードが失敗すると、アップグレードがキャンセルされ、デバイスは自動的にアップグレード前の状態に復元されます。問題を修正し、後で再試行してください。
- [自動キャンセルが無効（Auto-cancel disabled）]：アップグレードが失敗した場合、デバイスはそのままになります。問題を修正してすぐに再試行するか、手動でアップグレードをキャンセルして後で再試行してください。

詳細については、Threat Defense のアップグレードのキャンセルまたは再試行 （980 ページ）を参照してください。再試行またはキャンセルできない場合、または問題が解消されない場合は、Cisco TAC にお問い合わせください。

ハイアベイラビリティのアップグレードのトラブルシューティング

以下の問題は、ハイアベイラビリティのアップグレードに固有です。

未確定の変更を展開しないと、アップグレードは開始されません。

未確定の変更がないにもかかわらず、すべての未確定の変更を展開する必要があることを示すエラーメッセージが表示される場合は、アクティブユニットにログインして（スタンバイユニットをアップグレードする必要があることに注意してください）、マイナーな変更を作成し、展開してください。その後、変更を元に戻し、再展開してから、スタンバイでアップグレードを再試行します。

この方法では解決せず、ユニットが推奨されるものとは異なるソフトウェアバージョンを実行している場合は、ロールを切り替えてスタンバイユニットをアクティブにしてから、高可用性を一時停止します。一時停止したアクティブユニットから展開して高可用性を再開し、ロールを切り替えてアクティブユニットを再びスタンバイにします。これでアップグレードが動作するはずです。

スタンバイのアップグレード中にアクティブユニットからの展開が失敗するか、アプリケーション同期エラーが発生する。

これは、スタンバイのアップグレード中にアクティブユニットから展開した場合に発生する可能性があります。この操作は、サポートされていません。エラーが発生してもアップグレードを続行してください。両方のユニットをアップグレードした後に、必要な設定変更を行い、アクティブユニットから展開します。エラーは解決するはずです。

これらの問題を回避するために、一方のユニットのアップグレード中にもう一方のユニットで設定変更を行ったり展開したりしないでください。また、異なるバージョンのペアに設定変更を展開しないでください。

アップグレード中に行われた設定変更が失われる。

何らかの理由で、設定変更を行い、異なるバージョンのペアに展開する必要がある場合は、両方のユニットに変更を加える必要があります。そうしないと、下位バージョンのアクティブユニットをアップグレードした後にそれらの設定変更が失われます。

アップグレード後に高可用性が一時停止される。

アップグレード後の再起動の後に、システムがライブラリの更新や Snort の再起動といった最終的な自動タスクを実行している間は、高可用性が一時的に停止されます。アップグレードの「直後」にCLIにログインすると、多くの場合、この状態が見られます。アップグレードが完全に完了して Device Manager が使用可能になっても高可用性が自動的に再開されない場合は、手動で実行してください。

1. アクティブデバイスとスタンバイデバイスの両方にログインし、タスクリストを確認します。両方のデバイスで、実行されているすべてのタスクが完了するまで待ちます。高可用性を再開するのが早すぎると、その後に、フェールオーバーが原因で停止するという問題が発生する可能性があります。
2. **[デバイス（Device）]**>**[高可用性（High Availability）]**を選択し、歯車メニュー（⚙）から [HAの再開（Resume HA）] を選択します。

異なるバージョンのペアでフェールオーバーが発生しない。

高可用性の利点は、トラフィックや検査を中断することなく展開をアップグレードできることですが、アップグレードプロセスの実行中は、その全体でフェールオーバーが無効になります。つまり、一方のデバイスがオフラインの場合には、当然、フェールオーバーは無効になりますが（フェールオーバーするものがない、つまり、本質的にすでにフェールオーバーされているため）、それだけではなく、異なるバージョンのペアでもフェールオーバーは無効になります。異なるバージョンのペアが許可される（一時的に）のは、アップグレード中のみです。何らかの問題が発生しても影響が最小限になるメンテナンスウィンドウ中に実行するようにアップグレードをスケジュールし、そのウィンドウ内で両方のデバイスをアップグレードするための十分な時間を確保してください。

アップグレードが一方のデバイスでのみ失敗したか、一方のデバイスが復元され、現在は、異なるバージョンのペアが動作している。

異なるバージョンのペアは、一般的な動作ではサポートされていません。下位バージョンのデバイスをアップグレードするか、上位バージョンのデバイスを復元してください。パッチの場合は復元がサポートされていないため、下位バージョンのデバイスを正常にアップグレードできないときは、高可用性を解除し、一方または両方のデバイスのイメージを再作成してから、高可用性を再確立する必要があります。

ハイ アベイラビリティ ペアでの装置交換

必要に応じて、ネットワーク トラフィックを中断することなくハイ アベイラビリティ グループ内の装置を交換できます。

手順

ステップ 1 交換する装置が機能している場合は、ピア装置にフェールオーバーするようにし、デバイス CLI の **shutdown** コマンドを使用して、デバイスをグレースフルシャットダウンします。装置が機能していない場合は、ピアがアクティブモードで動作していることを確認します。

管理者権限がある場合は、Device Manager CLI コンソールから **shutdown** コマンドを入力することもできます。

ステップ 2 装置をネットワークから取り除きます。

ステップ 3 交換装置を設置して、インターフェイスを再接続します。

ステップ 4 交換装置でデバイス セットアップ ウィザードを完了します。

ステップ 5 ピア装置で[ハイアベイラビリティ（High Availability）]ページにアクセスし、設定をクリップボードにコピーします。装置がプライマリ装置か、セカンダリ装置かに注意してください。

保留中の変更がある場合は、それらの変更を展開し、展開が完了するまで待ってから続行します。

ステップ 6 交換装置で [ハイアベイラビリティ（High Availability）] グループで [設定（Configure）] をクリックして、ピアから反対側の装置タイプを選択します。つまり、ピアがプライマリの場合は [セカンダリ（Secondary）] を選択し、ピアがセカンダリの場合は [プライマリ（Primary）] を選択します。

ステップ 7 ピアから HA の設定を貼り付け、IPsec キーを入力します（使用する場合）。[HAの有効化（Activate HA）] をクリックします。

展開が完了すると、装置はピアに連絡して HA グループに参加します。アクティブなピアの設定がインポートされ、選択内容に基づいて、交換装置がグループ内のプライマリ装置またはセカンダリ装置になります。これで、HA が正常に動作していることを確認し、必要に応じてモードを切り替えて、新しい装置をアクティブな装置にできます。

ハイ アベイラビリティのモニター

ここでは、ハイアベイラビリティをモニターする方法について説明します。

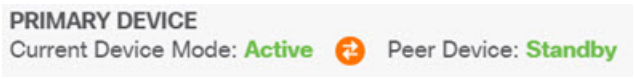
イベントビューアとダッシュボードには、ログインしているデバイスに関するデータだけが表示されることに注意してください。両方のデバイスの統合された情報は表示されません。

フェールオーバーの全般的なステータスと履歴のモニタリング

次の方法で、高可用性の全般的なステータスと履歴をモニターできます。

- [デバイス概要（Device Summary）]（[デバイス（Device）] をクリック）の [ハイアベイラビリティ（High Availability）] グループに装置のステータスが表示されます。

- [ハイアベイラビリティ（High Availability）] ページ（**[デバイス（Device）] > [ハイアベイラビリティ（High Availability）]** をクリック）に両方の装置のステータスが表示されます。失敗した場合は、直近の失敗理由（フェールオーバー履歴から）が表示されます。それらの間にある同期のアイコンをクリックすると、追加のステータスが表示されます。



- [ハイアベイラビリティ（High Availability）] ページで、ステータスの横にある [フェールオーバー履歴（Failover History）] リンクをクリックします。CLI コンソールが開き、**show failover history details** コマンドが実行されます。このコマンドを CLI または CLI コンソールに直接入力することもできます。

CLI コマンド

CLI または CLI コンソールで次のコマンドを使用できます。

- **show failover**

  装置のフェールオーバー状態についての情報を表示します。

- **show failover history** ［**details**］

  過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。**details** キーワードを追加すると、ピアユニットのフェールオーバー履歴が表示されます。この情報は、トラブルシューティングに役立ちます。

- **show failover state**

  両方の装置のフェールオーバー状態が表示されます。この情報には、装置のプライマリまたはセカンダリステータス、装置のアクティブ/スタンバイステータス、最後にレポートされたフェールオーバーの理由などが含まれます。

- **show failover statistics**

  フェールオーバー インターフェイスの送信（tx）パケット数と受信（rx）パケット数が表示されます。たとえば、装置がパケットを送信しているのに受信パケットがないことが出力に示されている場合は、リンクに問題があります。ケーブルに問題がある、ピアで正しくない IP アドレスが設定されている、装置によってフェールオーバー インターフェイスが異なるサブネットに接続されているといった可能性があります。

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

フェールオーバーおよびステートフル フェールオーバー リンクの設定が表示されます。次に例を示します。

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  ハイアベイラビリティに関してモニターされているインターフェイスに関する情報が表示されます。詳細は、HA モニター対象インターフェイスのステータスのモニタリング（278 ページ）を参照してください。

- **show running-config failover**

  実行コンフィギュレーション内のフェールオーバー コマンドを表示します。これらは、ハイ アベイラビリティを設定するコマンドです。

HA モニター対象インターフェイスのステータスのモニタリング

いずれかのインターフェイスの HA モニタリングを有効にしている場合は、CLI または CLI コンソールで **show monitor-interface** コマンドを使用して、モニター対象インターフェイスのステータスを確認できます。

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

モニター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。

- (Waiting)（Unknown (Waiting) などのように他のステータスと結合）：インターフェイスはピア装置上の対応するインターフェイスから hello パケットをまだ受信していません。
- 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。

HA 関連の Syslog メッセージのモニタリング

システムは、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。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。Syslog メッセージの説明については、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html にある『*Cisco Threat Defense Syslog Messages*』を参照してください。

（注） フェールオーバー時には、システムが論理的にシャットダウンされた後にインターフェイスが起動し、Syslog メッセージ 411001 および 411002 が生成されます。これは通常のアクティビティです。

Syslog メッセージを表示するには、**[デバイス（Device）]**>**[ロギング設定（Logging Settings）]** で診断ロギングを設定する必要があります。メッセージを確実にモニターできるように、外部 Syslog サーバーを設定してください。

ピア装置での CLI コマンドのリモート実行

CLI から failover exec コマンドを使用することにより、ピアにログインすることなく、ピアデバイスに show コマンドを入力できます。

failover exec {**active** | **standby** | **mate**} コマンド

コマンドを実行する装置（アクティブまたはスタンバイ）を指定するか、ログインしている装置ではない方の装置が応答するようにする場合は **mate** を入力します。

たとえば、ピアのインターフェイス設定と統計情報を表示するには、次のように入力します。

```
> failover exec mate show interface
```

configure コマンドは入力できません。この機能は、**show** コマンドで使用します。

（注） アクティブ装置にログインしている場合は、**failover reload-standby** コマンドを使用してスタンバイ装置をリロードできます。

これらのコマンドは、Device Manager CLI コンソールからは入力できません。

ハイ アベイラビリティ（フェールオーバー）のトラブルシューティング

ハイ アベイラビリティ グループ内の装置が期待どおりに機能していない場合は、次の手順による設定のトラブルシューティングを検討します。

アクティブな装置にピア装置が「障害（Failed）」と表示されている場合は、装置の障害状態のトラブルシューティング （282 ページ）を参照してください。

手順

ステップ 1 各デバイス（プライマリとセカンダリ）から次の手順を実行します。

- フェールオーバーリンクのその他のデバイスの IP アドレスに ping を実行します。
- 別のリンクを使用する場合は、ステートフル フェールオーバー リンクの他方のデバイスの IP アドレスに ping を実行します。

ping が失敗する場合は、各デバイス上のインターフェイスが同じネットワークセグメントに接続されていることを確認します。直接ケーブル接続を使用している場合は、ケーブルを確認します。

ステップ 2 次の一般的なチェックを行います。

- プライマリとセカンダリで重複している管理 IP アドレスを確認します。
- 装置の重複しているフェールオーバー IP アドレスとステートフル フェールオーバー IP アドレスを確認します。
- 各デバイスの同等のインターフェイスポートが同じネットワークセグメントに接続されていることを確認します。

ステップ 3 スタンバイデバイスのタスクリストまたは監査ログを確認します。アクティブなデバイスで展開が成功するごとに、「アクティブノードからの設定のインポート（Configuration import from Active node）」タスクの成功を確認できる必要があります。タスクが失敗する場合は、フェールオーバーリンクを確認して、展開を再度実行してください。

（注） 失敗した展開タスクがタスクリストに示されている場合は、展開ジョブ中にフェールオーバーが発生している可能性があります。展開タスクを開始したときにスタンバイデバイスがアクティブ装置であったが、タスク中にフェールオーバーが発生した場合、展開は失敗します。この問題を解決するには、モードを切り替えてスタンバイ装置を再びアクティブ装置にしてから、設定変更を再展開します。

ステップ 4 **show failover history** コマンドを使用して、デバイスの状態変更に関する詳細情報を取得します。

以下の点を確認します。

- アプリケーションの同期エラー。

```
12:41:24 UTC Dec 6 2017

App Sync     Disabled     HA state progression failed due to APP SYNC timeout
```

アプリケーションの同期フェーズは、アクティブデバイスの設定がスタンバイデバイスに転送されるフェーズです。アプリケーションの同期エラーが発生するとデバイスは無効状態になり、そのデバイスをアクティブにすることはできなくなります。

アプリケーションの同期の問題により、デバイスが無効状態になっている場合は、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 リンクのエンドポイント用に、デバイスの別のインターフェイスを使用することができます。リンクの各端には同じポート番号を使用する必要があります。

show failover コマンドの結果、セカンダリデバイスが疑似スタンバイ状態にあると表示される場合は、セカンダリデバイスのフェールオーバーリンクに、プライマリデバイスに設定したアドレスとは異なる IP アドレスを設定している可能性があります。フェールオーバーリンクの両方のデバイスで同じプライマリ/セカンダリ IP アドレスを使用していることを確認します。

疑似スタンバイ状態は、プライマリとセカンダリで異なる IPsec キーが設定されている可能性も示しています。

その他のアプリケーションの同期の問題については、HA アプリケーション同期障害のトラブルシューティング （283 ページ）を参照してください。

- （アクティブからスタンバイに移行して戻る）フェールオーバーの頻度が異常に高い場合、フェールオーバーリンクに問題がある可能性があります。最悪のシナリオでは、両方の装置がアクティブになり、トラフィックの通過が中断されます。リンクの各端に ping を実行して接続を確認します。**show arp** を使用して、フェールオーバー IP アドレスと ARP マッピングが適切であるか確認することもできます。

  フェールオーバーリンクが正常で正しく設定されている場合は、ピアのポーリング時間とホールド時間、インターフェイスのポーリング時間とホールド時間を増やすか、HA の監視対象インターフェイスの数を減らすか、インターフェイスのしきい値を増やすことを検討してください。

- インターフェイスチェックが原因のエラー。[インターフェイスチェック（Interface Check）] 理由には、障害が発生したと見なされるインターフェイスの一覧が含まれています。それらのインターフェイスをチェックして、正しく設定されていること、ハードウェアの問題がないことを確認します。リンクの反対側のスイッチの設定に問題がないことを確認します。問題がない場合は、それらのインターフェイスに対する HA モニタリングの無効化を検討します。または、インターフェイス障害のしきい値やタイミングを増やすこともできます。

```
06:17:51 UTC Jan 15 2017

Active     Failed     Interface check

                        This Host:3

                           admin: inside

                           ctx-1: ctx1-1

                           ctx-2: ctx2-1

                        Other Host:0
```

ステップ 5 スタンバイ装置を検出できず、フェールオーバーリンクの LAN またはケーブル接続の不良など、具体的な理由を見つけられない場合は、次の手順を実行します。

a) スタンバイ装置で CLI にログインし、**failover reset** コマンドを入力します。このコマンドにより、装置の状態が「障害」から「非障害」に変わります。次に、アクティブデバイスの HA ステータスを確認します。スタンバイピアが検出される場合は、これで終了です。

b) アクティブな装置で CLI にログインし、**failover reset** コマンドを入力します。アクティブとスタンバイの両方の装置で HA ステータスがリセットされます。デバイス間のリンクが再確立されるのが理想的です。HA のステータスを確認します。正しくない場合は手順を続行します。

c) アクティブデバイスの CLI から、または Device Manager から、まず HA を中断してから HA を再開します。CLI コマンドは **configure high-availability suspend** および **configure high-availability resume** です。

d) これらの手順が失敗する場合は、スタンバイ デバイスを **reboot** します。

装置の障害状態のトラブルシューティング

ピア装置のハイ アベイラビリティ ステータス（[デバイス（Device）] または **[デバイス（Device）]** > **[ハイアベイラビリティ（High Availability）]** ページ）で装置が故障としてマークされている場合、アクティブ装置である装置 A と故障したピアである装置 B に基づいて、考えられる一般的な原因は次のとおりです

- 装置 B がハイアベイラビリティ向けに設定されていない場合（スタンドアロンモードのままになっている場合）、装置 A は装置 B を故障として表示します。
- 装置 B で HA を一時停止すると、装置 A は装置 B を故障として表示します。
- 装置 B をリブートすると、装置 B がリブートを完了してフェールオーバーリンク経由で通信を再開するまで装置 A は装置 B を故障として表示します。
- 装置 B でアプリケーションの同期（App Sync）が失敗すると、装置 A は装置 B を故障として表示します。HA アプリケーション同期障害のトラブルシューティング（283 ページ）を参照してください。

- 装置 B で装置またはインターフェイスのヘルスモニタリングが失敗すると、装置 A は装置 B を故障として表示します。システム上の問題がないか装置 B を確認します。デバイスをリブートしてみます。装置がおおむね正常な場合は、装置またはインターフェイスのヘルスモニタリング設定を緩和することを検討します。**show failover history** の出力にインターフェイス正常性チェックのエラーに関する情報が示されます。
- 両方の装置がアクティブな場合、各装置はピアを故障として表示します。通常、これはフェールオーバー リンクに問題があることを示しています。

  ライセンスの問題を示している可能性もあります。デバイスは一貫したライセンス（両方とも評価モードであるか、両方が登録されている）を保持している必要があります。登録されている場合、使用するスマート ライセンス アカウントは別々であっても構いませんが、どちらのアカウントも輸出制限対象の機能で有効または無効のいずれか同じものを選択している必要があります。輸出規制機能に関する設定が不整合な状態で IPsec 暗号化鍵を設定すると、HA を有効化した後に両方のデバイスがアクティブになります。これはサポートされているネットワーク セグメント上のルーティングに影響を与え、回復させるにはセカンダリ装置で HA を手動で中断する必要があります。

HA アプリケーション同期障害のトラブルシューティング

ピア装置が HA グループへの参加に失敗する場合、またはアクティブ装置からの変更を展開しているときにピア装置で障害が発生する場合は、障害が発生した装置にログインして [ハイアベイラビリティ（High Availability）] ページに移動し、[フェールオーバー履歴（Failover History）] リンクをクリックします。**show failover history** 出力にアプリケーション同期の障害が示されている場合、装置がハイ アベイラビリティ グループとして正しく機能できることをシステムが確認する、HA の検証段階に問題があります。

このタイプの障害は、次のように表示されます。

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
App Sync                  Disabled                  CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

理想としては、From State が App Sync のときに「All validation passed」というメッセージが表示され、ノードが Standby Ready 状態になります。任意の検証で障害が発生すると、ピアは

Disabled（Failed）状態になります。問題を解決して、ピアがハイ アベイラビリティ グループとして再度機能するようにする必要があります。アクティブ装置に変更を加えてアプリケーションの同期エラーを修正した場合は、ピア ノードを結合するために、それらを展開して HA を再開する必要があります。

次のメッセージは障害の発生を示し、問題の解決方法について説明しています。これらのエラーは、ノードの結合時および後続の各展開時に発生する可能性があります。ノードの結合中は、システムにより、アクティブ装置で最後に展開された設定に対してチェックが実行されます。

- 「ライセンス登録モードがプライマリ ノードとセカンダリ ノードで一致していません。（License registration mode mismatch between Primary and Secondary Node.）」

  ライセンスエラーは、1 つのピアが評価モードになっているときにもう一方のピアが登録されたことを示します。ピアを HA グループに参加させるには、ピアを両方とも登録するか、両方とも評価モードにする必要があります。登録したデバイスを評価モードに戻すことはできないため、**[デバイス（Device）]** > **[スマートライセンス（Smart License）]** ページからもう一方のピアを登録する必要があります。

  登録するデバイスがアクティブ装置の場合、デバイスの登録後に展開を実行します。展開することで装置は強制的に更新され、設定が同期されます。これにより、セカンダリ装置はハイ アベイラビリティ グループに正しく参加できます。

- 「ライセンス エクスポート コンプライアンスがプライマリ ノードとセカンダリ ノードで一致していません。（License export compliance mismatch between Primary and Secondary Node.）」

  ライセンス コンプライアンス エラーは、デバイスが異なる Cisco Smart Software Manager アカウントに登録されており、1 つのアカウントでは輸出規制された機能が有効で、もう一方のアカウントでは無効になっていることを示します。デバイスは、輸出規制された機能の設定（有効または無効）が同じアカウントに登録される必要があります。**[デバイス（Device）]** > **[スマートライセンス（Smart License）]** ページでデバイス登録を変更します。

- 「ソフトウェア バージョンがプライマリ ノードとセカンダリ ノードで一致していません。（Software version mismatch between Primary and Secondary Node.）」

  ソフトウェア不一致エラーは、ピアが異なるバージョンの Threat Defense ソフトウェアを実行していることを示します。一度に 1 台のデバイスにソフトウェアアップグレードをインストールしている場合、システムは一時的にのみ不一致を許容します。ただし、ピアのアップグレードの間に設定変更を展開することはできません。この問題を解決するには、ピアをアップグレードしてから展開をやり直します。

- 「物理インターフェイスがプライマリ ノードとセカンダリ ノードで一致していません。（Physical interfaces mismatch between Primary and Secondary Node.）」

  HA グループのスタンバイ装置には、アクティブ装置に存在するすべての物理インターフェイスを持たせる必要があり、それらのインターフェイスには同じハードウェア名とタイプ（GigabitEthernet1/1 など）を持たせる必要があります。このエラーは、アクティブ装置に存在する一部のインターフェイスがスタンバイ装置に存在しないことを示しています。ス

タンバイ装置にはアクティブ装置よりも多くのインターフェイスを含めることができます。そのため、アクティブにする装置を切り替えるか、または別のピア装置を選択してください。ただし、インターフェイスの不一致状態は一時的にする必要があります。たとえば、ある装置でインターフェイスモジュールを交換していて、そのモジュールを使用せずに短時間装置を実行する必要がある場合などです。通常の動作では、両方の装置についてインターフェイスの数とタイプが同じである必要があります。

- 「フェールオーバー リンク インターフェイスがプライマリ ノードとセカンダリ ノードで一致していません。（Failover link interface mismatch between Primary and Secondary Node.）」

  各装置でフェールオーバー物理インターフェイスをネットワークにリンクする場合、同じ物理インターフェイスを選択する必要があります。たとえば、各装置でGigabitEthernet1/8にします。このエラーは、異なるインターフェイスを使用したことを示しています。エラーを解決するには、ピア装置のケーブル配線を修正します。

- 「ステートフル フェールオーバー リンク インターフェイスが、プライマリ ノードとセカンダリ ノードで一致していません。（Stateful failover link interface mismatch between Primary and Secondary Node.）」

  別々のステートフル フェールオーバー リンクを使用する場合、各装置でステートフル フェールオーバー インターフェイスをネットワークにリンクするときに、同じ物理インターフェイスを選択する必要があります。たとえば、各装置で GigabitEthernet1/7 にします。このエラーは、異なるインターフェイスを使用したことを示しています。エラーを解決するには、ピア装置のケーブル配線を修正します。

- 「フェールオーバー/ステートフル フェールオーバー リンク EtherChannel のメンバー インターフェイスが、プライマリ ノードとセカンダリ ノードで一致していません（Failover/Stateful failover link EtherChannel's member interfaces mismatch between Primary and Secondary Node）」

  フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスのいずれかに EtherChannel インターフェイスを選択する場合、EtherChannel は各デバイスで同じ ID とメンバーインターフェイスを持つ必要があります。このエラーメッセージは、不一致があるのがフェールオーバーリンクかステートフル フェールオーバー リンクかを示します。エラーを解決するには、EtherChannelインターフェイスの設定を修正し、各デバイスで同じ ID を使用し、同じインターフェイスを含めるようにします。

- 「デバイスのモデル番号がプライマリ ノードとセカンダリ ノードで一致していません。（Device Model Number mismatch between Primary and Secondary Node.）」

  HA グループに参加するピアは、まったく同じモデルのデバイスである必要があります。このエラーは、ピアが同じデバイスモデルではないことを示しています。異なるピアを選択して HA を設定する必要があります。

- アクティブノードとスタンバイノードを同じシャーシに配置することはできません。

  同じハードウェアシャーシでホストされているデバイスを使用してハイアベイラビリティを設定することはできません。同じシャーシで複数のデバイスをサポートするモデルでハイアベイラビリティを設定する場合は、別のハードウェアに存在するデバイスを選択する必要があります。

- 「不明なエラーが発生しました。もう一度お試しください。（Unknown error occurred, please try again.）」

  アプリケーションの同期中に問題が発生しましたが、システムが問題を特定できませんでした。もう一度設定を展開してみてください。

- 「ルール パッケージが破損しています。ルール パッケージを更新して、もう一度試してください。（Rule package is corrupted. Please update the rule package and try again.）」

  侵入ルールデータベースに問題があります。障害が発生したピアで、**[デバイス（Device）]**> **[更新（Updates）]** に移動して、[ルール（Rule）] グループの [今すぐ更新（Update Now）] をクリックします。更新が完了するのを待って、変更を展開します。アクティブ装置から展開を再試行できます。

- プライマリ ノードとセカンダリ ノードのクラウドサービスの登録ステータスが一致しません。

  一方のノードは Cisco Cloud に登録されていますが、もう一方のノードは登録されていません。高可用性グループを形成するには、両方のノードが登録されているか、どちらも登録されていないことが必要です。各デバイスで **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** に移動し、両方のデバイスが同じクラウドサービスリージョンに登録されていることを確認します。

- アクティブ ノードとスタンバイ ノードとで異なるクラウド リージョンを設定することはできません。

  デバイスが異なるシスコ クラウドサービス リージョンに登録されています。どのリージョンが正しいかを確認し、スマート ライセンスから他のデバイスの登録を解除し、再登録時に正しいリージョンを選択してください。両方のデバイスのリージョンが間違っている場合は、両方のデバイスの登録を解除し、正しいリージョンに再登録します。

- 「展開パッケージが破損しています。（Deployment package is corrupted.）再度実行してください。（Please try again.）」

  これはシステムエラーです。展開をもう一度試して、この問題を解決する必要があります。

第 11 章

インターフェイス

ここでは、脅威に対する防御デバイスでのインターフェイスの設定方法について説明します。

Threat Defense インターフェイスについて

Threat Defense には、データインターフェイスやManagementインターフェイスが組み込まれています。

インターフェイス接続（物理的または仮想）のためにケーブルを接続するとき、インターフェイスを設定する必要があります。最小限の作業として、トラフィックを通過させることができるようにインターフェイスを指定して有効化します。インターフェイスがブリッジグループのメンバーである場合、これで十分です。ブリッジ グループのメンバーでない場合、インターフェイスにIPアドレスを割り当てる必要があります。単一の物理インターフェイスではなく、VLANサブインターフェイスを特定のポートで作成する場合、通常、物理インターフェイスで

はなくサブインターフェイス上で IP アドレスを設定します。VLAN サブインターフェイスを使用すると、物理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。これは、スイッチのトランク ポートに接続する場合に役立ちます。パッシブインターフェイスでは IP アドレスを設定しません。

[インターフェイス（Interfaces）]ページには、インターフェイスタイプのサブページが含まれます（[インターフェイス（Interfaces）]（物理インターフェイスの場合）、[ブリッジグループ（Bridge Groups）]、[仮想トンネルインターフェイス（Virtual Tunnel Interfaces）]、[EtherChannel（EtherChannels）]、[VLAN]（Firepower 1010 の場合））。Firepower 4100/9300 EtherChannel は[インターフェイス（Interfaces）] ページには表示されますが、[EtherChannel] ページには表示されないことに注意してください。これは、Device Manager ではなく FXOS の EtherChannel パラメータのみを変更できるためです。各ページに、利用可能なインターフェイスとそれぞれの名前、アドレス、モード、状態が示されます。インターフェイスのステータスは、インターフェイスのリストで直接オン/オフを変更できます。このリストは、設定に基づいたインターフェイス特性を示します。メンバーインターフェイスを参照するには、ブリッジグループ、EtherChannel、または VLAN インターフェイス上で [開く/閉じる（open/close）] 矢印を使用します。メンバーインターフェイスは対応するリストにも表示されます。サポートされている親インターフェイスのサブインターフェイスを表示することもできます。これらのインターフェイスが仮想インターフェイスおよびネットワーク アダプタにどのようにマッピングされるかについては、Threat Defense の物理インターフェイスへの VMware ネットワークアダプタとインターフェイスのマッピング方法 （20 ページ）を参照してください。

以下の各トピックでは、Device Manager を使用してインターフェイスを設定する場合の制限事項、およびインターフェイス管理に関するその他の概念について説明します。

インターフェイス モード

インターフェイスごとに次のモードのいずれかを設定できます。

ルーテッド

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。通常、これらのインターフェイスをスイッチ、別のルータ上のポート、またはISP/WAN ゲートウェイに接続します。

インライン

インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。

パッシブ

パッシブ インターフェイスは、スイッチ SPAN（スイッチド ポート アナライザ）またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニターします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができませ

ん。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

スイッチポート（Firepower 1010）
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、脅威に対する防御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。トラング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。管理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。

BridgeGroupMember

ブリッジ グループは、脅威に対する防御 デバイス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。すべてのインターフェイスは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。

BVI に名前を付けると、ルーテッド インターフェイスと BVI の間のルーティングを実行できます。この場合、BVI はメンバー インターフェイスとルーテッド インターフェイス間のゲートウェイとして機能します。BVI に名前を指定しない場合、ブリッジ グループメンバーのインターフェイス上のトラフィックはブリッジ グループを離れることができません。通常、インターネットにメンバーインターフェイスをルーティングするため、インターフェイスに名前を付けます。

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脅威に対する防御 デバイスの予備インターフェイスを使用する方法があります。ブリッジグループのメンバーインターフェイスにエンドポイントを直接接続できます。また、BVI と同じネットワークにより多くのエンドポイントを追加するために、スイッチを接続できます。

管理/診断インターフェイス

管理インターフェイス

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Device Manager 管理、スマートライセンス、およびデータベースの更新に使用されます。または、管理インターフェイスの代わりにデータインターフェイスを使用して Threat Defense デバイスを管理できます。管理インターフェイスでは、独自の Linux IP アドレスとスタティックルーティングが使用されます。管理インターフェイスは、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]**ページで、または **configure network** コマンドを使用して CLI で設定できます。

ハードウェアデバイスの場合、管理インターフェイスを設定する一つの方法は、ポートをネットワークに接続しないことです。代わりに、管理 IP アドレスのみを設定し、インターネットからの更新情報を得るためのゲートウェイとして、データインターフェイスを使用するように設定します。次に、HTTPS/SSH トラフィック（デフォルトで HTTPS は有効）への内部インターフェイスを開き、内部 IP アドレスを使用して Device Manager を開きます（管理アクセスリストの設定 （924 ページ） を参照）。

Threat Defense Virtual の推奨設定は、Management0/0 を内部インターフェイスと同じネットワークに接続し、内部インターフェイスをゲートウェイとして使用することです。

診断インターフェイス（レガシー）

7.3 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。

7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。

7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージするか、別の診断インターフェイスを引き続き使用できます。診断インターフェイスのサポートは今後のリリースで削除されるため、できるだけ早くインターフェイスをマージする必要があります。管理インターフェイスと診断インターフェイスを手動でマージするには、管理インターフェイスと診断インターフェイスのマージ（369ページ）を参照してください。自動マージを防止する設定には、次のものが含まれます。

- 「管理」という名前のデータインターフェイス。この名前は、マージされた管理インターフェイスで使用するために予約されています。
- 診断の IP アドレス
- 診断で有効な DNS
- Syslog、または RADIUS（リモートアクセス VPN 用）送信元インターフェイスが診断
- 送信元インターフェイスが指定されておらず、管理専用（診断を含む）として設定されているインターフェイスが少なくとも 1 つある AD または RADIUS（リモートアクセス VPN 用）。これらのサービスのデフォルトルートルックアップは、管理専用ルーティングテーブルからデータルーティングテーブルに変更されていて、管理にフォールバックされません。したがって、管理専用インターフェイスを使用するには、ルートルックアップに依存する代わりに、その特定のインターフェイスを選択する必要があります。
- スタティックルートまたは診断の SLA モニタ
- 診断を使用した FlexConfig
- 診断用の DDNS

レガシー診断インターフェイスの動作の詳細については、このガイドの 7.3 バージョンを参照してください。

個別の管理ネットワークの設定に関する推奨事項

（ハードウェアデバイス）分離した管理ネットワークを使用する場合は、物理的管理インターフェイスをスイッチまたはルータに有線で接続します。

Threat Defense Virtual では、Management0/0 を任意のデータ インターフェイスから個別のネットワークに接続します。デフォルトの IP アドレスを使用している場合、管理 IP アドレスまた

は内部インターフェイス IP アドレスは同一サブネット上にあるため、いずれかを変更する必要があります。

次に、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** を選択し、管理インターフェイスを編集して、接続されたネットワークで IPv4 アドレスまたは IPv6 アドレス（あるいはその両方）を設定します。必要に応じて、ネットワーク上の他のエンドポイントに IPv4 アドレスを指定するように DHCP サーバーを設定できます。管理ネットワーク上にインターネットへのルートを持つルータがある場合、それをゲートウェイとして使用します。なければ、データインターフェイスをゲートウェイとして使用します。

セキュリティ ゾーン

各インターフェイスは単一のセキュリティ ゾーンに割り当てることができます。ゾーンに基づいてセキュリティ ポリシーを適用されます。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。

各ゾーンにはインターフェイスのモードに直接関係するモードがあります。インターフェイスは、同じモードのセキュリティゾーンにのみ追加できます。

ブリッジ グループでは、メンバー インターフェイスをゾーンに追加できますが、ブリッジ仮想インターフェイス（BVI）を追加することはできません。

ゾーンにManagementインターフェイスは含めないでください。ゾーンは、データインターフェイスにのみ適用されます。

セキュリティ ゾーンは [オブジェクト（Objects）] ページで作成できます。

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、各メンバーインターフェイスではなくブリッジ仮想インターフェイス（BVI）上でグローバルアドレスを設定します。次のいずれかをグローバル アドレスとして指定することはできません。
  - 内部で予約済みの IPv6 アドレス：fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - 未指定のアドレス（::/128 など）
  - ループバック アドレス（::1/128）
  - マルチキャスト アドレス（ff00::/8）
  - リンクローカル アドレス（fe80::/10）

- 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およびネイバー探索などのネットワーク検出機能に使用できます。ブリッジ グループでは、BVI で IPv6 を有効にすると、自動的に各ブリッジ グループのメンバー インターフェイスのリンクローカル アドレスが設定されます。リンクローカルアドレスがセグメントでのみ使用可能であり、インターフェイスMACアドレスに接続されているため、各インターフェイスは独自のアドレスを持つ必要があります。

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。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。

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。

インターフェイスに関する注意事項と制約事項

ここでは、インターフェイスに関する制限事項について説明します。

インターフェイス設定の制限事項

Device Manager を使用してデバイスを設定する場合、インターフェイス設定に関するいくつかの制限があります。次の機能のいずれかが必要である場合、デバイスを設定するために Management Centerを使用する必要があります。

- ルーテッド ファイアウォール モードのみがサポートされます。トランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- パッシブ インターフェイスの設定は可能ですが、ERSPAN インターフェイスを設定することはできません。
- 冗長インターフェイスは設定できません。

- Device Manager で EtherChannel を設定できるモデルは、Firepower 1000、Firepower 2100、Cisco Secure Firewall 3100、ISA 3000 です。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。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。
- 追加できるブリッジ グループは 1 つだけです。
- Threat Defense は、ルーテッドインターフェイスでのみ IPv4 PPPoE をサポートします。PPPoE は、ハイアベイラビリティ ユニットではサポートされません。

デバイス モデルによる VLAN サブインターフェイスの最大数

デバイスモデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データ インターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。

次の表で、各デバイス モデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 1010	60
Firepower 1120	512
Firepower 1140、1150	1024
Firepower 2100	1024
Cisco Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
Threat Defense Virtual	50
ISA 3000	100

物理インターフェイスの設定

少なくとも、使用する物理インターフェイスは有効にする必要があります。通常は名前も付けて、IP アドレッシングを設定します。VLAN サブインターフェイスを設定する予定の場合、パッシブ モード インターフェイスを設定している場合、またはインターフェイスをブリッジ グループに追加する予定の場合は、IP アドレッシングを設定しません。 Firepower 4100/9300 EtherChannel は、単一の物理インターフェイスとともに Device Manager の [インターフェイス（Interfaces）]ページに表示され、この手順はそれらの EtherChannel にも適用されます。シャー

シ上の FXOS で、Firepower 4100/9300 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。

（注） 物理インターフェイスを Firepower 1010 スイッチポートとして設定するには、VLAN インターフェイスおよびスイッチポートの設定（Firepower 1010）（320 ページ）を参照してください。

物理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するには、パッシブ モードでの物理インターフェイスの設定 （344 ページ）を参照してください。

接続されたネットワークでの送信を一時的に防ぐために、インターフェイスを無効にできます。インターフェイスの設定を削除する必要はありません。

手順

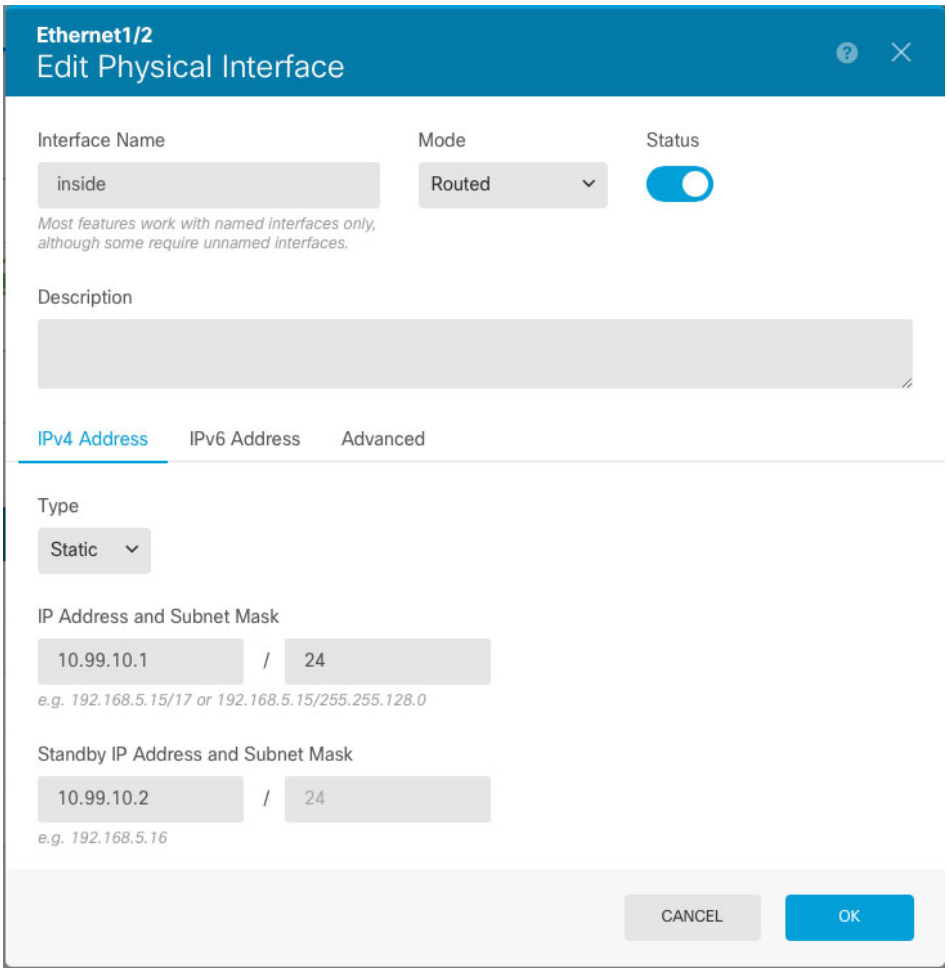
ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 編集する物理インターフェイスの [編集（edit）] アイコン（）をクリックします。

高可用性設定でフェールオーバー リンクまたはステートフル フェールオーバー リンクとして使用しているインターフェイスを編集することはできません。

ステップ 3 次の設定を行います。



a) [インターフェイス名（Interface Name）] を設定します。

インターフェイスの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。**注**：EtherChannel に追加するインターフェイスの名前は設定しないでください。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード（Mode）]を選択します。

- [ルーテッド（Routed）]：ルーテッド モード インターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォール ポリシーなど、すべてのファイアウォール機能の管理下に置かれます。これが通常のインターフェイス モードです。

- [インライン（Inline）]：インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。インラインセットで使用するインターフェイスを編集する場合は、初期モードとして**ルーテッド**モードを選択し、どのタイプのIPアドレッシングも設定しないでください。
- [パッシブ（Passive）]：パッシブ インターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワーク中のトラフィック フローをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、パッシブモードでの物理インターフェイスの設定 （344 ページ）を参照してください。パッシブインターフェイスには IP アドレスを設定できません。
- [Switch Port]：（Firepower 1010）スイッチポートは、同じ VLAN 上のポート間でのハードウェアスイッチングを可能にします。スイッチングされたトラフィックはセキュリティポリシーの対象にはなりません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、次を参照してください。VLANインターフェイスおよびスイッチポートの設定（Firepower 1010） （320 ページ）

後でこのインターフェイスをブリッジ グループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

Firepower 4100/9300 デバイス上のインターフェイスの場合は、FXOS でもインターフェイスを有効にする必要があります。

この物理インターフェイスのサブインターフェイスを設定する予定の場合、すでに設定している可能性が高いです。[保存（Save）] をクリックして、VLAN サブインターフェイスと 802.1Q トランキングの設定（334ページ）に進みます。保存しない場合は、次に進みます。

（注） サブインターフェイスを設定している場合でも、インターフェイスに名前を付けて、IPアドレスを指定できます。これは一般的な設定ではありませんが、必要だとわかっている場合は設定できます。

d) （任意） [説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注） インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定（934 ページ）を参照してください。

- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択したグループ名を指定します。
  - [PPPoEユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoEパスワード（PPPoE Password）]：ISP によって提供されたパスワードを指定します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

    PAP は認証時にクリアテキストのユーザ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。

- [PPPoEの学習済みルートメトリック（PPPoE Learned Route Metric）]：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ます。有効な値は1～255です。デフォルトでは、学習したルートのアドミニストレーティブディスタンスは1です。
- [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoEサーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IPアドレスタイプ（IP Address Type）]：PPPoEサーバからIPアドレスを取得するには、[動的（Dynamic）]を選択します。ISPから静的IPアドレスが割り当てられている場合は、[静的（Static）]を選択することもできます。

ステップ5 （オプション）[IPv6アドレス（IPv6 Address）]タブをクリックして、IPv6アドレスを設定します。

- [状態（State）]：グローバルアドレスを設定しない場合にIPv6処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）]を選択します。リンクローカルアドレスはインターフェイスのMACアドレス（*Modified* EUI-64形式）に基づいて生成されます。

  （注） IPv6を無効にしても、明示的なIPv6アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスのIPv6処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6ステートレス自動設定では、デバイスが存在するリンクで使用するIPv6グローバルプレフィックスのアドバタイズメントなどの、IPv6サービスを提供するようにルータが設定されている場合に限り、グローバルなIPv6アドレスが生成されます。IPv6ルーティングサービスがリンクで使用できない場合、リンクローカルIPv6アドレスのみが取得され、そのデバイスが属するネットワークリンクの外部にはアクセスできません。リンクローカルアドレスはModified EUI-64インターフェイスIDに基づいています。

  RFC 4862では、ステートレス自動設定用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されていますが、この場合は、Threat Defenseデバイスがルータアドバタイズメントメッセージを送信します。メッセージを抑制して、RFCに準拠するためには、[RAを抑制（Suppress RA）]を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティックグローバルIPv6アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力しま

す。IPv6アドレッシングの詳細については、IPv6アドレス指定（291ページ）を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）]オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

（注） 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。例、fe80::20d:88ff:feee:6a82。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。

- [スタンバイIPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。
- [RAを抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Threat Defenseはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  Threat Defense デバイスで 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抑制できます。

ステップ 6 （任意）詳細オプションの設定（350ページ）。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 **[OK]** をクリックします。

次のタスク

- インターフェイスを適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定（167 ページ） を参照してください。

- ダイナミック DNS サービスプロバイダーに完全修飾ドメイン名（FQDN）を登録し、DNS サーバの IPv4 と IPv6 の両方のインターフェイスアドレスが更新されるように DDNS を設定します。ダイナミック DNS（DDNS）の設定 （939 ページ） を参照してください。

管理インターフェイスの設定

管理インターフェイスは、[インターフェイス（Interface）] ページのデータインターフェイスとともに表示される特別なインターフェイスですが、データインターフェイスとしては動作しません。管理インターフェイスには次の使用法があります。

- IP アドレスへの Web および SSH 接続を開き、インターフェイスからデバイスを設定できます。
- システムはこの IP アドレスを使用してスマート ライセンスおよびデータベースの更新情報を取得します。
- このインターフェイスは syslog にも使用できます。

CLI セットアップ ウィザードを使用すると、システムの初期設定時にデバイスの管理アドレスとゲートウェイを設定します。Device Manager のセットアップウィザードを使用すると、管理アドレスとゲートウェイはデフォルトのまま変更されません。

必要に応じて、Device Manager でこれらのアドレスを変更できます。**configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用して、CLI で管理アドレスおよびゲートウェイを変更することもできます。デフォルトの管理インターフェイス設定に戻すには、**configure network** {**ipv4** | **ipv6**} **dhcp-dp-route** コマンドを使用します。

管理ネットワーク上の他のデバイスが DHCP サーバーとして機能している場合、スタティックアドレスを定義するか、または DHCP を介してアドレスを取得できます。 ほとんどのプラットフォームでは、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得します。

注意 現在接続されているアドレスを変更した場合は、その変更がすぐに適用されるため、変更の保存と同時に Device Manager （または CLI）にアクセスできなくなります。デバイスに接続し直す必要があります。新しいアドレスが管理ネットワークで使用できることを確認します。

始める前に

7.4以降にアップグレードしていて、管理インターフェイスと診断インターフェイスをまだマージしていない場合は、管理インターフェイスと診断インターフェイスのマージ （369ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[デバイス] > [インターフェイス] リンクをクリックします。 >

ステップ 2 管理インターフェイスを編集します。

ステップ 3 管理**ゲートウェイ**の定義方法を選択します。

ゲートウェイは、システムがインターネット経由でスマートライセンスとデータベース更新（VDB、ルール、地理位置情報、URL など）を取得し、管理 DNS サーバと NTP サーバに到達する方法を決定します。次のオプションから選択します。

静的 IP オプション：

- [データインターフェイスをゲートウェイとして使用（Use the Data Interfaces as the Gateway）]：管理インターフェイスに別の管理ネットワークが接続されていない場合、このオプションを選択します。トラフィックは、ルーティングテーブルに基づいてインターネットにルーティングされ、通常は、外部インターフェイスを通過します。このオプションは Threat Defense Virtual デバイスではサポートされません。
- [管理インターフェイスに固有のゲートウェイを使用（Use Unique Gateways for the Management Interface）]：管理インターフェイスに接続されている別の管理ネットワークがある場合、IPv4 および IPv6 に固有のゲートウェイ（以下）を指定します。

DHCP IP オプション：

- [データインターフェイスへのフォールバックが可能な管理インターフェイス用に一意のゲートウェイを使用（Use Unique Gateways for the Management Interface with Fallback to Data Interfaces）]：DHCP サーバがゲートウェイを提供する場合、システムは管理インターフェイスを介してゲートウェイに管理トラフィックをルーティングします。DHCP サーバがゲートウェイを提供しない場合、システムはデータ インターフェイス ルーティング テーブルに基づいて管理トラフィックをルーティングし、通常は外部インターフェイスを介してトラフィックを送信します。このオプションは Threat Defense Virtual デバイスではサポートされません。
- [管理インターフェイス用に一意のゲートウェイを使用（フォールバックなし）（Use Unique Gateways for the Management Interface (no Fallback)）]：システムは、DHCP サーバの提供するゲートウェイに管理インターフェイスを介して管理トラフィックをルーティングします。DHCP サーバがゲートウェイを提供しない場合、システムが到達できるのは管理インターフェイスのローカルホストのみになります。データインターフェイスを介してルーティングするには、[フォールバック（Fallback）] オプションを選択します。

ステップ 4 **IPv4** または **IPv6** 管理アドレス、サブネットマスクか IPv6 プレフィックス、および必要に応じてゲートウェイを設定します。

少なくとも 1 組のプロパティを設定する必要があります。1 組は空白にし、そのアドレッシング方式を無効にします。

- 静的 IP アドレスを設定するには、[タイプ（Type）] > [静的（Static）]を選択します。 >

- **[タイプ（Type）] > [DHCP]** を選択し、DHCP または IPv6 自動設定によってアドレスおよびゲートウェイを取得します。

ステップ 5 （任意） スタティック **IPv4** アドレスを設定する場合は、インターフェイスで DHCP サーバーを設定します。

管理インターフェイスで DHCP サーバーを設定すると、管理ネットワークのクライアントは DHCP プールからアドレスを取得できます。このオプションは Threat Defense Virtual デバイスではサポートされません。

a) **[DHCPサーバを有効化（Enable DHCP Server）] > [オン（On）]**をクリックします。
b) サーバーの [アドレスプール（Address Pool）] を入力します。

アドレスプールとは、アドレスを要求するクライアントに対してサーバーが提供できる、最小から最大までの IP アドレスの範囲です。IP アドレスの範囲は管理アドレスと同じサブネット上にある必要があり、次のものを含めることはできません：インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネットのネットワーク アドレス。プールに開始/終了アドレスをハイフンで区切って指定します。たとえば、192.168.45.46-192.168.45.254 などです。

ステップ 6 [詳細設定（Advanced）] ページで、IPv4の場合は 8ー1500、IPv6 を有効にした場合は 1280ー1500 の管理インターフェイスの **MTU** を設定します。

デフォルト値は 1500 バイトです。

ステップ 7 [保存（Save）] をクリックして警告を読み、[OK] をクリックします。

ブリッジ グループの設定

ブリッジ グループは 1 つ以上のインターフェイスをグループ化する仮想インターフェイスです。インターフェイスをグループ化する主な理由は、スイッチドインターフェイスのグループを作成することにあります。そのため、ブリッジグループに含まれているインターフェイスにワークステーションやその他のエンドポイントデバイスを直接接続できます。それらは別の物理スイッチを介して接続する必要はありませんが、スイッチをブリッジ グループ メンバーに接続することもできます。

グループ メンバーには IP アドレスはありません。代わりに、すべてのメンバー インターフェイスがブリッジ仮想インターフェイス（BVI）の IP アドレスを共有します。BVI で IPv6 を有効にすると、メンバー インターフェイスには一意のリンクローカル アドレスが自動的に割り当てられます。

メンバーインターフェイスは個別に有効または無効にします。そのため、未使用のインターフェイスはブリッジ グループから削除することなく無効化できます。ブリッジ グループ自体は常に有効になっています。

通常は、メンバー インターフェイス経由で接続されているエンドポイントの IP アドレスを提供するブリッジグループ インターフェイス（BVI）にDHCPサーバーを設定します。ただし、

必要に応じて、メンバー インターフェイスに接続されているエンドポイントにスタティック アドレスを設定できます。ブリッジ グループ内のすべてのエンドポイントには、ブリッジ グループの IP アドレスと同じサブネットの IP アドレスが必要です。

ガイドラインと制約事項

- ブリッジグループを 1 つ追加できます。
- Device Manager 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。
- Firepower 2100 シリーズ または Threat Defense Virtual デバイスにブリッジ グループを設定することはできません。
- 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。
- ISA 3000 は、ブリッジグループ BVI1 を使用して事前に設定されています（名前は付けられていません。これは、ルーティングに参加しないことを意味します）。BVI1 にはすべてのデータインターフェイス（GigabitEthernet1/1（outside1）、GigabitEthernet1/2（inside1）、GigabitEthernet1/3（outside2）、および GigabitEthernet1/4（inside2））が含まれます。ネットワークに合わせて BVI1 IP アドレスを設定する必要があります。

始める前に

ブリッジグループのメンバーになるインターフェイスを設定します。具体的には、各メンバーインターフェイスは、次の要件を満たしている必要があります。

- インターフェイスには名前が必要です。
- 静的に、または DHCP を介してインターフェイス用に定義された IPv4 または IPv6 アドレスは設定できません。現在使用しているインターフェイスからアドレスを削除する必要がある場合、そのインターフェイスのその他の設定（アドレスを持つインターフェイスに依存するスタティック ルート、DHCP サーバー、NAT ルールなど）も削除する必要がある場合があります。
- インターフェイスをブリッジ グループに追加する前に、セキュリティ ゾーン（ゾーン内にある場合）からそのインターフェイスを削除し、そのインターフェイスのすべての NAT ルールを削除する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、[ブリッジグループ（Bridge Groups）] をクリックします。

ブリッジグループのリストに、既存のブリッジグループが表示されます。各ブリッジグループのメンバーインターフェイスを表示するには、開/閉矢印をクリックします。また、メンバー

インターフェイスは[インターフェイス（Interfaces）]または[VLAN（VLANs）]ページでも個別に表示されます。

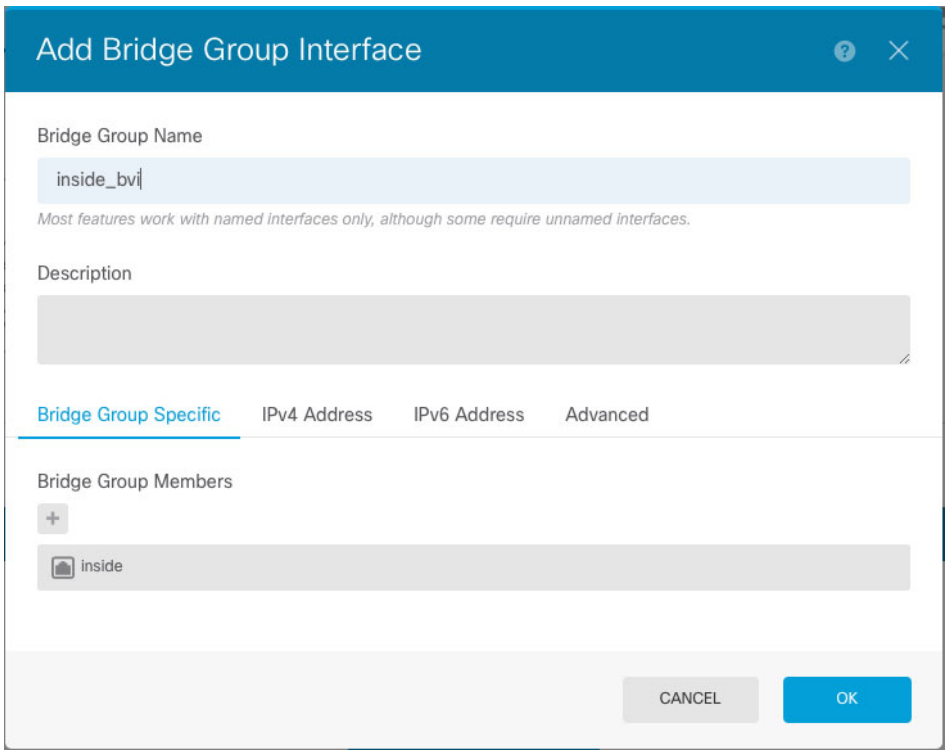
ステップ 2 次のいずれかを実行します。

- BVI1 ブリッジ グループの編集アイコン（）をクリックします。
- [ブリッジグループの作成（Create Bridge Group）] をクリックするか、プラス アイコン（）をクリックして、新しいグループを作成します。

  （注） ブリッジ グループは 1 つ設定できます。ブリッジ グループをすでに定義している場合は、新しいグループ作成するのではなく、そのグループを編集する必要があります。新しいブリッジグループを作成する必要がある場合は、まず既存のブリッジ グループを削除する必要があります。

- 不要になったブリッジ グループの [削除（delete）] アイコン（）をクリックします。ブリッジ グループを削除すると、そのメンバーは標準のルーテッド インターフェイスになり、NAT ルールまたはセキュリティ ゾーンのメンバーシップはすべて維持されます。インターフェイスを編集して、IP アドレスを付与できます。新しいブリッジ グループにそれらのインターフェイスを追加する場合は、まず NAT ルールを削除し、インターフェイスをセキュリティ ゾーンから削除する必要があります。

ステップ 3 次を設定します。



a) （任意）[インターフェイス名（Interface Name）] を設定します。

ブリッジグループの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。この BVI を他の名前付きインターフェイス間のルーティングに参加させる場合は、名前を設定します。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) （任意）[説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

c) [ブリッジグループメンバー（Bridge Group Members）] のリストを編集します。

1 つのブリッジ グループに最大 64 個のインターフェイスまたはサブインターフェイスを追加できます。

- インターフェイスの追加：プラスアイコン（+）をクリックし、1 つ以上のインターフェイスをクリックし、[OK] をクリックします。
- インターフェイスの削除：対象にカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。ブリッジ グループの IP アドレスとサブネット マスクを入力します。接続されているエンドポイントはすべて、このネットワーク上に存在することになります。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注） インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定（934 ページ）を参照してください。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバーからアドレスを取得する必要がある場合は、このオプションを選択します。これはブリッジ グループの一

般的なオプションではありませんが、必要に応じて設定できます。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。

- [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
- [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカル アドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクローカル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

  （注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定（291 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注） 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。例、fe80::20d:88ff:feee:6a82。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。

- [スタンバイ IP アドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RAを抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Threat Defense デバイスはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  Threat Defense デバイスで 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抑制できます。

ステップ 6 （任意）詳細オプションの設定 （350 ページ）。

ブリッジ グループ メンバー インターフェイスに対して最も詳細なオプションを設定しますが、一部はブリッジ グループ インターフェイスでも使用できます。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 [OK] をクリックします。

次のタスク

- 使用する予定のすべてのメンバー インターフェイスが有効になっていることを確認します。
- ブリッジ グループの DHCP サーバを設定します。DHCP サーバの設定 （934 ページ）を参照してください。
- メンバー インターフェイスを適切なセキュリティ ゾーンに追加します。セキュリティ ゾーンの設定 （167 ページ）を参照してください。
- アイデンティティ、NAT、アクセスなどのポリシーにより、ブリッジ グループとメンバー インターフェイスに必要なサービスが提供されることを確認します。

EtherChannel の設定

ここでは、EtherChannel とそれらの設定方法について説明します。

（注） 次のモデルでは、Device Manager で EtherChannel を追加できます。

- Firepower 1000
- Firepower 2100
- Cisco Secure Firewall 3100
- ISA 3000

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。 Firepower 4100/9300の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。また、Threat Defense Virtual などの他のモデルでは、Device Manager で EtherChannel を設定できません。

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 グループは、最大 8 個のアクティブ インターフェイスを設定できます。

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。

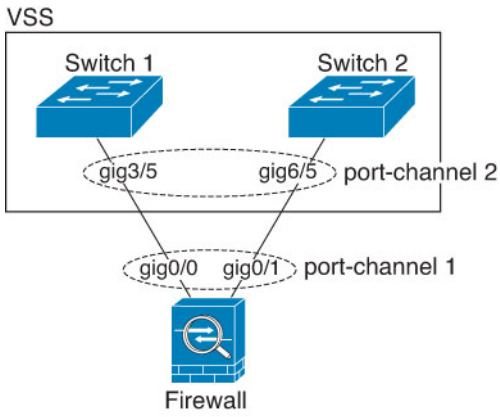
別のデバイスの EtherChannel への接続

Threat Defense 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 Threat Defense 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。

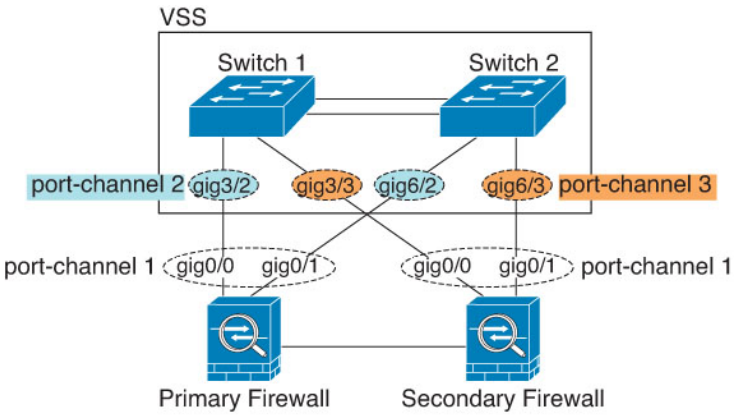
図 *12 : VSS/vPC* への接続



（注） Threat Defense デバイスがトランスペアレント ファイアウォール モードになっており、2 組の VSS/vPC スイッチ間に Threat Defense デバイスを配置する場合は、EtherChannel 内で Threat Defense デバイス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。

Threat Defense デバイスをアクティブ/スタンバイフェールオーバー展開で使用する場合、Threat Defense デバイスごとに 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 Threat Defense デバイスで、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 Threat Defense デバイスに接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の Threat Defense 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 Threat Defense デバイスに送信しないようにするためです。

図 *13*：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。
- 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

Threat Defense デバイスは、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。

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。

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。

Firepower および Secure Firewall ハードウェア

ポートチャネル インターフェイスは、内部インターフェイスの内部データ 0/1 の MAC アドレスを使用します。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。シャーシ上のすべての EtherChannel インターフェイスは同じ MAC アドレスを使用するため、たとえば、SNMP ポーリングを使用する場合、複数のインターフェイスが同じ MAC アドレスを持つことに注意してください。

（注） メンバーインターフェイスは、再起動後に内部データ 0/1 MAC アドレスのみを使用します。再起動する前に、メンバーインターフェイスは独自の MAC アドレスを使用するた再起動後に新しいメンバーインターフェイスを追加する場合、MAC アドレスを更新するためにもう一度再起動する必要があります。

EtherChannel インターフェイスのガイドライン

ブリッジ グループ

Device Manager 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。

高可用性

- EtherChannel インターフェイスを 高可用性 リンクとして使用する場合、高可用性 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 高可用性 リンク自体が必要であるためです。
- EtherChannel 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。

- 高可用性の EtherChannel インターフェイスをモニターできます。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、デバイスレベルの高可用性をモニタしているときには、EtherChannel 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 インターフェイスを高可用性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。高可用性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、高可用性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 高可用性 が発生することはありません。

モデルのサポート

- 次のモデルでは、Device Manager で EtherChannel を追加できます。
  - Firepower 1000
  - Firepower 2100
  - Cisco Secure Firewall 3100
  - ISA 3000

  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。 Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。また、ASA 5500-X シリーズなどの他のモデルでは、Device Manager で EtherChannel を設定できません。
- 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。

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 グループは、最大 8 個のアクティブ インターフェイスを設定できます。
- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。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。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、CIsico Secure Firewall 3100 の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。

- Threat Defense 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。
- Threat Defense デバイスは、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 タギングを有効にすると、Threat Defense デバイスはタグ付きの 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。
- 次のデバイスモデルは、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。
  - Firepower 1000
  - Firepower 2100
  - Cisco Secure Firewall 3100
- 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 Threat Defense 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、Threat Defense 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 Threat Defense コンフィギュレーションは、メンバー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 の追加

EtherChannel を追加して、メンバーインターフェイスを割り当てます。

（注） 次のモデルでは、Device Manager で EtherChannel を追加できます。

- Firepower 1000
- Firepower 2100
- Cisco Secure Firewall 3100
- ISA 3000

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。 Firepower 4100/9300の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。また、ASA 5500-X シリーズなどの他のモデルでは、Device Manager で EtherChannel を設定できません。

始める前に

- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。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。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、CIsico Secure Firewall 3100 の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。
- メンバーインターフェイスに名前を付けることはできません。

注意 コンフィギュレーション内で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。

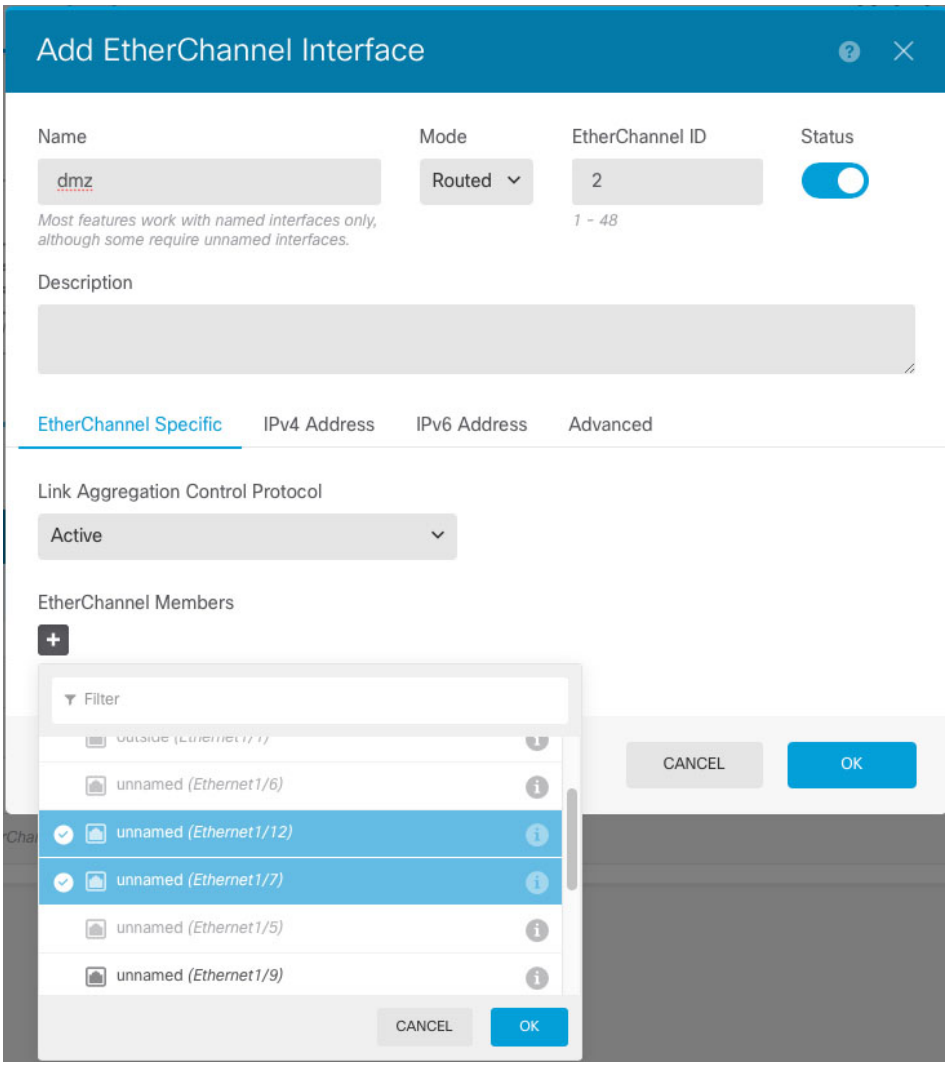
手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、[EtherChannel（EtherChannels）] をクリックします。

[EtherChannel] リストには、既存の EtherChannel、それらの名前、アドレス、および状態が表示されます。各 EtherChannel のメンバーインターフェイスを表示するには、開/閉矢印をクリックします。メンバーインターフェイスは[インターフェイス（Interfaces）] ページにも個別に表示されます。

ステップ 2 [EtherChannelの作成（Create EtherChannel）] をクリックするか（現在の EtherChannel がない場合）、またはプラス アイコン（+）をクリックして [EtherChannel] をクリックし、新しい EtherChannel を作成します。

ステップ 3 次を設定します。



a) [インターフェイス名（Interface Name）] を設定します。

EtherChannel の名前を 48 文字以内で設定します。英字は小文字にする必要があります。例、[inside] または [outside]。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード（Mode）] を設定します。

- [ルーテッド（Routed）]：ルーテッドモードインターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォール ポリシーなど、すべてのファイアウォール機能の管理下に置かれます。トラフィックがインターフェイスを経由するようにする場合は、このモードを使用します。これが通常のインターフェイス モードです。
- [インライン（Inline）]：インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。インラインセットで使用するインターフェイスを編集する場合は、初期モードとして**ルーテッド**モードを選択し、どのタイプの IP アドレッシングも設定しないでください。
- [パッシブ（Passive）]：パッシブ インターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワーク中のトラフィック フローをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、パッシブモードでの物理インターフェイスの設定 （344 ページ）を参照してください。

c) [EtherChannel ID] を 1 ～ 48 の範囲で設定します（Firepower 1010 の場合は 1 ～ 8）。

d) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

e) （任意） [説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

f) [EtherChannelモード（EtherChannel Mode）] を指定します。

- [アクティブ（Active）]：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（On）]：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。

g) [EtherChannel メンバー（EtherChannel Members）] を追加します。

EtherChannel には、最大 8 つの（無名）インターフェイスを追加できます。

- インターフェイスの追加：プラスアイコン（+）をクリックし、1 つ以上のインターフェイスをクリックし、[OK] をクリックします。
- インターフェイスの削除：対象にカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注） インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定 （934 ページ）を参照してください。
- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択したグループ名を指定します。
  - [PPPoEユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoEパスワード（PPPoE Password）]：ISP によって提供されたパスワードを指定します。

- [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

  PAP は認証時にクリアテキストのユーザ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。

- [PPPoEの学習済みルートメトリック（PPPoE Learned Route Metric）]：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ます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブディスタンスは 1 です。

- [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。

- [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクローカル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

  （注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  RFC 4862 では、ステートレス自動設定用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されていますが、この場合は、Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6アドレッシングの詳細については、IPv6アドレス指定（291ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注） 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。例、fe80::20d:88ff:feee:6a82。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。

- [スタンバイIPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RAを抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Threat Defenseはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  Threat Defense デバイスで 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抑制できます。

ステップ 6 [詳細（Advanced）] をクリックし、速度を設定して、メンバーインターフェイスの速度を設定します。

その他の高度なオプションを設定することもできます。詳細オプションの設定（350ページ）を参照してください。

ステップ 7 [OK] をクリックします。

次のタスク

- EtherChannel を適切なセキュリティゾーンに追加します。セキュリティゾーンの設定（167ページ） を参照してください。

VLAN インターフェイスおよびスイッチポートの設定（Firepower 1010）

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。ここでは、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、VLAN へのスイッチ ポートの割り当てなど、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、この項では、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 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。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。また、これらのインターフェイスを IPS 専用（パッシブインターフェイス）に設定することもできます。
- 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、Threat Defense 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、IPS 専用インターフェ

イス（インラインセットおよびパッシブインターフェイス）、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、Threat Defense デバイスは 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 Threat Defense 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、ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

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。

（注） PoE は Firepower 1010E ではサポートされていません。

Firepower 1010 スイッチ ポートの注意事項と制約事項

高可用性

- 高可用性を使用する場合は、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。高可用性は、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 高可用性 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、高可用性 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：

- 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。詳細オプションの設定 （350 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
- 等コストマルチパス（ECMP）ルーティング
- パッシブインターフェイス
- EtherChannel
- フェールオーバーおよびステートリンク

その他の注意事項と制約事項

- 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。

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。最初に、スイッチポートに割り当てる VLAN ごとに VLAN インターフェイスを設定する必要があります。

（注） 特定の VLAN 上でのスイッチポート間のスイッチングのみを有効にし、VLAN と他の VLAN またはファイアウォール インターフェイス間のルーティングを望まない場合は、VLAN インターフェイス名を空のままにします。この場合、IP アドレスを設定する必要もありません。IP 設定は無視されます。

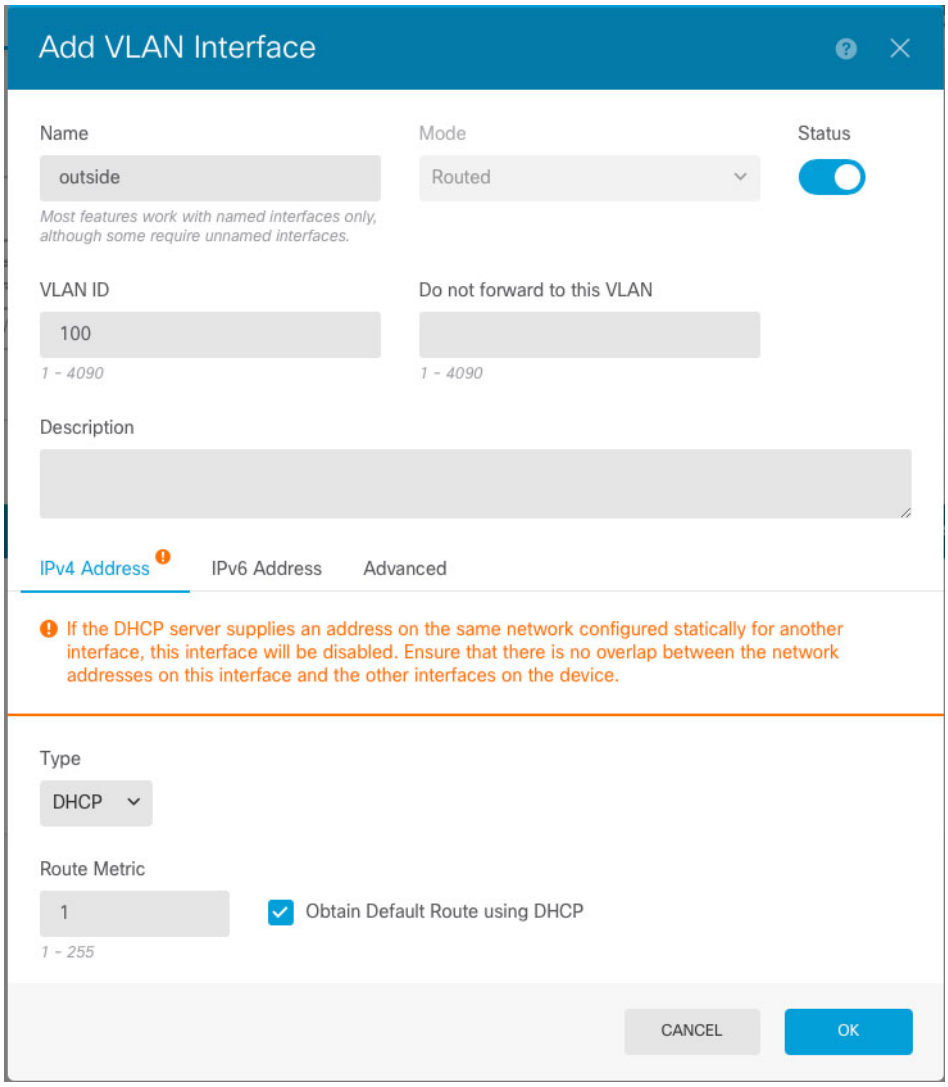
手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックしてから、[VLAN（VLANs）] をクリックします。

VLAN リストには、既存の VLAN インターフェイスが表示されます。各 VLAN に関連付けられているスイッチポートを表示するには、開/閉矢印をクリックします。また、スイッチポートは [インターフェイス（Interfaces）] ページでも個別に表示されます。

ステップ 2 [VLANインターフェイスの作成（Create VLAN Interface）]（現在の VLAN がない場合）またはプラス アイコン（+）をクリックして、新しい VLAN インターフェイスを作成します。

ステップ 3 次を設定します。



a) [インターフェイス名（Interface Name）] を設定します。

VLAN の名前を 48 文字以内で設定します。英字は小文字にする必要があります。例、[inside] または [outside]。

VLANと他のVLANまたはファイアウォールインターフェイス間でルーティングしない場合は、VLANインターフェイス名を空白のままにします。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード（Mode）] は [ルーテッド（Routed）] のままにします。

後でこの VLAN インターフェイスをブリッジグループに追加すると、モードは自動的に **BridgeGroupMember** に変更されます。ブリッジグループのメンバーインターフェイスには、IP アドレスを設定できません。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

d) [VLAN ID] を 1 ～ 4070 の間で設定します。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

e) （任意）[このVLANに転送しない（Do not forward to this VLAN）] フィールドに、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 ID を入力します。

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。

f) （任意）[説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

（注） インターフェイスに対して設定されているDHCPサーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスのIPアドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCPサーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定（934 ページ）を参照してください。

- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスがDSL モデム、ケーブルモデム、またはISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択したグループ名を指定します。
  - [PPPoEユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoEパスワード（PPPoE Password）]：ISPによって提供されたパスワードを指定します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または[MSCHAP] を選択します。

    PAPは認証時にクリアテキストのユーザ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。
  - [PPPoEの学習済みルートメトリック（PPPoE Learned Route Metric）]：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ます。有効な値は1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブディスタンスは1です。
  - [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
  - [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）]を選択します。リンクロー

カル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

（注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  RFC 4862 では、ステートレス自動設定用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されていますが、この場合は、Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定（291 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注） 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。例、fe80::20d:88ff:feee:6a82。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。

- [スタンバイ IP アドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RA を抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるよう

に、Threat Defenseはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

Threat Defense デバイスで 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抑制できます。

ステップ 6 （任意）詳細オプションの設定 （350 ページ）。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 [OK] をクリックします。

次のタスク

- VLAN を適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定（167 ページ） を参照してください。

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。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、Threat Defense デバイスとのすべての接続は、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。

始める前に

アクセスポートを割り当てる VLAN ID に VLAN インターフェイスを追加します。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。「VLAN インターフェイスの設定（322 ページ）」を参照してください。

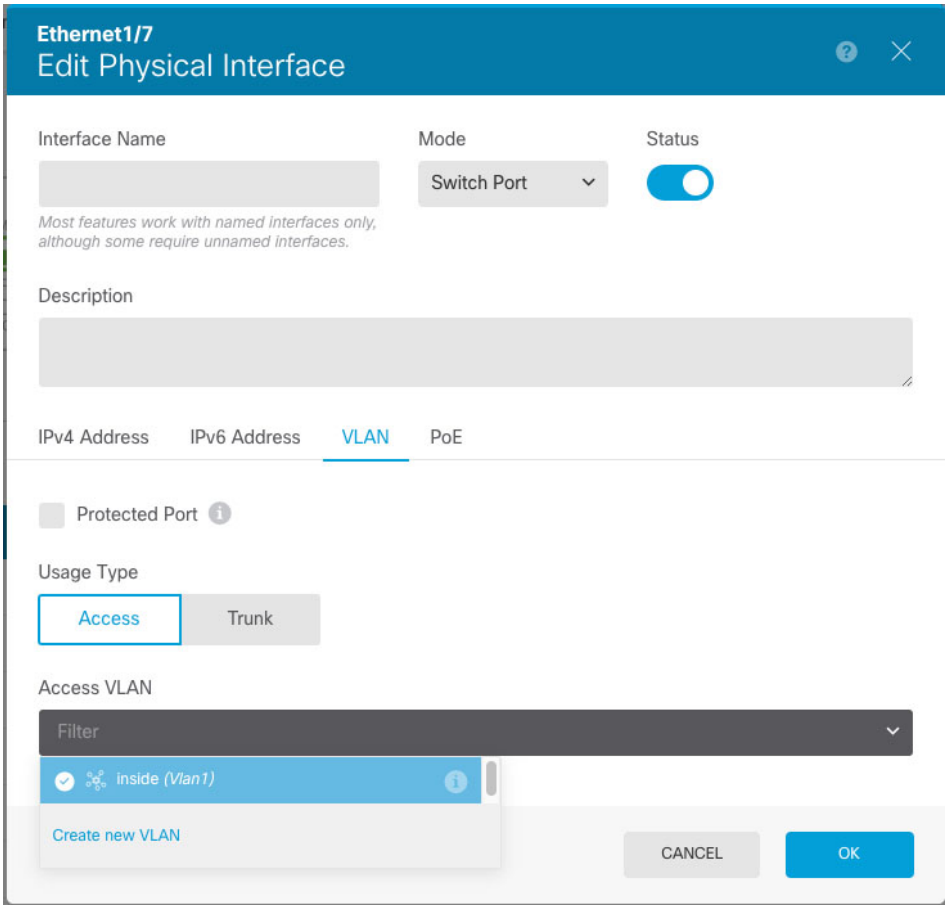
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 編集する物理インターフェイスの [編集（edit）] アイコン（）をクリックします。

ステップ 3 次の設定を行います。



a) スイッチポートの[インターフェイス名（Interface Name）]は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。

b) [モード（Mode）] を [スイッチポート（Switch Port）] に設定します。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（）に設定します。

d) （任意）[説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [VLAN] をクリックして、次のように設定します。

a) （任意） このスイッチポートを保護対象として設定するには、[保護ポート（Protected Port）] チェックボックスをオンにします。これにより、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ぐことができます。

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この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。

b) [使用タイプ（Usage Type）] で、[アクセス（Access）] をクリックします。

c) [アクセスVLAN（Access VLAN）] の場合は、下矢印をクリックして既存の VLAN インターフェイスのいずれかを選択します。

新しい VLAN インターフェイスを追加するには、[新しいVLANの作成（Create new VLAN）] をクリックします。VLAN インターフェイスの設定 （322 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。

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、タグなしトラフィックと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。

始める前に

トランクポートを割り当てる VLAN ID ごとに VLAN インターフェイスを追加します。「VLAN インターフェイスの設定 （322 ページ）」を参照してください。

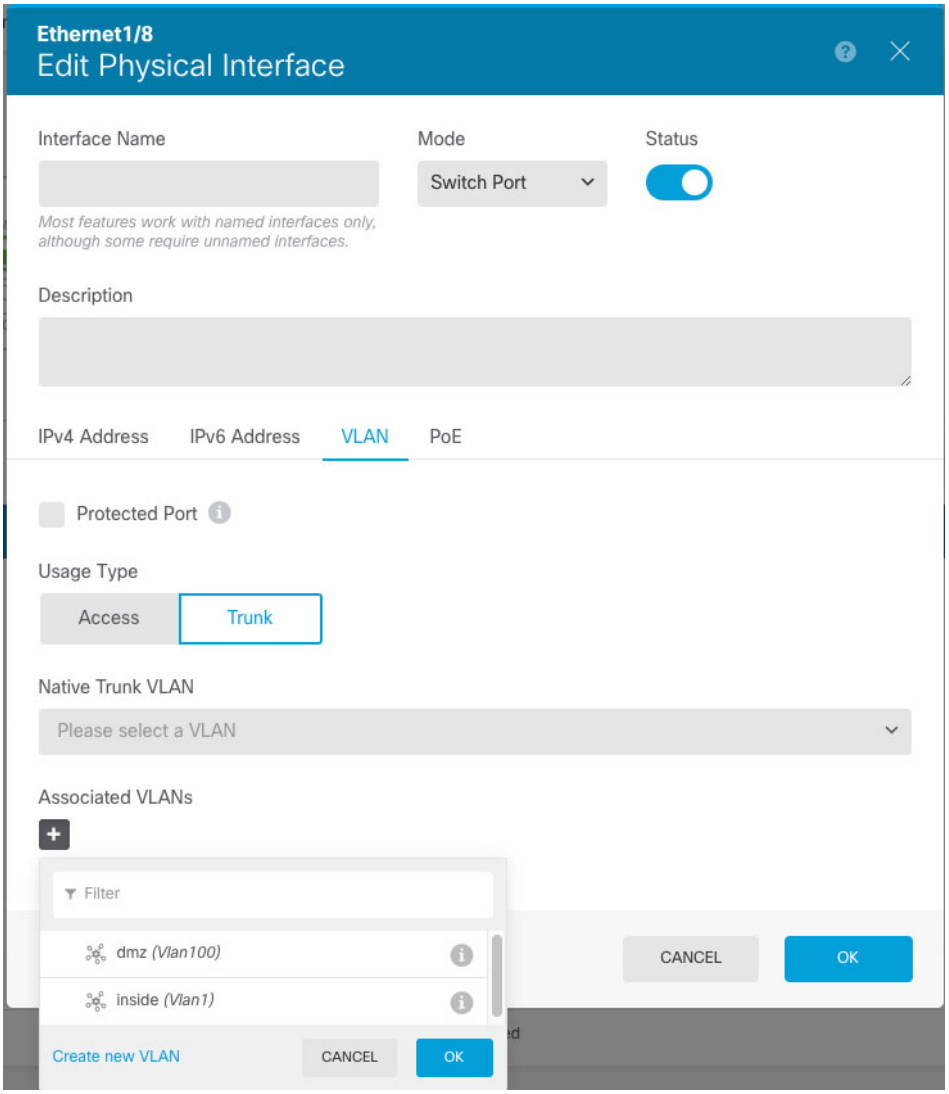
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 編集する物理インターフェイスの [編集（edit）] アイコン（）をクリックします。

ステップ 3 次の設定を行います。



a) スイッチポートの [インターフェイス名（Interface Name）] は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。

b) [モード（Mode）] を [スイッチポート（Switch Port）] に設定します。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（）に設定します。

d) （任意）[説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [VLAN] をクリックして、次のように設定します。

a) （任意） このスイッチポートを保護対象として設定するには、[保護ポート（Protected Port）] チェックボックスをオンにします。これにより、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ぐことができます。

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この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。

b) [使用タイプ（Usage Type）] で、[トランク（Trunk）] をクリックします。

c) （任意） [ネイティブトランク VLAN（Native Trunk VLAN）] の場合は、下矢印をクリックしてネイティブ VLAN の既存の VLAN インターフェイスのいずれかを選択します。

デフォルトのネイティブ VLAN ID は 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。

新しい VLAN インターフェイスを追加するには、[新しい VLAN の作成（Create new VLAN）] をクリックします。「VLAN インターフェイスの設定 （322 ページ）」を参照してください。

d) [関連付けられている VLAN（Associated VLANs）] で、プラス アイコン（+）をクリックして、1 つまたは複数の既存の VLAN インターフェイスを選択します。

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。

新しい VLAN インターフェイスを追加するには、[新しい VLAN の作成（Create new VLAN）] をクリックします。VLAN インターフェイスの設定 （322 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。

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。

（注） PoE は Firepower 1010E ではサポートされていません。

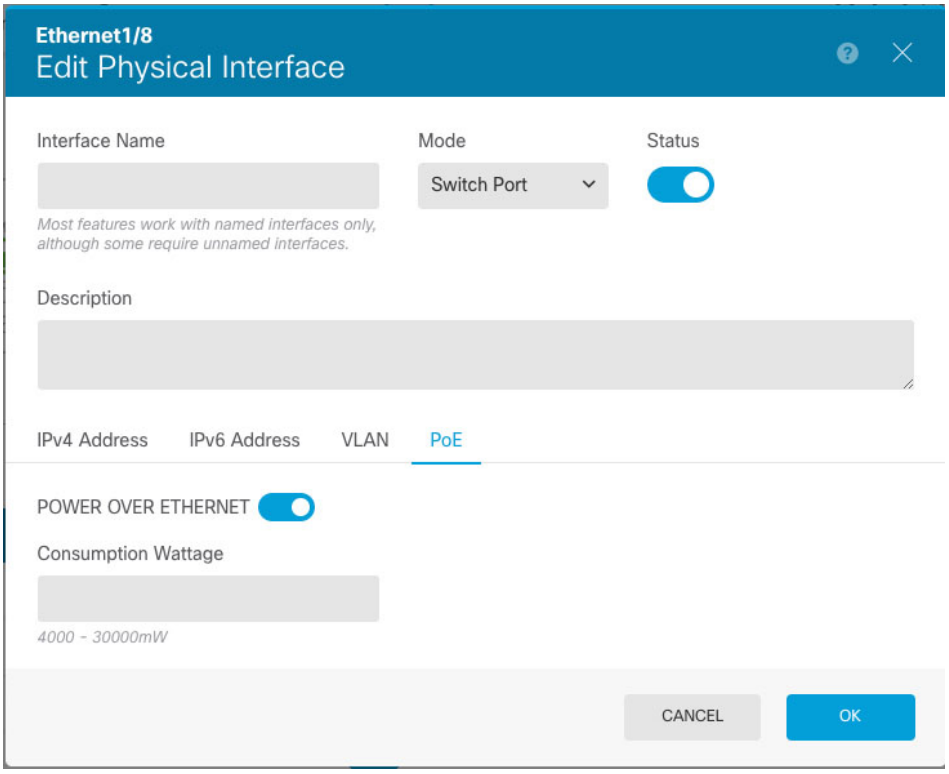
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 Ethernet 1/7 または 1/8 の編集アイコン（）をクリックします。

ステップ 3 [PoE] をクリックして、次のように設定します。



a) [Power Over Ethernet] を有効にするには、スライダ（）をクリックして有効にします。

PoE はデフォルトでイネーブルです。

b) （任意） 必要なワット数を正確に把握している場合は、[消費ワット数（Consumption Wattage）] を入力します。

デフォルトでは、PoE は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。特定のワット数が判明していて、LLDP ネゴシエーションを無効にする場合は、4000 ～ 3 万ミリワットの値を入力します。

ステップ 4 [OK] をクリックします。

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使用すると、物理インターフェイスを異なる VLAN ID が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デバイスを追加しなくても、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。

物理インターフェイスをスイッチのトランク ポートに接続する場合は、サブインターフェイスを作成します。スイッチ トランク ポートで表示できる各 VLAN のサブインターフェイスを作成します。物理インターフェイスをスイッチのアクセス ポートに接続する場合は、サブインターフェイスを作成しても意味がありません。

ガイドラインと制約事項

- 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。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスを有効にする必要があるため、インターフェイスに名前を付けないことでトラフィックを通過させないようにします。物理インターフェイスにタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます。
- Firepower 1010：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。
- 必要に応じて詳細設定を変更することはできますが、ブリッジグループ メンバーインターフェイスの IP アドレスを設定することはできません。
- 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。
- Threat Defense はダイナミック トランキング プロトコル（DTP）をサポートしないため、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と同じ組み込みの MAC アドレスを使用するので、脅威に対する防御デバイス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、脅威に対する防御 デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。EtherChannel にサブインターフェイスを追加するには、[EtherChannel] をクリックします。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

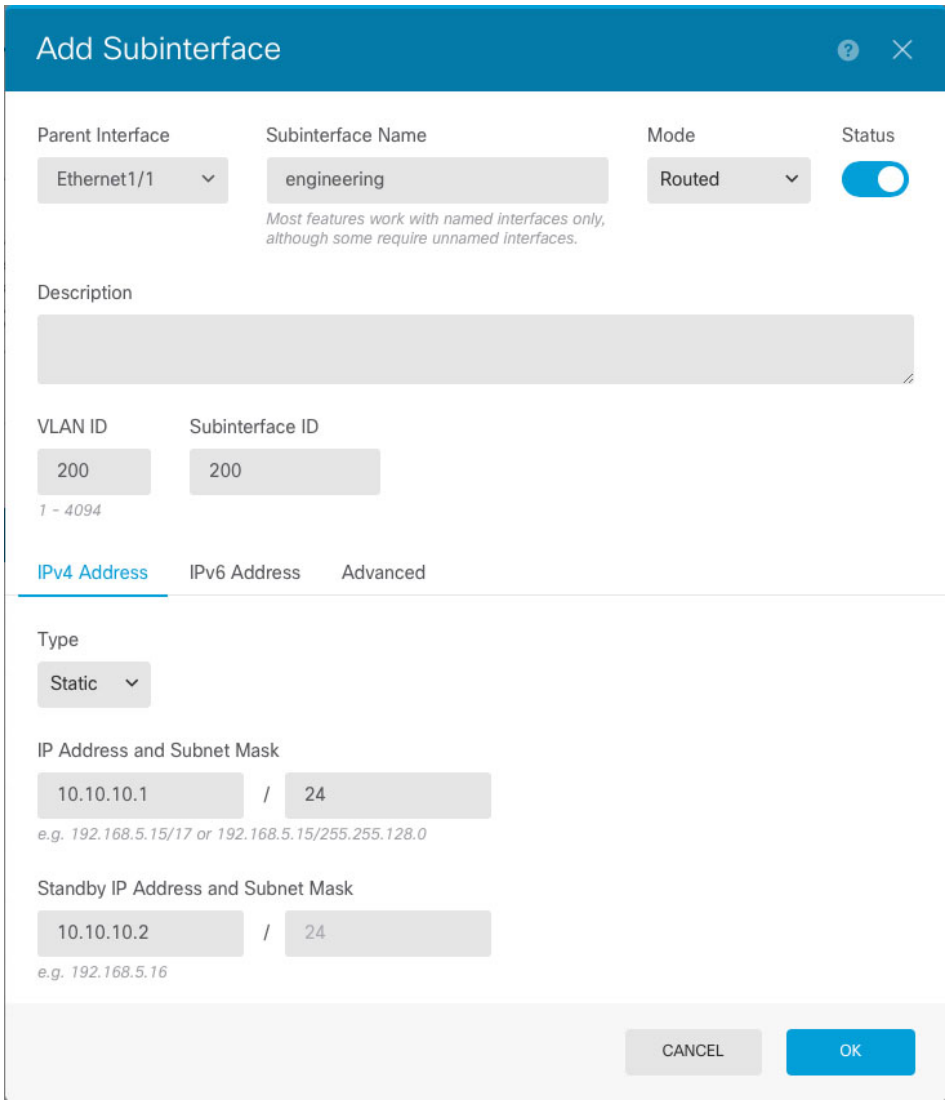
ステップ 2 次のいずれかを実行します。

- [Interfaces] ページで、プラスアイコン（  ）をクリックして、新しいサブインターフェイスを作成します。
- [EtherChannel] ページで、プラスと下矢印のアイコン（）をクリックし、[Subinterface] を選択します。
- 編集するサブインターフェイスの編集アイコン（  ）をクリックします。

サブインターフェイスが不要になった場合は、このサブインターフェイスの [削除（delete）] アイコン（  ）をクリックして削除します。

ステップ 3 [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

ステップ 4 親インターフェイス、名前、および説明を設定します。



a) [Parent Interface] を選択します。

親インターフェイスは、サブインターフェイスの追加先となる物理インターフェイスです。いったん作成したサブインターフェイスの親インターフェイスは変更できません。

b) [Subinterface Name]（最大 48 文字）を設定します。

英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。

（注） 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

c) [モード（Mode）] を [ルーテッド（Routed）] に設定します。

後でこのインターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

d) （任意） [Description] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

e) [VLAN ID] を設定します。

このサブインターフェイス上のパケットにタグを付けるために使用する VLAN ID を 1 ～ 4094 の範囲で入力します。

f) [サブインターフェイスID（Subinterface ID）] を設定します。

サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。この ID は、インターフェイス ID に追加されます。たとえば、Ethernet1/1.100 のようになります。便宜上 VLAN ID を一致させることもできますが、必須ではありません。いったん作成したサブインターフェイスの ID は変更できません。

ステップ 5 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック（Static）]：変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

（注） インターフェイスに対して設定されているDHCPサーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスのIPアドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCPサーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定（934 ページ）を参照してください。

- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスがDSL モデム、ケーブルモデム、またはISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択したグループ名を指定します。
  - [PPPoEユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoEパスワード（PPPoE Password）]：ISPによって提供されたパスワードを指定します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

    PAPは認証時にクリアテキストのユーザ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。
  - [PPPoEの学習済みルートメトリック（PPPoE Learned Route Metric）]：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ます。有効な値は1～255です。デフォルトでは、学習したルートのアドミニストレーティブディスタンスは1です。
  - [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
  - [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 6 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクロー

カル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

（注） IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  RFC 4862 では、ステートレス自動設定用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されていますが、この場合は、Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定（291 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注） 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。例、fe80::20d:88ff:feee:6a82。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。

- [スタンバイ IP アドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RA を抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるよう

に、Threat Defenseはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

Threat Defense デバイスで 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抑制できます。

ステップ 7 （任意）詳細オプションの設定 （350 ページ）。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 8 **[OK]** をクリックします。

次のタスク

- サブインターフェイスを適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定 （167 ページ） を参照してください。
- ダイナミック DNS サービスプロバイダーに完全修飾ドメイン名（FQDN）を登録し、DNS サーバの IPv4 と IPv6 の両方のインターフェイスアドレスが更新されるように DDNS を設定します。ダイナミック DNS（DDNS）の設定 （939 ページ） を参照してください。

パッシブ インターフェイスの設定

パッシブインターフェイスは、スイッチ SPAN（スイッチドポート アナライザ）またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニターします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。

パッシブ展開で設定されたシステムでは、特定のアクション（トラフィックのブロッキングなど）を実行できません。パッシブ インターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

パッシブインターフェイスを使用して、ネットワーク上のトラフィックをモニタし、トラフィックに関する情報を収集します。たとえば、侵入ポリシーを適用して、ネットワークを攻撃する脅威のタイプを特定したり、ユーザーが作成している Web 要求の URL カテゴリを確認できます。さまざまなセキュリティ ポリシーおよびルールを実装して、アクティブに展開されたシステムの動作を確認し、アクセス制御やその他のルールに基づいてトラフィックをドロップできます。

ただし、パッシブインターフェイスはトラフィックに影響を与えることができないため、多数の設定上の制限が存在します。これらのインターフェイスは、システムがトラフィックをピークすることを可能にするだけです。パッシブインターフェイスに入るパケットがデバイスを出ることはありません。

ここでは、パッシブ インターフェイスとそれらの設定方法について説明します。

パッシブ インターフェイスを使用する理由

パッシブ インターフェイスの主な目的は、単純なデモンストレーション モードを提供することです。単一の送信元ポートをモニターするようにスイッチをセットアップし、ワークステーションを使用して、パッシブ インターフェイスでモニターしたテスト トラフィックを送信できます。これにより、脅威に対する防御システムが接続を評価したり脅威を特定したりする方法を確認できます。システムの実行方法に問題がなければ、その方法をネットワーク内にアクティブに展開して、パッシブ インターフェイスの設定を削除できます。

ただし、次のサービスを提供するために実稼働環境でパッシブインターフェイスを使用することもできます。

- 純粋な IDS 展開：システムをファイアウォールまたは IPS（侵入防御システム）として使用しない場合、IDS（侵入検知システム）としてパッシブに展開できます。この展開方法では、アクセス制御ルールを使用してすべてのトラフィックに侵入ポリシーを適用します。また、システムでスイッチ上の複数の送信元ポートもモニタします。さらに、ダッシュボードを使用してネットワークで見られる脅威をモニターできます。ただし、このモードでは、この脅威を防ぐためにできることはありません。
- 混合展開：アクティブ ルーテッド インターフェイスとパッシブ インターフェイスを同じシステム上に混在させることができます。これにより、脅威に対する防御デバイスをいくつかのネットワークでファイアウォールとして展開すると同時に、複数のパッシブ インターフェイスを他のネットワーク内のトラフィックをモニターするように設定することができます。

パッシブ インターフェイスの制限

パッシブ モード インターフェイスとして定義する物理インターフェイスには次の制限があります。

- パッシブ インターフェイスのサブインターフェイスは設定できません。
- パッシブ インターフェイスをブリッジ グループに含めることはできません。
- パッシブ インターフェイスで IPv4 アドレスまたは IPv6 アドレスを設定することはできません。
- パッシブ インターフェイスに [管理専用（Management Only）] オプションを選択することはできません。

- このインターフェイスはパッシブ モード セキュリティ ゾーンにのみ含めることができます。ルーテッド セキュリティ ゾーンに含めることはできません。
- パッシブ セキュリティ ゾーンをアクセス制御またはアイデンティティ ルールの送信元基準に含めることは可能です。パッシブ ゾーンを宛先基準で使用することはできません。パッシブ ゾーンとルーテッド ゾーンを同じルールに混在させることもできません。
- パッシブ インターフェイスの管理アクセス ルール（HTTPS または SSH）を設定することはできません。
- パッシブ インターフェイスを NAT ルールで使用することはできません。
- パッシブ インターフェイスのスタティック ルートを設定することはできません。パッシブ インターフェイスをルーティング プロトコルの設定で使用することもできません。
- パッシブ インターフェイスで DHCP サーバを設定することはできません。パッシブ インターフェイスを使用して自動設定で DHCP 設定を取得することもできません。
- パッシブ インターフェイスを syslog サーバ設定で使用することはできません。
- パッシブ インターフェイスではどのタイプの VPN も設定することはできません。

ハードウェア Threat Defense パッシブインターフェイスのスイッチの設定

ハードウェア 脅威に対する防御 デバイス上のパッシブインターフェイスは、ネットワークスイッチを正しく設定している場合にのみ機能します。次の手順は、Cisco Nexus 5000 シリーズスイッチに基づいています。別のタイプのスイッチでは、コマンドが異なる可能性があります。

基本的な考え方としては、SPAN（スイッチド ポート アナライザ）またはミラー ポートを設定し、そのポートにパッシブ インターフェイスを接続し、スイッチでモニタリング セッションを設定して、1 つまたは複数の送信元ポートから SPAN またはミラー ポートにトラフィックのコピーを送信します。

手順

ステップ 1 スイッチ上のポートをモニタ（SPAN またはミラー）ポートとして設定します。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

ステップ 2 モニタへのポートを特定するモニタリング セッションを定義します。

SPAN またはミラー ポートを宛先ポートとして定義していることを確認します。次の例では、2 つの送信元ポートがモニタされています。

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

ステップ 3 （任意）**show monitor session** コマンドを使用して、設定を確認します。

次の例に、セッション 1 の概要出力を示します。

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ 4 脅威に対する防御パッシブインターフェイスからスイッチ上の宛先ポートにケーブルを物理的に接続します。

物理接続を行う前後に、パッシブ モードでインターフェイスを設定できます。パッシブ モードでの物理インターフェイスの設定 （344 ページ） を参照してください。

Threat Defense Virtual パッシブインターフェイスの VLAN の設定

Threat Defense Virtual デバイスのパッシブインターフェイスは、仮想ネットワーク上で VLAN を正しく設定した場合にのみ機能します。次の手順を実行してください。

- Threat Defense Virtual インターフェイスを、無差別モードで設定した VLAN に接続します。その後、パッシブ モードでの物理インターフェイスの設定（344 ページ）での説明に従ってインターフェイスを設定します。パッシブ インターフェイスでは、プロミスキャス VLAN 上のすべてのトラフィックのコピーが認識されます。
- 同じ VLAN に、1 つ以上のエンドポイント デバイス（仮想 Windows システムなど）を接続します。VLAN からインターネットへの接続がある場合は、単一のデバイスを使用できます。それ以外の場合は、トラフィックを通過させるために 2 つ以上のデバイスが必要です。URL カテゴリのデータを取得するには、インターネット接続が必要です。

パッシブ モードでの物理インターフェイスの設定

インターフェイスはパッシブ モードで設定できます。パッシブに機能する場合、インターフェイスは（ハードウェア デバイスの）スイッチそのものまたは（Threat Defense Virtual の）プロミスキャス VLAN に設定されたモニタリング セッションで送信元ポートからのトラフィックを単にモニターします。スイッチまたは仮想ネットワークで設定する必要がある内容の詳細については、次のトピックを参照してください。

- ハードウェア Threat Defense パッシブインターフェイスのスイッチの設定 （342 ページ）
- Threat Defense Virtual パッシブインターフェイスの VLAN の設定 （343 ページ）

トラフィックに影響を及ぼすことなくモニタ対象スイッチポートからのトラフィックを分析するには、パッシブ モードを使用します。パッシブ モードを使用するエンドツーエンドの例については、ネットワーク上のトラフィックをパッシブにモニタする方法 （90 ページ）を参照してください。

手順

ステップ 1 [Device] をクリックし、[Interfaces] サマリーにあるリンクをクリックし、[Interfaces] または [EtherChannel] をクリックします。

ステップ 2 編集する物理インターフェイスまたはEtherChannelの編集アイコン（  ）をクリックします。

現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブインターフェイスに変換する場合は、最初にセキュリティ ゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。

ステップ 3 [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

ステップ 4 次を設定します。

- [インターフェイス名（Interface Name）]：最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、monitor などです。
- [モード（Mode）]：[パッシブ（Passive）] を選択します。
- （オプション）[説明（Description）]：説明は 200 文字以内で、改行を入れずに 1 行で入力します。

（注） IPv4アドレスまたはIPv6アドレスを設定することはできません。[詳細（Advanced）] タブで変更できるのは、MTU、デュプレックス、速度設定のみです。

ステップ 5 [OK] をクリックします。

次のタスク

パッシブインターフェイスを作成するだけでは、インターフェイスで確認されるトラフィックの情報を十分にダッシュボードに示すことはできません、次の手順も実行する必要があります。使用例で次の手順について説明します。ネットワーク上のトラフィックをパッシブにモニタする方法 （90 ページ）を参照してください。

- パッシブ セキュリティ ゾーンを作成し、それにインターフェイスを追加します。セキュリティ ゾーンの設定 （167 ページ）を参照してください。
- パッシブ セキュリティ ゾーンを送信元ゾーンとして使用するアクセス制御ルールを作成します。通常は、これらのルールに侵入ポリシーを適用して、IDS（侵入検知システム）モニタリングを実装します。アクセス コントロール ポリシーを設定する （612 ページ）を参照してください。
- 必要に応じて、パッシブ セキュリティ ゾーン向けに SSL 復号およびアイデンティティ ルールを作成し、セキュリティ インテリジェンス ポリシーを有効にします。

インラインセットの設定

インラインセットは、IPS 専用インターフェイスを提供します。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

インラインセットはワイヤ上のバンプのように動作し、2 つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にデバイスをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

ガイドラインと制約事項

- インラインセットは、Firepower 1000 シリーズ、Firepower 2100、Cisco Secure Firewall 3100 のデバイスモデルでのみ設定できます。
- インラインセットで許可されるインターフェイスタイプ：物理、EtherChannel。
- インラインセットに管理インターフェイスを含めることはできません。
- インラインセットで使用されるインターフェイスの属性（名前、モード、インターフェイス ID、MTU、IP アドレス）は変更できません。
- タップモードを有効にすると、Snort フェールオープンは無効になります。
- Bidirectional Forwarding Detection（BFD）エコーパケットは、インラインセットを使用するときに、デバイスを介して許可されません。BFD を実行しているデバイスの両側に 2 つのネイバーがある場合、デバイスは 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。

- インラインセットとパッシブインターフェイスについては、デバイスではパケットで802.1Qヘッダーが2つまでサポートされます（Q-in-Qサポートとも呼ばれます）。ファイアウォールタイプのインターフェイスではQ-in-Qはサポートされず、802.1Qヘッダーは1つだけサポートされることに注意してください。
- インライン セット内のインターフェイスは、ルーティング、NAT、DHCP（サーバー、クライアント、またはリレー）、VPN、TCP インターセプト、アプリケーション インスペクション、または NetFlow をサポートしません。

始める前に

- 脅威防御インライン ペア インターフェイスに接続する STP 対応スイッチに対して STP PortFast を設定することを推奨します。
- インライン セットのメンバーとなる物理インターフェイスまたは EtherChannel インターフェイスを設定します。名前、デュプレックス、速度、ルーテッドモード（パッシブを選択しないでください）の値のみを設定します。手動 IP アドレス、DHCP、または PPoE などのアドレッシングタイプは設定しないでください。

（注） インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。

手順

ステップ 1 [デバイス（Device）] をクリックして、[インターフェイス（Interfaces）] サマリーのリンクをクリックしてから、[インラインセット（Inline Sets）] をクリックします。

ステップ 2 次のいずれかを実行します。

- [+] をクリックして、新しいインラインセットを作成します。
- 既存のインラインセットを変更するには、そのインラインセットの編集アイコン（）をクリックします。
- インラインセットが不要になった場合は、そのインラインセットの削除アイコン（）をクリックします。

ステップ 3 次のオプションを構成します

- インラインセットの [名前（Name）] を設定します。
- （オプション）[MTU] を変更します。

  デフォルトのMTUは1500です。より大きなパッケージを処理するには、より高い値に設定できます。

ステップ 4 [一般（General）] タブで、インターフェイスペアを追加します。ペアごとに 2 つのインターフェイスを選択する必要があります。不要なペアは削除できます。

インラインセットにインターフェイスを追加すると、そのモードは [ルーテッド（Routed）] から [インライン（Inline）] に変更されます。インターフェイスの属性は、インラインセットから削除するまで編集できません。

ステップ 5 [詳細（Advanced）] タブで、次のオプションパラメータを設定します。

- [モード（Mode）] : [インライン（Inline）] モードは標準モードであり、デバイスを通過するトラフィックに影響を与えます。

  [タップ（Tap）] モードでは、デバイスはインラインで展開されますが、ネットワーク トラフィック フローは妨げられません。代わりに、デバイスは各パケットのコピーを作成して、パケットを分析できるようにします。それらのタイプのルールでは、ルールがトリガーされると侵入イベントが生成され、侵入イベントのテーブルビューにはトリガーの原因となったパケットがインライン展開でドロップされたことが示されることに注意してください。インライン展開されたデバイスでタップモードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワーク間の配線をセットアップし、デバイスで生成される侵入イベントのタイプを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更してドロップルールを追加できます。デバイスをインラインで展開する準備ができたら、タップモードを無効にして、デバイスとネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。[タップ（Tap）] モードは、トラフィックによってはデバイスのパフォーマンスに大きく影響することに注意してください。

- [Snortフェールオープン（Snort Fail Open）] : Snort プロセスがビジーであるか、ダウンしている場合に、インスペクション（有効）またはドロップ（無効）されることなく、新規および既存のトラフィックを通過させる場合は、[ビジー（Busy）] オプションおよび [ダウン（Down）] オプションのいずれかまたは両方を有効または無効にします。

  デフォルトでは、Snort プロセスがダウンしている場合、トラフィックはインスペクションなしで通過し、Snort プロセスがビジーの場合、トラフィックはドロップされます。

  Snort プロセスが次の場合。

  - [ビジー（Busy）] : トラフィックバッファが満杯なため、トラフィックを高速処理できません。デバイスの処理量を超えるトラフィックが存在していること、またはその他のソフトウェアリソースの問題があることを示しています。
  - [ダウン（Down）] : プロセスの再起動を必要とする設定を展開したため、プロセスが再起動中です。

  Snort プロセスは、ダウンしてから再起動すると、新しい接続のインスペクションを実行します。Snort プロセスでは、誤検出と検出漏れを防ぐために、インラインインターフェイス、ルーテッドインターフェイス、またはトランスペアレントインターフェイスの既存の接続のインスペクションは実行されません。これは、プロセスがダウンしていた間に初期のセッション情報が失われている可能性があるためです。

（注） Snort フェール オープン時には、Snort プロセスに依存する機能は働きません。そのような機能には、アプリケーション制御とディープインスペクションが含まれます。システムでは、シンプルかつ容易に判断できるトランスポート層とネットワークの特性を使用して、基本的なアクセスコントロールのみ実行されます。

- [リンクステートの伝達（Propagate Link State）]：リンクステートの伝達を設定します。

  リンクステートの伝達によって、インラインセットのインターフェイスの 1 つが停止した場合、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンクステートが変化すると、デバイスはその変化を検知し、その変化に合わせて他のインターフェイスのリンクステートを更新します。ただし、デバイスからリンクステートの変更が伝達されるまで最大 4 秒かかります。障害状態のネットワークデバイスを自動的に避けてトラフィックを再ルーティングするようにルータが設定されている復元力の高いネットワーク環境では、リンク ステートの伝達が特に有効です。

ステップ 6 [OK] をクリックします。

高度なインターフェイス オプションの設定

[詳細（Advanced）] オプションには、MTU、ハードウェア設定、管理専用、MAC アドレス、およびその他の設定が含まれています。

MAC アドレスについて

Media Access Control（MAC）アドレスを手動で設定してデフォルトをオーバーライドできます。

高可用性設定の場合は、インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの両方を設定できます。アクティブユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな 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。

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）：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。詳細オプションの設定 （350 ページ）を参照してください。

- 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。
- 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、Threat Defense 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。

MTU について

MTU は、Threat Defense デバイス 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。

パス MTU ディスカバリ

Threat Defenseデバイス 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。

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。

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） Threat Defense デバイス 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します。

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 Threat Defense 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 フレームとは、標準的な最大値 1522 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。ジャンボフレームに対応するために、MTU を 9,000 バイト以上に設定できます。最大値はモデルによって異なります。

（注） MTU を増やすとジャンボ フレームに割り当てるメモリが増え、他の機能（アクセス ルールなど）の最大使用量が制限される場合があります。Threat Defense Virtual のデフォルト値の 1,500 よりも MTU のサイズを大きくする場合は、システムを再起動する必要があります。高可用性にデバイスが設定されている場合、スタンバイ デバイスも再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、その他のモデルを再起動する必要はありません。

詳細オプションの設定

高度なインターフェイス オプションには、ほとんどのネットワークに適合するデフォルト設定が用意されています。ネットワーキングの問題を解決している場合または高可用性を設定する場合にのみ、これを設定します。

次の手順では、インターフェイスが定義済みであることを前提としています。インターフェイスを最初に編集または作成するときに、これらの設定を編集することもできます。

制限事項

- ブリッジ グループの場合は、このほとんどのオプションはメンバー インターフェイスに対して設定します。DAD 試行回数と HA モニタリングの有効化を除き、これらのオプションはブリッジ仮想インターフェイス（BVI）では使用できません。
- 管理インターフェイスに MTU、デュプレックス、速度を設定することはできません。

- 拡張オプションは、Firepower 1010 スイッチポートでは使用できません。
- Firepower 4100/9300 のインターフェイスにデュプレックスおよび速度を設定することはできません。インターフェイスのこれらの機能を設定するには、FXOS を使用します。
- パッシブ インターフェイスでは、MTU、デュプレックス、速度のみ設定できます。インターフェイスの管理のみを行うことはできません。

手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、次にインターフェイスタイプをクリックして、インターフェイスのリストを表示します。

ステップ 2 編集するインターフェイスの編集アイコン（  ）をクリックします。

ステップ 3 [詳細オプション（Advanced Options）] をクリックします。

ステップ 4 インターフェイスの状態を高可用性設定でピア装置にフェールオーバーするかどうか判断する際の要素にする場合は、[HAモニタリングの有効化（Enable for HA Monitoring）] を選択します。

このオプションは、高可用性を設定しない場合は無視されます。インターフェイスの名前を設定しない場合も、無視されます。

ステップ 5 データ インターフェイスを管理専用に指定する場合は、[管理専用（Management Only）] を選択します。

管理専用インターフェイスはトラフィックの通過を許可しないため、データインターフェイスを管理専用に設定する意味はあまりありません。管理/診断インターフェイスは、常に管理専用であるため、この設定を変更することはできません。

ステップ 6 Cisco Trustsec を有効にするには、[セキュリティグループタグの伝達（Propagate Security Group Tag）] を選択します。

名前付きか名前なしかにかかわらず、物理、サブインターフェイス、EtherChannel、VLAN、管理、または BVI インターフェイスで Cisco TrustSec を有効または無効にできます。デフォルトでは、インターフェイスに名前を付けると、Cisco TrustSec が自動的に有効になります。

ステップ 7 [MTU]（最大伝送ユニット）を任意の値に設定します。

デフォルトの MTU は 1500 バイトです。最小値と最大値は、プラットフォームによって異なります。ジャンボフレームが頻繁にやり取りされるネットワークでは、大きな値に設定します。

（注） ISA 3000 シリーズデバイス、Threat Defense Virtual で MTU を 1500 より大きい値に設定する場合は、デバイスを再起動する必要があります。高可用性にデバイスが設定されている場合、スタンバイデバイスも再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、その他のモデルを再起動する必要はありません。

ステップ 8 （物理インターフェイスのみ）速度およびデュプレックスの設定を変更します。

デフォルトでは、インターフェイスは接続相手のインターフェイスに対し、互いに最適なデュプレックスおよび速度をネゴシエートしますが、必要に応じて、特定のデュプレックスおよび速度を強制的に適用することもできます。記載されているオプションは、インターフェイスでサポートされているものだけです。ネットワークモジュールのインターフェイスにこれらのオプションを設定する前に、インターフェイス設定の制限事項 （292 ページ） をお読みください。

- [二重（Duplex）]：[ハーフ（Half）]、または [フル（Full）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）]：実際のオプションは、モデルとインターフェイスタイプによって異なります。速度、[自動（Auto）]、[ネゴシエーションなし（No Negotiate）]、または [SFPを検出（Detect SFP）] を選択してください。Firepower 1100 または 2100 SFP ファイバポートの場合、[ネゴシエーションなし（No Negotiate）] を指定すると速度が 1,000 Mbps に設定され、フロー制御パラメータとリモート障害情報のリンクネゴシエーションがディセーブルになります。（Cisco Secure Firewall 3100 のみ）[SFPを検出（Detect SFP）] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。
- （Cisco Secure Firewall 3100 のみ）[自動ネゴシエーション（Auto Negotiation）]：インターフェイスのタイプに応じて、フロー制御パラメータとリモート障害情報のリンクステータスをネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード（Forward Error Correction Mode）]：（Cisco Secure Firewall 3100 のみ）25 Gbps 以上のインターフェイスの場合は、前方誤り訂正（FEC）を有効にします。EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に前方誤り訂正を設定する必要があります。**自動**を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *6*：自動設定のデフォルト *FEC*

トランシーバタイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-SR	第 108 条 RS-FEC	第 108 条 RS-FEC
25G-LR	第 108 条 RS-FEC	第 108 条 RS-FEC
10/25G-CSR	第 108 条 RS-FEC	第 74 条 FC-FEC
25G-AOC*x*M	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション

ステップ 9 [IPv6設定（IPv6 Configuration）] を変更します。

- [DHCPクライアントの有効化（Enable DHCP Client）]：DHCPv6 を使用してアドレスを取得します。

  ルータアドバタイズメントからデフォルトルートを取得するには、[DHCPを使用してデフォルトルートを取得（Obtain default route using DHCP）] をオンにします。

- [Enable DHCP for IPv6 address configuration]：IPv6 ルータのアドバタイズメント パケットに、管理アクセス設定フラグを設定するかどうか。このフラグは、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 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。
- [Enable DHCP for IPv6 non-address configuration]：IPv6 ルータのアドバタイズメント パケットに、その他のアクセス設定フラグを設定するかどうか。このフラグは、DHCPv6 から DNS サーバ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。
- [DADの試行（DAD Attempts）]：インターネット上で重複アドレス検出（DAD）を実行する頻度（0 ～ 600）。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD はアドレスがインターフェイスに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検証します。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。インターフェイスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。重複アドレス検出（DAD）プロセスを無効にするには、この値を 0 に設定します。

ステップ 10 （必要に応じて、サブインターフェイスおよび高可用性装置に推奨されます。）MAC アドレスを設定します。

デフォルトでは、システムはインターフェイスのネットワーク インターフェイス カード（NIC）に焼き込まれた MAC アドレスを使用します。したがって、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 MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MACアドレス（MAC Address）]：H.H.H 形式の Media Access Control。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。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

- [スタンバイMACアドレス（Standby MAC Address）]：高可用性で使用します。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 11 [OK] をクリックします。

インターフェイスの変更のスキャンとインターフェイスの移行

デバイスのインターフェイスを変更すると、デバイスは変更が発生したことを Device Manager に通知します。インターフェイスのスキャンを実行するまで、設定を展開することはできません。Device Manager では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。

インターフェイスのスキャンと移行について

Scanning

デバイスのインターフェイスを変更すると、デバイスは変更が発生したことを Device Manager に通知します。インターフェイスのスキャンを実行するまで、設定は展開できません。インターフェイスの追加、削除、または復元を検出するスキャンの後に設定を展開できますが、削除されたインターフェイスを参照している設定の部分は展開されません。

スキャンを必要とするインターフェイスの変更には、インターフェイスの追加や削除が含まれます。たとえば、ネットワークモジュールの変更、Firepower 4100/9300 シャーシ上に割り当てられたインターフェイスの変更、Threat Defense Virtual でのインターフェイスの変更などです。

次の変更は、スキャン後の展開をブロックしません。

- セキュリティゾーンのメンバーシップ
- EtherChannel インターフェイスのメンバーシップ
- Firepower 1010 VLAN インターフェイス スイッチ ポートのメンバーシップ
- BVI を参照するポリシーのブリッジ グループ インターフェイスのメンバーシップ

（注） syslog サーバーの出力インターフェイスの変更によって展開がブロックされることはありませんが、syslog サーバーの設定は、手動で、またはインターフェイス交換機能を使用して修正する必要があります。

Migrating

新しいインターフェイスの追加や未使用のインターフェイスの削除が、脅威に対する防御の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、セキュリティゾーン、NAT、VPN、ルーティング、DHCP サーバーなど、脅威に対する防御設定内の多くの場所で直接参照できます。

Device Manager では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。

（注） 移行機能は、名前、IPアドレス、およびその他の設定をインターフェイス間でコピー「しません」。この機能は、古いインターフェイスではなく新しいインターフェイスを参照するようにセキュリティポリシーを変更します。移行する前に、新しいインターフェイスの設定を手動で設定する必要があります。

インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。インターフェイスの追加と削除を同時に行っても移行プロセスは機能します。ただし、削除されたインターフェイスやそれらを参照するポリシーを「手動で」編集することはできません。そのため、移行を段階的に実行する方が簡単になる場合があります。

同じタイプのインターフェイスを交換する場合（たとえば、ネットワークモジュールを RMA する必要がある場合）は、次のことができます。1. シャーシからモジュールを取り外す。2. スキャンを実行する。3. 削除されたインターフェイスとは関係のない変更を展開する。4. モジュールを交換する。5. 新しいスキャンを実行する。6. インターフェイス関連の変更を含め、設定を展開します。新しいインターフェイスのインターフェイス ID と特性が古いインターフェイスと同じである場合は、移行を実行する必要はありません。

インターフェイスのスキャンと移行に関する注意事項と制限事項

サポートされていないインターフェイスの移行

- BVI への物理インターフェイス
- ファイアウォール インターフェイスへのパッシブインターフェイス
- ブリッジグループメンバー
- EtherChannel インターフェイスメンバー
- ISA 3000 ハードウェア バイパス メンバー
- Firepower 1010 VLAN インターフェイスまたはスイッチポート
- 診断インターフェイス
- HA フェールオーバーおよびステートリンク
- さまざまなタイプのインターフェイスの移行（たとえば、物理インターフェイスを必要とする機能へのブリッジ グループ インターフェイスの移行）

その他のガイドライン

- インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。

- Threat Defense Virtual では、インターフェイスリストの末尾でインターフェイスの追加や削除が行われるだけです。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤ったインターフェイスと一致します。
- スキャン/移行が失敗した場合は、シャーシの元のインターフェイスを復元し、元の状態に戻すために再スキャンします。
- バックアップの場合は、新しいインターフェイスを使用して新しいバックアップを作成してください。古い設定で復元すると、古いインターフェイス情報が復元され、スキャン/置換を再度実行する必要が生じます。
- HA の場合は、アクティブユニットでインターフェイススキャンを実行する前に、両方の装置で同じインターフェイスの変更を行います。アクティブユニットでスキャン/移行を実行する必要があるだけです。設定の変更はスタンバイ ユニットに複製されます。

インターフェイスのスキャンと移行

Device Manager でインターフェイスの変更をスキャンし、削除されたインターフェイスからインターフェイス設定を移行します。インターフェイス設定の移行のみを必要とする場合は（スキャンは不要）、次の手順のうちスキャンに関連するステップを無視してください。

（注） 移行機能は、名前、IP アドレス、およびその他の設定をインターフェイス間でコピー「しません」。この機能は、古いインターフェイスではなく新しいインターフェイスを参照するようにセキュリティポリシーを変更します。移行する前に、新しいインターフェイスの設定を手動で設定する必要があります。

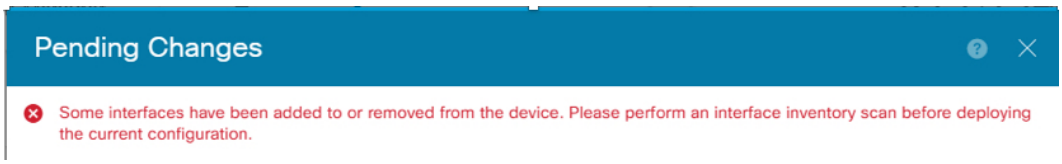
手順

ステップ 1 シャーシでインターフェイスを追加または削除します。

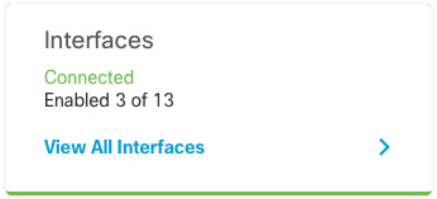
インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスの置き換えを実行することをお勧めします。

ステップ 2 インターフェイスの変更をスキャンします。

インターフェイスのスキャンを実行するまで、設定は展開できません。スキャンの前に展開しようとすると、次のエラーが表示されます。

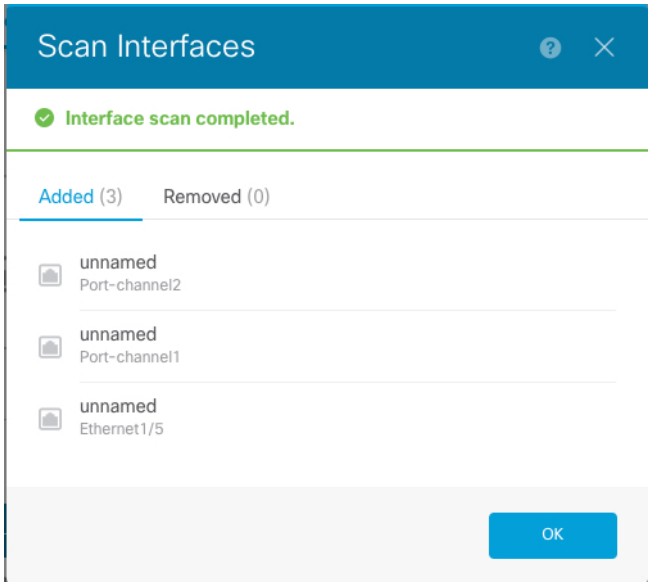


a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

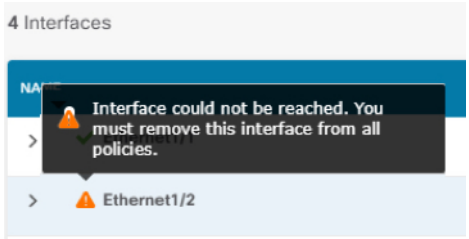


b) [インターフェイス（Interfaces）] アイコン（ ）をクリックします。

c) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



スキャン後、削除されたインターフェイスは、[インターフェイス（Interfaces）] ページに注意記号とともに表示されます。



ステップ 3 既存のインターフェイスを新しいインターフェイスに移行するには、次の手順を実行します。

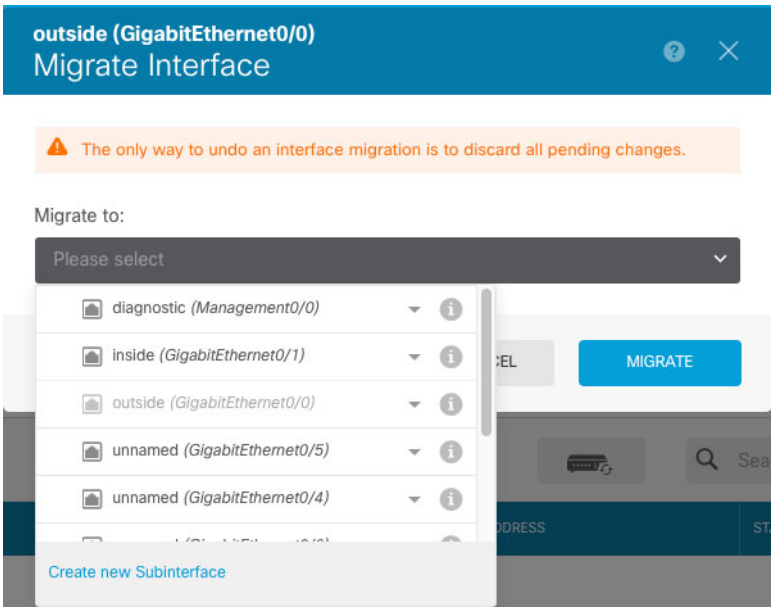
a) 新しいインターフェイスに名前、IP アドレスなどを設定します。

削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、まず古いインターフェイスをダミーの名前と IP アドレスで再設定する必要があります。

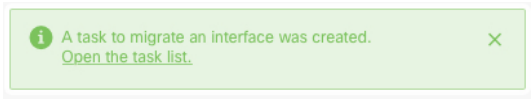
b) 古いインターフェイスの [移行（Migrate）] アイコンをクリックします。

このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに移行されます。

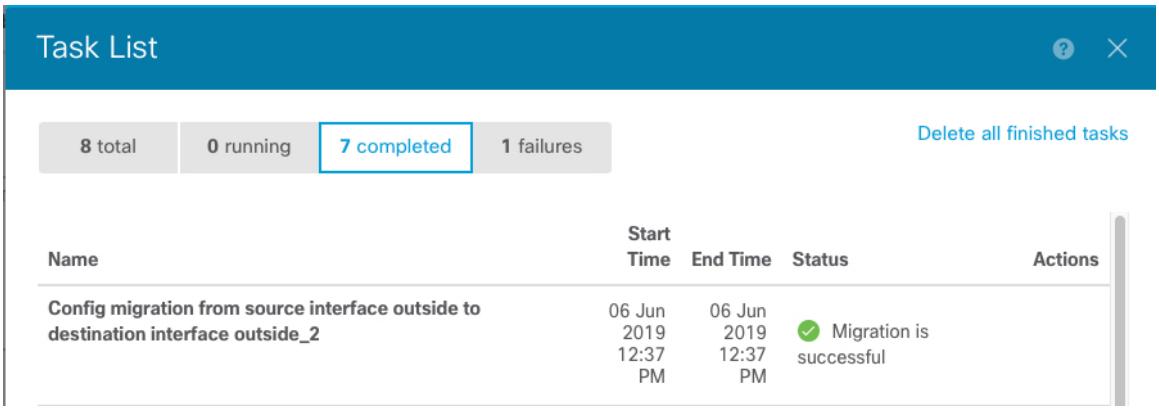
c) [移行先：（Migrate to:）] ドロップダウンリストから新しいインターフェイスを選択します。



d) [インターフェイス（Interfaces）] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。



e) [タスクリスト（Task List）] を調べて、移行が成功したことを確認します。

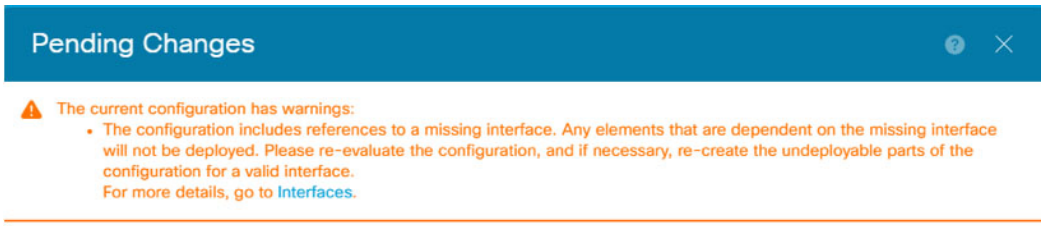


f) 移行が失敗した場合は、API エクスプローラで理由を確認できます。

API エクスプローラを開くには、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。**[インターフェイス（Interface）] > [GET /jobs/interfacemigrations]** を選択し、[試してみる（Try it Out!）] をクリックします。

ステップ 4 設定を展開します。

削除されたインターフェイスを参照する設定の部分は展開されません。その場合、次のメッセージが表示されます。



ステップ 5 シャーシの古いインターフェイスを取り外し、別のスキャンを実行します。

削除されたインターフェイスのうちポリシーで使用されなくなったものは、[インターフェイス（Interfaces）] ページから削除されます。

ステップ 6 設定を再度展開し、使用していないインターフェイスを設定から削除します。

Secure Firewall 3100 のネットワークモジュールの管理

最初にファイアウォールの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。

初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、次の手順を参照してください。

ブレークアウトポートの設定

40GB 以上のインターフェイスごとに 10GB のブレークアウトポートを設定できます。この手順では、ポートの分割と再参加の方法について説明します。ブレークアウトポートは、EtherChannel への追加を含め、他の物理イーサネットポートと同じように使用できます。

ハイアベイラビリティの場合は、アクティブユニットでこの手順を実行します。インターフェイスの変更は他のユニットに複製されます。

始める前に

- サポートされているブレークアウトケーブルを使用する必要があります。詳細については、ハードウェア設置ガイドを参照してください。
- このインターフェイスは、ご使用の構成では使用できませんサブインターフェイスを持つことも、EtherChannel の一部にすることもできません。
- ハイアベイラビリティの場合、ハイアベイラビリティ用のインターフェイスの命名、有効化、またはモニタリングもできません。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 40GB 以上のインターフェイスから 10GB ポートを分割するために、インターフェイスの右側にある [ブレークアウト（Breakout）] アイコン（  ）をクリックします。

確認ダイアログボックスで、[OK] をクリックします。インターフェイスが使用中の場合は、エラーメッセージが表示されます。分割を再試行する前に、ユースケースを解決する必要があります。たとえば、別のインターフェイスを使用するように設定を変更することができます。

たとえば、Ethernet2/1 40GB インターフェイスを分割する場合、分割後の子インターフェイスは、Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3、および Ethernet2/1/4 として識別されます。

インターフェイスのグラフィックでは、分割されたポートは  によって示されます。ブレークアウトポートのステータスの詳細を示すページは、左右の矢印をクリックしてスクロールすることができます。

ステップ 3 ブレークアウトポートを再参加させるには、インターフェイスの右側にある [参加（Join）] アイコン（）をクリックします。

確認ダイアログボックスで、[OK] をクリックします。子ポートが使用中の場合は、エラーメッセージが表示されます。再参加を再試行する前に、ユースケースを解決する必要があります。たとえば、別のインターフェイスを使用するように設定を変更することができます。

インターフェイスのすべての子ポートを再参加させる必要があります。

ステップ 4 設定を展開します。

ネットワークモジュールの追加

初回起動後にファイアウォールにネットワークモジュールを追加するには、次の手順を実行します。新しいモジュールを追加するには、再起動が必要です。

手順

ステップ 1 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。

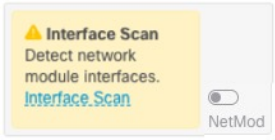
ハイアベイラビリティの場合は、両方のユニットにネットワークモジュールをインストールします。

ステップ 2 ファイアウォールを再起動します。システムの再起動またはシャットダウン（1006ページ）を参照してください。ハイアベイラビリティの場合は、スタンバイユニットを再起動してから、スタンバイユニットでこの手順の残りを実行します。

ステップ 3 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

次のグラフィックは、インターフェイススキャンが必要であることを示しています。

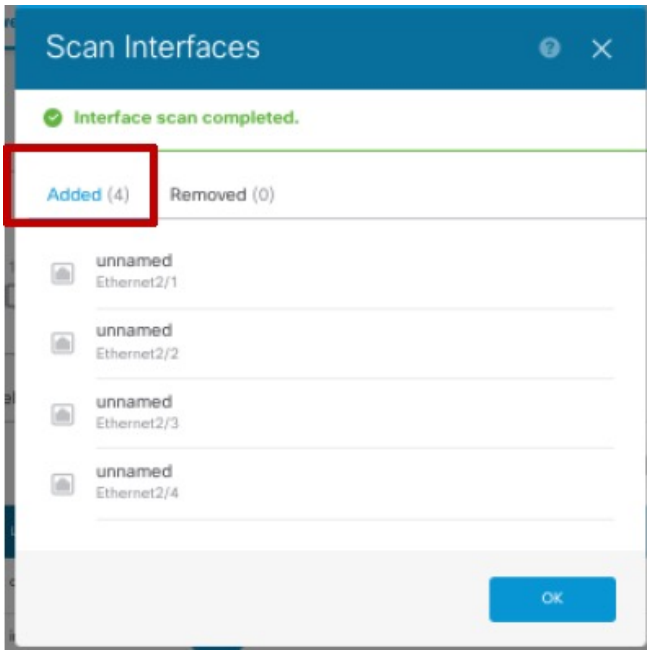
図 *14*：インターフェイススキャンが必要



ステップ 4 [インターフェイススキャン（Interface Scan）] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

図 *15* : インターフェイスのスキャン

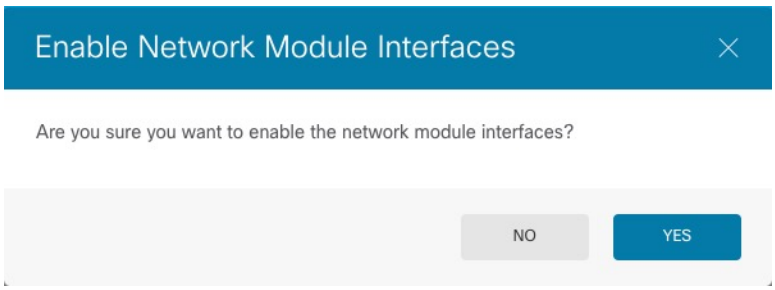


ステップ 5 インターフェイスのグラフィックで、スライダー（ ）をクリックしてネットワークモジュールを有効にします。

図 *16* : ネットワークモジュールの有効化

ステップ 6 ネットワークモジュールを有効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 *17* : 有効化の確認



ステップ 7 ハイアベイラビリティの場合は、アクティブユニットを変更し（アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー） （267 ページ）を参照）、新しいスタンバイユニットに対して上記の手順を実行します。

ネットワークモジュールの交換方法

再起動することなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。この手順では、古いモジュールをシャットダウンし、新しいモジュールをインストールして有効にする方法について説明します。

始める前に

ハイアベイラビリティの場合、フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。ハイアベイラビリティを解除する必要があります（ハイアベイラビリティの破棄 （266 ページ）を参照）。モジュールをホットスワップした後、ハイアベイラビリティを再編成できます。

手順

ステップ 1 ハイアベイラビリティの場合、ホットスワップを実行するユニットがスタンバイノードであることを確認します。アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー）（267 ページ）を参照してください。

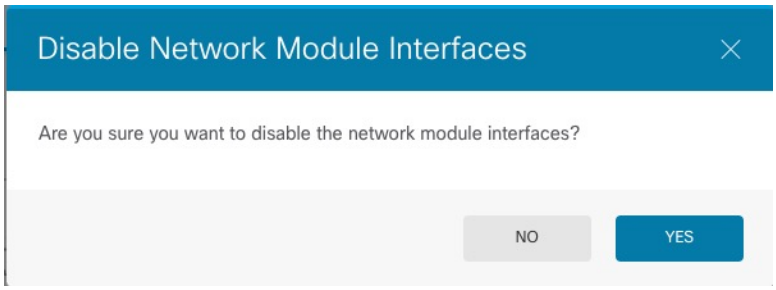
ステップ 2 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

ステップ 3 インターフェイスのグラフィックで、スライダー（  ）をクリックしてネットワークモジュールを無効にします。

図 *18*：ネットワークモジュールの無効化

ステップ 4 ネットワークモジュールを無効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 *19* : 無効化の確認



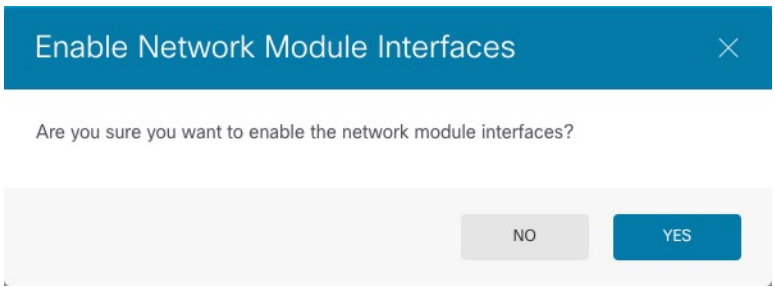
ステップ 5 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。

ステップ 6 インターフェイスのグラフィックで、スライダー（ ）をクリックしてネットワークモジュールを有効にします。

図 *20* : ネットワークモジュールの有効化

ステップ 7 ネットワークモジュールを有効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 *21* : 有効化の確認



ネットワークモジュールを別のタイプに交換する

ネットワークモジュールを別のタイプに交換する場合は、再起動が必要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。

始める前に

ハイアベイラビリティの場合、フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。ハイアベイラビリティを解除する必要があります（ハイアベイラビリティの破棄（266ページ）を参照）。これにより、アクティブユニットの再起動時にダウンタイムが発生するようになります。ユニットの再起動が完了したら、ハイアベイラビリティを再編成できます。

手順

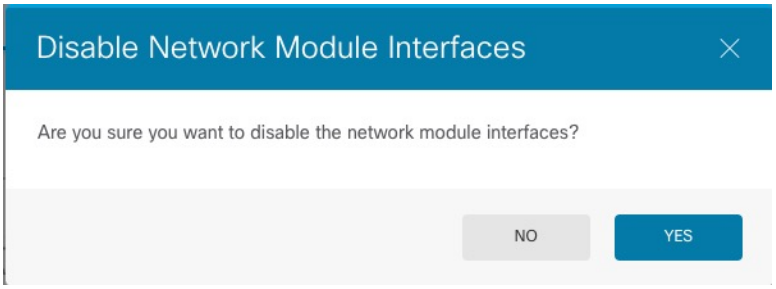
ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。ハイアベイラビリティの場合は、最初にスタンバイユニットでこの手順を実行します。

ステップ 2 インターフェイスのグラフィックで、スライダー（）をクリックしてネットワークモジュールを無効にします。

図 *22 :* ネットワークモジュールの無効化

ステップ 3 ネットワークモジュールを無効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 *23 :* 無効化の確認



ステップ 4 ハードウェア設置ガイドに従って、デバイスの古いネットワークモジュールを取り外し、新しいネットワークモジュールと交換します。

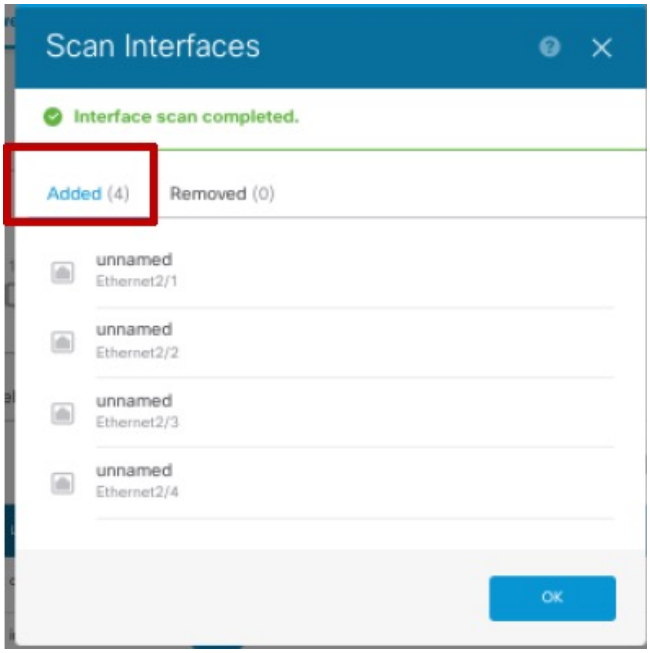
ステップ 5 ファイアウォールを再起動します。システムの再起動またはシャットダウン（1006ページ）を参照してください。

ステップ 6 [インターフェイス（Interfaces）] ページの次のグラフィックは、インターフェイススキャンが必要であることを示しています。[インターフェイススキャン（Interface Scan）] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

図 *24* : インターフェイススキャンが必要

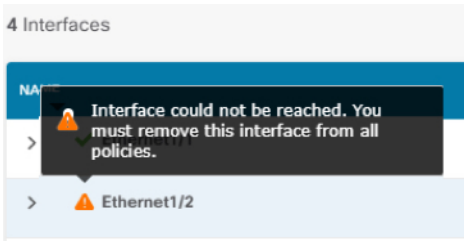
ステップ 7 インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

図 *25* : インターフェイスのスキャン



スキャン後、削除されたインターフェイスは、[インターフェイス（Interfaces）]ページに注意記号とともに表示されます。

図 *26* : 削除されたインターフェイス



ステップ 8 ネットワークモジュールのインターフェイスの数が減少した場合は、削除されたインターフェイスを直接参照する設定を削除する必要があります。

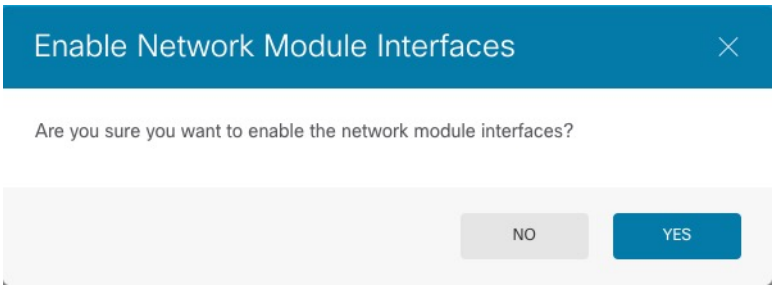
セキュリティゾーンを参照するポリシーは影響を受けません。必要に応じて、設定を別のインターフェイスに移行させることができます。インターフェイスのスキャンと移行（356ページ）を参照してください。

ステップ 9 インターフェイスのグラフィックで、スライダー（ ）をクリックしてネットワークモジュールを有効にします。

図 *27* : ネットワークモジュールの有効化

ステップ 10 ネットワークモジュールを有効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 *28* : 有効化の確認



ステップ 11 インターフェイス速度を変更するには、詳細オプションの設定（350 ページ）を参照してください。

デフォルトの速度は、[SFPを検出（Detect SFP）] に設定されています。これにより、取り付けられている SFP から適切な速度が検出されます。速度を手動で特定の値に設定しており、その速度の変更が必要になった場合にのみ、速度を修正する必要があります。

ステップ 12 設定を変更する必要がある場合は、[展開（Deployment）] アイコンをクリックします。

ネットワークモジュールの変更を保存するためだけに展開する必要はありません。

ステップ 13 ハイアベイラビリティの場合は、アクティブユニットを変更し（アクティブ ピアとスタンバイ ピアの切り替え（強制フェールオーバー） （267 ページ）を参照）、新しいスタンバイユニットに対して上記の手順を実行します。

ネットワーク モジュールの取り外し

ネットワークモジュールを完全に削除する場合は、次の手順に従います。ネットワークモジュールを削除するには、再起動が必要です。

始める前に

ハイアベイラビリティの場合は、フェールオーバーリンクがネットワークモジュール上にないことを確認してください。

手順

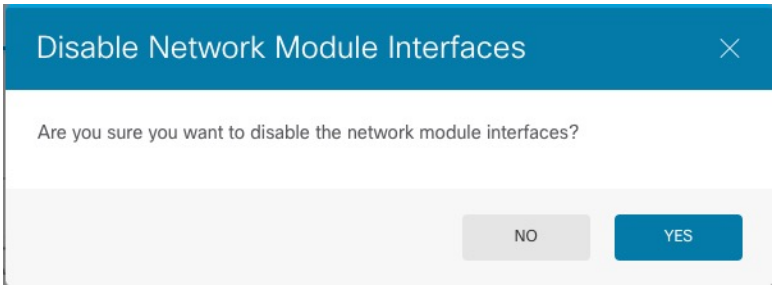
ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。ハイアベイラビリティの場合は、最初にスタンバイユニットでこの手順を実行します。

ステップ 2 インターフェイスのグラフィックで、スライダー（）をクリックしてネットワークモジュールを無効にします。

図 *29* : ネットワークモジュールの無効化

ステップ 3 ネットワークモジュールを無効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 *30* : 無効化の確認



ステップ 4 ファイアウォールで、ネットワークモジュールを削除します。

ステップ 5 ファイアウォールを再起動します。システムの再起動またはシャットダウン（1006ページ）を参照してください。

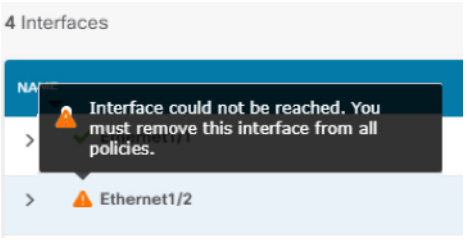
ステップ 6 [インターフェイス（Interfaces）] ページの次のグラフィックは、インターフェイススキャンが必要であることを示しています。[インターフェイススキャン（Interface Scan）] をクリックして、ネットワークモジュールの適切な詳細情報でページを更新します。

図 *31* : インターフェイススキャンが必要

ステップ 7 インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

スキャン後、削除されたインターフェイスは、[インターフェイス（Interfaces）] ページに注意記号とともに表示されます。

図 *32* : 削除されたインターフェイス



ステップ 8 削除されたインターフェイスを直接参照するすべての設定を削除する必要があります。

セキュリティゾーンを参照するポリシーは影響を受けません。必要に応じて、設定を別のインターフェイスに移行させることができます。インターフェイスのスキャンと移行（356ページ）を参照してください。

ステップ 9 設定を変更する必要がある場合は、[展開（Deployment）] アイコンをクリックします。

ネットワークモジュールの変更を保存するためだけに展開する必要はありません。

ステップ 10 ハイアベイラビリティの場合は、アクティブユニットを変更し（アクティブピアとスタンバイピアの切り替え（強制フェールオーバー）（267ページ）を参照）、新しいスタンバイユニットに対して上記の手順を実行します。

管理インターフェイスと診断インターフェイスのマージ

Threat Defense 7.4 以降では、マージされた管理インターフェイスと診断インターフェイスがサポートされます。診断インターフェイスを使用する設定がある場合、インターフェイスは自動的にマージされないため、次の手順を実行する必要があります。この手順では、設定の変更を確認し、場合によっては手動で設定を修正する必要があります。

バックアップ/復元機能は、マージの状態（マージされていないかマージされている）を保存および復元します。たとえば、インターフェイスをマージしてから、古いマージされていない設定を復元すると、復元された設定はマージされていない状態になります。

次の表に、レガシー診断インターフェイスで使用可能な設定と、マージの完了方法を示します。

表 7: *Device Manager* 統合管理インターフェイスのサポート

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
インターフェイス		「管理」インターフェイスが [Interfaces] ページに表示され、設定できるようになりました。以前は、**[System Settings]** > **[Management Interface]** ページで設定が可能でした。
• IP アドレス	手動で削除する必要があります。	代わりに現在の管理 IP アドレスが使用されます。 高可用性の場合、管理インターフェイスはスタンバイ IP アドレスをサポートしません。各ユニットには、フェールオーバー後も維持される独自の IP アドレスがあります。そのため、現在のアクティブユニットとの通信に単一の管理 IP アドレスを使用することはできません。 [Interfaces] ペインで設定するか、**configure network ipv4** または **configure network ipv6** コマンドを使用して CLI で設定します。
• 「診断」名	自動的に「管理」に変更されます。 （注） 他のインターフェイスに「管理」という名前を付けることはできません。マージを続行するには、名前を変更する必要があります。	「管理」に変更されます。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
スタティック ルート	手動で削除する必要があります。	**サポートしない** 管理インターフェイスには、データインターフェイスに基づく個別の Linux ルーティングテーブルがあります。脅威に対する防御 には、実際のところ、データインターフェイス用と管理専用インターフェイス用の 2 つの「データ」ルーティングテーブルがあります（以前は診断インターフェイスが含まれていましたが、管理専用に設定されたすべてのインターフェイスも含まれています）。トラフィックタイプに応じて、脅威に対する防御 は 1 つのルーティングテーブルをチェックし、次に他のルーティングテーブルにフォールバックします。このルートルックアップには、診断インターフェイスは含まれておらず、管理用の Linux ルーティングテーブルも含まれていません。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（392ページ）」を参照してください。 **configure network static-routes** コマンドを使用して、CLI で Linux ルーティングテーブルのスタティックルートを追加できます。 （注） デフォルトルートは、**configure network ipv4** または **configure network ipv6** コマンドで設定します。
Syslog サーバー（Syslog Server）	自動的に管理インターフェイスに移動されました。	はい。 syslog サーバーの設定で、管理インターフェイスから syslog を送信するオプションを使用できるようになりました（6.3 以降）。syslog に関して診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。
RADIUS サーバー	自動的に管理インターフェイスに移動されました。	はい。 診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。 （注） ルートルックアップを指定した場合、脅威に対する防御 は管理専用インターフェイスからトラフィックを送信できなくなります。この場合、送信元インターフェイスとして管理専用インターフェイスを明示的に選択する必要があります。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
AD サーバー	必要に応じて、管理インターフェイスを手動で指定します。	はい。 デフォルトでは、ADサーバー通信のルートルックアップが実行され、7.4 より前のインターフェイスは指定できませんでした。7.4 以降、脅威に対する防御は、ルートルックアップを使用して管理専用インターフェイスからトラフィックを送信できなくなります。この場合、送信元インターフェイスとして管理専用インターフェイスを明示的に選択できるようになりました。
DDNS	手動で削除する必要があります。	**サポートしない**
DHCP サーバー	手動で削除する必要があります。	**サポートしない**
DNS サーバー	自動的に管理インターフェイスに移動されました。	はい。 診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。インターフェイス（[ANY]）を選択しなかった場合は、ルーティングルックアップも変更されます。ルーティングルックアップはデータルーティングテーブルを使用しますが、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックしません。 （注）　管理インターフェイスには、管理トラフィック専用の個別の DNS ルックアップ設定もあります。
SLA モニター	手動で削除する必要があります。	**サポートしない**
FlexConfig	手動で削除する必要があります。	**サポートしない**

始める前に

- デバイスの現在のモードを表示するには、脅威に対する防御 CLI で **show management-interface convergence** コマンドを入力します。次の出力は、管理インターフェイスがマージされていることを示しています。

```
> show management-interface convergence
management-interface convergence
>
```

次の出力は、管理インターフェイスがマージされていないことを示しています。

```
> show management-interface convergence
```

```
no management-interface convergence
>
```

- 高可用性ペアの場合は、アクティブユニットでこのタスクを実行します。マージされた設定は、自動的にスタンバイユニットに複製されます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

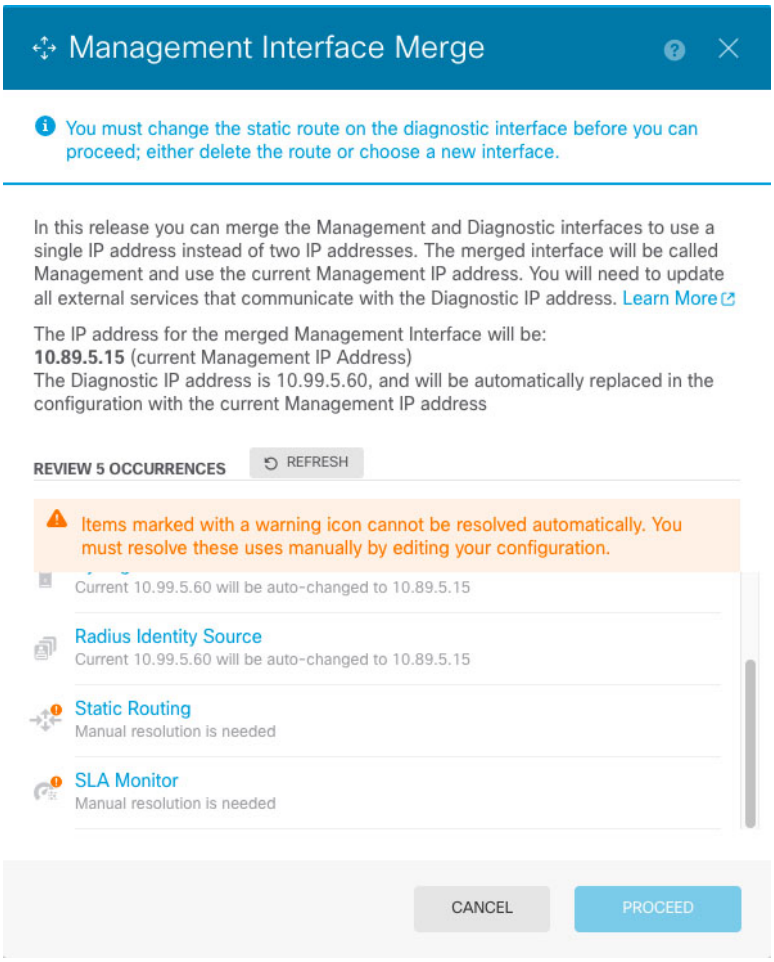
[Interfaces] テーブルの上部に、[Management Interface action needed] のメッセージとリンクが表示されます。

ステップ 2 診断インターフェイスを編集し、IP アドレスを削除します。

診断 IP アドレスを削除するまで、マージを完了できません。

ステップ 3 [Management Interface action needed] エリアの [Merge Management Interface] をクリックします。

[Management Interface Merge] ダイアログボックスに、設定内の診断インターフェイスのオカレンスがすべて表示されます。手動で設定を削除または変更する必要があるオカレンスは、警告アイコン付きで表示されます。自動移行も表示されます。



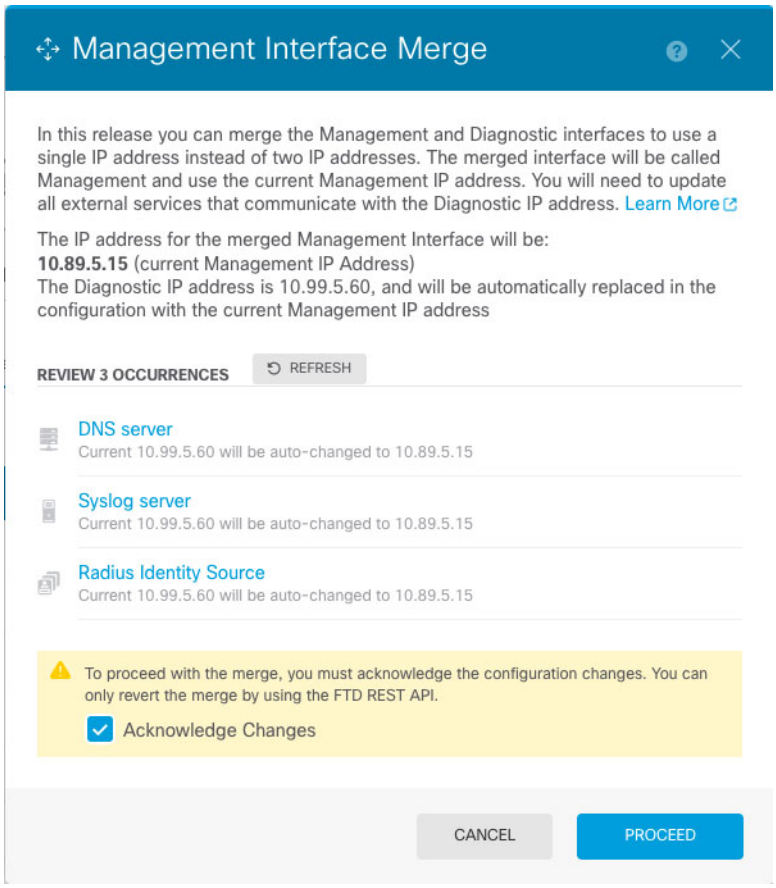
ステップ 4 リストされている設定を手動で削除または変更する必要がある場合は、次の手順を実行します。

設定を変更している間、参考のために [Management Interface Merge] ダイアログボックスは開いたままにできます。

a) 項目をクリックして設定ページを開きます。その後、項目を削除したり、データインターフェイスを選択したりできます。

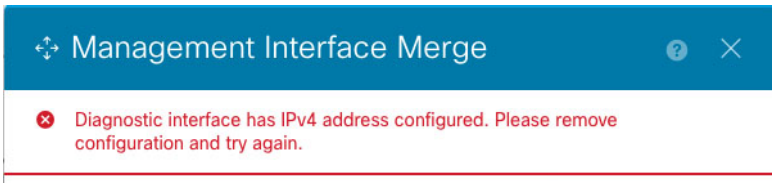
b) [Management Interface Merge] ダイアログボックスの内容を更新するには、[Refresh] をクリックします。

これで、警告は表示されなくなります。



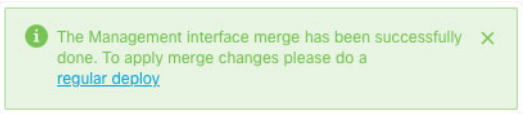
ステップ 5 [Acknowledge Changes] をクリックしてから、[Proceed] をクリックします。

診断 IP アドレスをまだ削除していない場合、次のエラーが表示されます。



この場合、診断 IP アドレスを削除してから、[Proceed] をもう一度クリックします。

設定がマージされると、成功バナーが表示されます。



ステップ 6 マージされた新しい設定を展開します。

注意 マージを続行しない場合は、展開する前に [Discard All] を使用して変更を破棄し、マージを元に戻すことができます。マージされた設定を展開すると、Device Manager からインターフェイスのマージを解除できます。ただし、診断インターフェイスは手動で再設定する必要があります。「管理インターフェイスのマージ解除（376ページ）」を参照してください。また、マージされていない設定を復元すると、デバイスはマージされていない設定に戻ります。

マージ後、[Interfaces] ページに管理インターフェイスが表示され、設定可能になります。以前は、**[System Settings]** > **[Management Interface]** ページで設定が可能でした。

ステップ 7 マージ後は、診断インターフェイスと通信する外部サービスがある場合、管理インターフェイスの IP アドレスを使用するように設定を変更する必要があります。

次に例を示します。

- SNMP クライアント
- RADIUS サーバー：RADIUS サーバーでは多くの場合、着信トラフィックの IP アドレスが確認されるため、その IP アドレスを管理アドレスに変更する必要があります。さらに、高可用性ペアの場合、プライマリとセカンダリの両方の管理 IP アドレスを許可する必要があります。診断インターフェイスは、アクティブユニットに存在する単一の「フローティング」IP アドレスをサポートしていましたが、管理インターフェイスはサポートしていません。

管理インターフェイスのマージ解除

Threat Defense 7.4 以降では、マージされた管理インターフェイスと診断インターフェイスがサポートされます。インターフェイスのマージを解除する必要がある場合は、次の手順を実行します。ネットワークをマージモード展開に移行する際は、一時的にマージ解除モードを使用することを推奨します。個別の管理インターフェイスと診断インターフェイスは、将来のすべてのリリースでサポートされなくなる可能性があります。

インターフェイスのマージを解除しても、元の診断設定は復元されません（アップグレードしてからインターフェイスをマージした場合）。診断インターフェイスを手動で再設定する必要があります。また、管理インターフェイスは「管理」という名前になり、名前を「診断」に変更することはできません。

または、バックアップ機能を使用して古いマージされていない設定を保存した場合は、その設定を復元できます。その場合、診断設定は変わらず、デバイスがマージされていない状態になります。

始める前に

- デバイスの現在のモードを表示するには、脅威に対する防御 CLI で **show management-interface convergence** コマンドを入力します。次の出力は、管理インターフェイスがマージされていることを示しています。

```
> show management-interface convergence
management-interface convergence
>
```

次の出力は、管理インターフェイスがマージされていないことを示しています。

```
> show management-interface convergence
no management-interface convergence
>
```

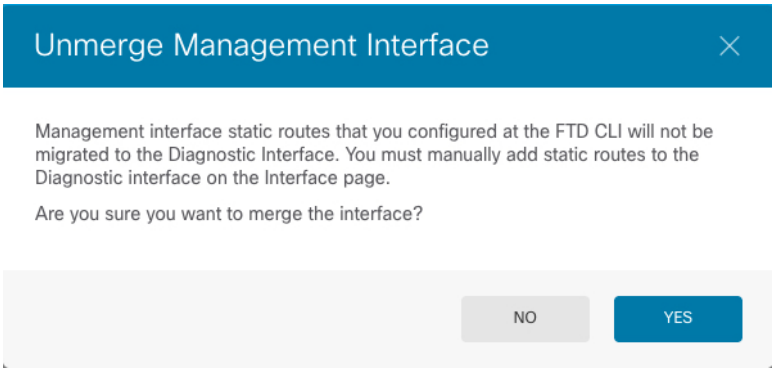
- 高可用性ペアの場合は、アクティブユニットでこのタスクを実行します。マージされていない設定は、自動的にスタンバイユニットに複製されます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

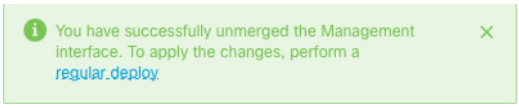
ステップ 2 [Management 1/1] インターフェイス行の右側にある [Unmerge]（[Unmerge]）をクリックし、[Unmerge Management Interface] ダイアログボックスで [Yes] をクリックします。

図 *33* : 管理インターフェイスのマージ解除



[Interfaces] ページの上部に成功メッセージが表示されます。

図 *34* : マージ解除成功



ステップ 3 新しいマージされていない設定を展開します。

マージの解除を続行しない場合は、展開する前に [Discard All] を使用して変更を破棄し、マージされたインターフェイスを保持できます。また、マージされた設定を復元すると、デバイスはマージされた設定に戻ります。

マージ解除後、**[System Settings]** > **[Management Interface]** ページに管理インターフェイスが表示され、設定可能になります。

停電時のハードウェアバイパスの設定（ISA 3000）

ハードウェア バイパスを有効にして、停電時でもトラフィックがインターフェイス ペア間を通過できるようにできます。サポートされているインターフェイスペアは銅線インターフェイスの GigabitEthernet 1/1 と 1/2、および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルを保有している場合は、銅線イーサネット ペア（GigabitEthernet 1/1 と 1/2）でのみハードウェアバイパスがサポートされます。デフォルトでは、サポートされている場合、両方のインターフェイスペアに対してハードウェアバイパスが有効になります。

ハードウェアバイパスがアクティブの場合、トラフィックはレイヤ1でそれらのインターフェイス ペア間を通過します。Device Manager と Threat Defense CLI の両方に、インターフェイスがダウンしていることが表示されます。ファイアウォール機能はないため、トラフィックのデバイス通過を許可することのリスクを理解している必要があります。

（この手順で説明されている）TCP シーケンス番号のランダム化は無効にすることをお勧めします。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 バイパスがアクティブになると、ISA 3000 はデータ パスには入らず、シーケンス番号は変換されません。受信側のクライアントが予期しないシーケンス番号を受信すると接続がドロップされるため、TCP セッションを再確立する必要があります。TCP シーケンス番号のランダム化が無効になっている場合でも、スイッチオーバー中に一時的にダウンするリンクがあるため、一部の TCP 接続は再確立する必要があります。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニターします。

始める前に

ハードウェア バイパスを機能させるための前提条件：

- インターフェイス ペアは同じブリッジ グループに配置する必要があります。
- 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 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

ページの上部にある [ハードウェアバイパス（Hardware Bypass）] セクションは、このデバイスに使用できるインターフェイスペアの現在の設定を示します。

ただし、ハードウェアバイパスを有効にする前に、ペアが同じブリッジグループで設定されていることを確認する必要があります。

ステップ 2 [編集（Edit）] をクリックしてハードウェアバイパスを設定します。

[ハードウェアバイパスの設定（Hardware Bypass Configuration）] ダイアログボックスが表示されます。

ステップ 3 自動ハードウェアバイパス動作を設定するには、インターフェイスペアごとに、[停電時のハードウェアバイパス（Hardware Bypass during Power Down）] エリアで次のいずれかのオプションを選択します。

- [無効化（Disable）]：ハードウェアバイパスを無効にします。トラフィックは、停電時にデバイスを通過しません。
- [有効化（Enable）]：停電時にハードウェアバイパスをアクティブにします。ハードウェアバイパスが、停電時にトラフィックが中断されないように確保します。バイパスされたトラフィックは検査されず、セキュリティポリシーは適用されないことに注意してください。電源が復旧したら、ハードウェアバイパスは自動的に無効になるため、トラフィックフローの通常の状態を維持することができ、検査も行われます。ハードウェアバイパスを無効にすると、トラフィックが一時的に中断する可能性があることに注意してください。
- [永続的に有効化（Enable with Persistence）]：停電時にハードウェアバイパスをアクティブにし、電源の復元後も有効な状態を維持します。電源が復旧したら、[手動ハードウェアバイパス（Manual Hardware Bypass）] スライダを使用してハードウェアバイパスを無効にする必要があります。このオプションでは、トラフィックに一時的な中断が発生したときに制御することができます。

ステップ 4 （任意） ハードウェアバイパスを手動で有効または無効にするには、[手動ハードウェアバイパス（Manual Hardware Bypass）] スライダをクリックします。

たとえば、システムをテストしたり、何らかの理由でデバイスを一時的にバイパスする必要がある場合があります。ハードウェアバイパスの状態を変更するには、設定を展開する必要があることに注意してください。設定を変更するだけでは不十分です。

ハードウェア バイパスを手動で有効化または無効化すると、次の Syslog メッセージが表示されます。メッセージ内の *pair* は 1/1-1/2 または 1/3-1/4 です。

- %FTD-6-803002：no protection will be provided by the system for traffic over GigabitEthernet *pair*
- %FTD-6-803003: User disabled bypass manually on GigabitEthernet *pair*

ステップ 5 [OK] をクリック

変更はすぐには適用されません。設定を展開する必要があります。

ステップ 6 （オプション）TCP シーケンス番号のランダム化を無効にするために必要な FlexConfig オブジェクトとポリシーを作成します。

a) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

b) 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

c) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

d) オブジェクトの名前を入力します。たとえば、 **Disable_TCP_Randomization** と入力します。

e) [テンプレート（Template）] エディタに、TCP シーケンス番号のランダム化を無効にするコマンドを入力します。

コマンドは **set connection random-sequence-number disable** ですが、ポリシーマップ内の特定のクラスに対して設定する必要があります。最も簡単なアプローチは、ランダムなシーケンス番号をグローバルに無効にする方法です。この場合、次のコマンドを入力する必要があります。

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

たとえば、TCP シーケンス番号のランダム化をグローバルに無効にしている場合、ネゲートテンプレートは次のようになります。

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) [OK] をクリックしてオブジェクトを保存します。

オブジェクトを FlexConfig ポリシーに追加する必要があります。オブジェクトを作成するだけでは十分ではありません。

h) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。

i) [グループリスト（Group List）] で [+] をクリックします。

j) [Disable_TCP_Randomization] オブジェクトを選択し、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

k) [保存（Save）] をクリックします。

これでポリシーを展開できます。

モニタリング インターフェイス

次の領域に、インターフェイスに関する一部の基本情報を表示できます。

- [デバイス（Device）]。インターフェイスの現在の状態をモニターするには、ポート グラフィックを使用します。ポートにマウスポインタを合わせると、そのポートの IP アドレス、EtherChannel メンバーシップ、有効ステータス、リンクステータスが表示されます。IP アドレスは DHCP を使用して静的に割り当てたり取得したりできます。

  インターフェイス ポートは、次のカラー コーディングを使用します。

  - 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
  - グレー：インターフェイスは無効です。
  - オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。

- **[モニタリング（Monitoring）]** > **[システム（System）]**。[スループット（Throughput）] ダッシュボードには、システムを介して移動するトラフィックに関する情報が表示されます。すべてのインターフェイスに関する情報を表示できます。または、調査する特定のインターフェイスを選択できます。
- **[モニタリング（Monitoring）]** > **[ゾーン（Zones）]**。これらのダッシュボードにはインターフェイスを設定するセキュリティ ゾーンに基づく統計情報が表示されます。詳細について、この情報を掘り下げることができます。

CLI でのインターフェイスのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、インターフェイス関連の動作と統計情報に関する詳細情報を取得することもできます。

- **show interface** はインターフェイスの統計情報と設定情報を表示します。このコマンドには多数のキーワードがあり、必要な情報を取得するために使用できます。使用可能なオプションを表示するには、「?」をキーワードとして使用します。
- **show ipv6 interface** はインターフェイスに関する IPv6 設定情報を表示します。
- **show bridge-group** は、メンバー情報や IP アドレスを含む、ブリッジ仮想インターフェイス（BVI）に関する情報を表示します。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィックフローに関する統計情報を表示します。
- **show ipv6 traffic** はデバイスを介した IPv6 トラフィックフローに関する統計情報を表示します。
- **show dhcpd** はインターフェイスの DHCP 使用状況に関する統計とその他の情報を表示し、特にインターフェイスで設定されている DHCP サーバーに関する情報が含まれます。
- **show switch vlan** は VLAN とスイッチポートの関連付けを表示します。

- **show switch mac-address-table** は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。
- **show arp** はダイナミック、スタティック、およびプロキシ ARP エントリを表示します。
- **show power inline** PoE ステータスを表示します。
- **show vpdn group** は PPPoE グループと、設定されているユーザー名と認証を表示します。
- **show vpdn username** は PPPoE のユーザー名とパスワードを表示します。
- **show vpdn session pppoe state** は PPPoE セッションのステータスを表示します。

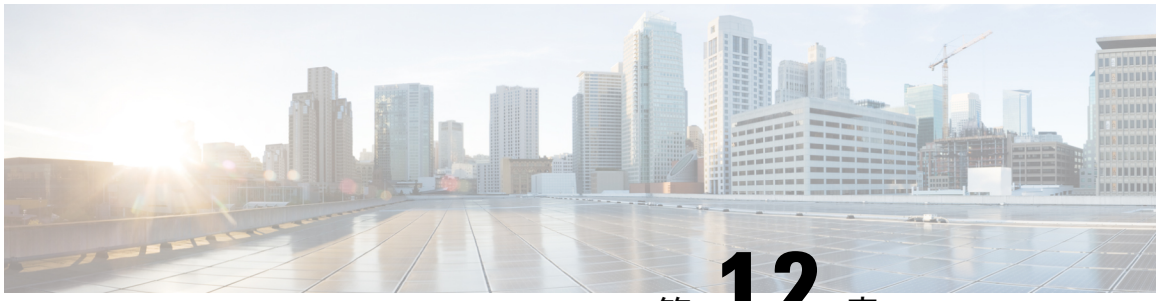
インターフェイスの例

使用例の章には、次のインターフェイス関連の例が含まれています。

- Device Manager でデバイスを設定する方法 （49 ページ）
- サブネットを追加する方法 （83 ページ）
- ネットワーク上のトラフィックをパッシブにモニタする方法 （90 ページ）

第 IV 部

ルーティング



第 12 章

ルーティングの基本ルートと静的ルート

システムはルーティングテーブルを使用して、システムに入力されるパケットの出力インターフェイスを決定します。ここでは、ルーティングの基本とデバイスで静的ルーティングを設定する方法について説明します。

ルーティングのベストプラクティス

ネットワーク内のルーティングプロセスの設計は、複雑なプロセスになる可能性があります。この章では、脅威に対する防御デバイスを、既存のネットワーク内で機能するように、およびネットワークですでに確立されているルーティングプロセスに参加するように設定していることを前提にしています。

そうではなく、新しいネットワークを作成している場合は、ルーティングプロトコルについて説明している箇所、およびネットワークに適した効果的なルーティング計画を設計する方法について説明している箇所を参照してください。この章では、プロトコルを選択するための推奨事項については説明しません。また、プロトコルの動作についても詳しく説明しません。

ネットワークが非常に小規模で、単に ISP にリンクするだけの場合は、少数のスタティックルートで十分であり、ルーティングプロトコルを実装する必要はまったくありません。

一方、多数のルータを含む大規模なネットワークを設定する場合は、内部ルーティング用に OSPF などのルーティングプロトコルを少なくとも 1 つ実装する必要があることが多く、場合によっては外部ルーティング用に BGP などのルーティングプロトコルを 1 つ実装する必要があります。サービスプロバイダーは、どのような外部ルーティングが必要になるかを理解する場合の助けになります。この状況に該当する場合は、まず 脅威に対する防御 を使用して設定可能なルーティングプロトコルを理解し、ネットワークを計画し、最後に計画に従って 脅威に対する防御 デバイスを設定します。

ルーティングの概要

ここでは、脅威に対する防御デバイス内でルーティングがどのように動作するのかを説明します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも 1 つの中間ノードがあります。ルーティングには、最適なルーティングパスの決定と、ネットワーク経由のパケットの転送という 2 つの基本的なアクティビティが含まれます。

サポートされるルーティング プロトコル

次の表では、Device Manager を使用して Threat Defense デバイスで設定できるルーティングプロトコルとテクノロジー、および設定を完了するために使用する必要があるメソッドについて説明します。

表 *8:* サポートされるルーティング プロトコル

ルーティング機能	コンフィギュレーション方式	注記
BGP	スマート CLI	**[デバイス（Device）]** > **[ルーティング（Routing）]** ページから BGP スマート CLI オブジェクトを設定します。 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトを使用してルートマップなどの BGP で使用されるオブジェクトを設定します。
Bidirectional Forwarding Detection（BFD）	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用して BFD を設定します。BFD は BGP でのみサポートされています。
EIGRP	スマートCLI	**[デバイス（Device）]** > **[ルーティング（Routing）]** ページで、EIGRP スマート CLI オブジェクトを設定します。 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトを使用してルートマップなどの EIGRP で使用されるオブジェクトを設定します。
IS-IS	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用して IS-IS を設定します。
マルチキャストルーティング	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用してマルチキャストルーティングを設定します。

ルーティング機能	コンフィギュレーション方式	注記
OSPFv2	スマートCLI	**[デバイス（Device）]** > **[ルーティング（Routing）]** ページから OSPFv2 スマート CLI オブジェクトを設定します。 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトを使用してルートマップなどの OSPFv2 で使用されるオブジェクトを設定します。
OSPFv3	—	OSPFv3 設定はサポートされていません。
ポリシーベースルーティング（PBR）	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用してポリシーベースルーティング（PBR）を設定します。
RIP	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用して RIP を設定します。
スタティックルート	Device Manager	**[デバイス（Device）]** > **[ルーティング（Device Routing）]** ページからスタティックルートをグローバルに、または仮想ルータごとに設定します。
仮想ルータ、VRF	Device Manager	**[デバイス（Device）]** > **[ルーティング（Device Routing）]** ページから仮想ルータを設定します。

ルート タイプ

ルートには、スタティックとダイナミックという 2 つのタイプがあります。

スタティックルートは、明示的に定義するものです。これらは安定した、通常は優先順位の高いルートであり、ルートの宛先へのトラフィックが常に正しいインターフェイスから送信されるようにするために使用します。たとえば、その他のルートでカバーされていないすべてのトラフィックをカバーする、デフォルトのスタティックルート（つまり IPv4 では 0.0.0.0/0、IPv6 では ::/0）を作成する場合などです。別の例では、常に使用する内部 syslog サーバーへのスタティックルートがあります。

ダイナミックルートは、OSPF、BGP、EIGRP、IS-IS、または RIP などのルーティングプロトコルの動作を通じて学習されるものです。ルートは直接定義しません。その代わりにルーティングプロトコルを設定すると、システムはネイバールータと通信してルーティングアップデートを送信し、ルーティングアップデートを順番に受信します。

ダイナミック ルーティング プロトコルはルーティングテーブルを調整し、着信ルーティング アップデート メッセージを分析することで、ネットワーク状況の変化に対応します。ネット

ワークが変化したことをメッセージが示している場合は、システム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。

スタティックルーティングは単純であり、基本的なルーティングの目的を果たします。ネットワークトラフィックが比較的予想しやすい環境や、ネットワーク設計が比較的単純な環境での使用に適しています。ただし、編集しない限りスタティックルートは変更できないため、ネットワークの変化に対応することはできません。

小規模ネットワークがある場合を除き、通常はスタティックルートを1つまたは複数のダイナミック ルーティング プロトコルと組み合わせます。明示ルートに一致しないトラフィックのデフォルトルートとして、少なくとも 1 つのスタティックルートを定義します。

（注） スマート CLI を使用して次のルーティングプロトコルを設定することができます：OSPF、BGP。FlexConfig を使用して、ASA ソフトウェアでサポートされるその他のルーティング プロトコルを設定します。

ルーティング テーブルとルート選択

NAT 変換（xlates）およびルールで出力インターフェイスを決定しない場合、システムはルーティングテーブルを使用してパケットのパスを決定します。

ルーティングテーブルのルートには、指定ルートに相対的な優先順位を定める「アドミニストレーティブ ディスタンス」というメトリックが含まれています。パケットが複数のルート エントリと一致する場合、最短距離のルート エントリが使用されます。直接接続されたネットワーク（インターフェイス上で定義されたネットワーク）の距離は0のため、これが常に優先されます。スタティック ルートのデフォルトの距離は 1 ですが、1 ～ 254 の距離で作成できます。

特定の宛先が指定されたルートは、デフォルト ルート（宛先が 0.0.0.0/0 または ::/0 のルート）よりも優先されます。

ルーティング テーブルへの入力方法

Threat Defense 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。Threat Defense デバイスは、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。

- Threat Defense デバイスが、（RIP などの）1 つのルーティングプロトコル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。

- Threat Defense デバイスが、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、Threat Defense デバイス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、Threat Defense デバイス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 *9:* 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]
VPN ルート	1
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（Unknown）	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、Threat Defense デバイスが 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、Threat Defense デバイスは 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。

VPN アドバタイズされたルート（V-Route/RRI）は、デフォルトのアドミニストレーティブディスタンス 1 のスタティックルートと同等です。ただし、ネットワークマスク 255.255.255.255 の場合と同じように優先度が高くなります。

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、Threat Defense デバイスは、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 Threat Defense デバイス 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、Threat Defense デバイス 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。

管理トラフィック用ルーティングテーブル

Threat Defense デバイスには、デバイス発信管理トラフィック用の次のルーティングテーブルが含まれています。

- Linux 管理ルーティングテーブル：Device Manager 管理セッション、ライセンス通信、データベース更新などの管理インターフェイスから送信される特別な管理トラフィックは、常に Linux 管理ルーティングテーブルを使用します。
- データルーティングテーブル：すべてのデバイス発信トラフィック（およびすべての通過トラフィック）は、デフォルトでデータルーティングテーブルを使用します。通常のデータインターフェイスはすべて、このルーティングテーブルに含まれます。ほとんどのサービスでは、特定のインターフェイスを選択できるため、そのインターフェイスに関連付けられているルートのみが使用されます。
- 管理専用ルーティングテーブル：管理専用インターフェイスに設定した管理インターフェイスとすべてのデータインターフェイスは、このルーティングテーブルに含まれます。これらのインターフェイスのいずれかからデバイス発信トラフィックを送信するには、サービスの設定時に特定の管理専用インターフェイスを選択する必要があります。DNS ルックアップの場合は例外です。ルートが見つからない場合、Threat Defense はデータを使用して自動的に管理にフォールバックすることもあります。管理専用インターフェイスにはスタティックルートを追加できますが、特殊な管理インターフェイスには追加できません。Threat Defense デバイスは、Linux にトラフィックを転送する管理用のデフォルトルートを自動的に追加します。この場合、Linux ルーティングテーブルで別のルートルックアップが行われます。Threat Defense CLI **configure network static-routes** コマンドを使用して、管理インターフェイスで使用可能な Linux ルーティングテーブルにスタティックルートを追加できます。

（注） デフォルトの Linux ルートは、**configure network ipv4** または **configure network ipv6** コマンドで設定します。

（注） 管理インターフェイスとレガシー診断インターフェイスをまだマージしていないデバイスについては、このガイドの 7.3 より前のバージョンを参照してください。

等コスト マルチパス（ECMP）ルーティング

Threat Defense デバイス 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。Threat Defense デバイスでは、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。

スタティック ルート

スタティック ルートを作成して、ネットワークの基本的なルーティングを提供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。

デフォルトルート

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、Threat Defense デバイス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。

脅威に対する防御 には、データインターフェイスと管理専用インターフェイス（特別な Linux 管理インターフェイスを含む）用の個別のルーティングテーブルがあります。データルーティングテーブルのデフォルトルートのみ追加できます。脅威に対する防御 は、Linux 管理インターフェイスにトラフィックを送信する管理専用ルーティングテーブルにデフォルトルートを自動的に追加します。このルートでは、Linux ルーティングテーブルで個別のルートルックアップが行われます。脅威に対する防御 CLI **configure network static-routes** コマンドを使用して、管理インターフェイスで使用可能な Linux ルーティングテーブルにスタティックルートを追加できます。

（注） デフォルトの Linux ルートは、**configure network ipv4** または **configure network ipv6** コマンドで設定します。

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、Threat Defense デバイス 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。

スタティック ルートのバックアップとスタティック ルートのトラッキング

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、関連付けられたインターフェイスがダウンした場合にのみルーティングテーブルから削除されます。

ルート トラッキングを実装すると、サービス レベル契約（SLA）モニターを使用してスタティック ルートの可用性を追跡し、プライマリ ルートが失敗したら自動的にバックアップ ルートをインストールすることができます。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。

ルートトラッキングを使用する場合、トラッキング対象のルートに宛先ネットワークのターゲット IP アドレスを関連付けます。その後、システムは ICMP エコー要求を使用して、そのアドレスに到達できることを定期的に確認します。指定された時間内にエコー応答がない場合、そのホストは到達不能と見なされ、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。

したがって、デフォルトルートなどの特定の宛先にバックアップ スタティック ルートを使用するには、次を実行する必要があります。

1. ゲートウェイや常時稼働サーバー（Web サーバーや syslog サーバーなど）のような、宛先ネットワーク上の信頼できる IP アドレスをモニターする SLA モニターを作成します。宛先ネットワークが正常で使用可能な間は、オフラインになる可能性があるシステムの IP アドレスをモニターしないでください。「SLA モニター オブジェクトの設定（399 ページ）」を参照してください。
2. 宛先へのプライマリルートを作成し、ルートの SLA モニターを選択します。このルートのメトリックは通常 1 です。「スタティック ルートの設定（396 ページ）」を参照してください。
3. プライマリルートが失敗した場合に使用されるバックアップ スタティック ルートを作成します。このルートには、プライマリルートより大きいメトリックが必要です。たとえば、プライマリルートが 1 の場合、バックアップルートは 10 にできます。また、通常はバックアップ ルートとは異なるインターフェイスを選択します。

スタティック ルーティングのガイドライン

ブリッジ グループ

- ルーテッド モードでは、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。
- 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 Threat Defense デバイス で発信されるトラフィックの場合（syslog または SNMP など）、Threat Defense デバイス 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。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。

- 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。

IPv6

- スタティック ルート トラッキング（SLA モニター）は、IPv6 ではサポートされていません。

等コストマルチパス（ECMP）トラフィック ゾーン

- ECMP トラフィック ゾーンのメンバー インターフェイスを同じセキュリティ ゾーンに保持して、これらのインターフェイスに異なるアクセス ルール、SSL ルール、または ID ルールが適用されないようにします。
- 特定の ECMP トラフィック ゾーンのネットワークには最大 8 つの等コスト ルートを設定できます。
- 最大 256 の ECMP トラフィック ゾーンを作成でき、ゾーンごとに最大 8 つのインターフェイスを使用できます。
- ECMP ゾーンには、物理インターフェイス、サブインターフェイス、および EtherChannel を含めることができます。次のものを含めることはできません。
  - ブリッジ グループ（BVI）またはそのメンバー
  - EtherChannel メンバー インターフェイス
  - HA インターフェイス（フェールオーバーまたはステートリンク）
  - 管理専用インターフェイス
  - サイト間 VPN 接続またはリモート アクセス VPN 接続に使用されるインターフェイス。
  - 仮想トンネル インターフェイス（VTI）またはその送信元インターフェイス。
  - VPN 管理アクセス用に設定されたインターフェイス。
- 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。

スタティック ルートの設定

システムのインターフェイスに直接接続されているネットワークに向かわないパケットの送信先をシステムに伝えるため、スタティック ルートを定義します。

少なくとも 1 つのスタティック ルート、ネットワーク 0.0.0.0/0 のデフォルト ルートが必要になります。このルートは、既存の NAT xlates（変換）またはスタティック NAT ルール、またはその他のスタティック ルートでは出力インターフェイスを判別できないパケットの送信先を定義します。

デフォルト ゲートウェイを使用してもすべてのネットワークに到達できない場合、他のスタティック ルートが必要になる可能性があります。たとえば、デフォルト ルートは通常、外部インターフェイスの上流に位置するルータです。デバイスに直接接続されていない追加の内部ネットワークがあり、それらにデフォルト ゲートウェイを介してアクセスできない場合、これらそれぞれの内部ネットワークに対してスタティック ルートが必要です。

システムのインターフェイスに直接接続されたネットワークのスタティック ルートを定義することはできません。システムは自動でこれらのルートを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーにあるリンクをクリックします。

ステップ 2 仮想ルータを有効にした場合は、スタティック ルートを設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [ルーティングの選択（Select Routing）] ページで、次のいずれかを実行します。

- 新しいルートを追加するには、[+] をクリックします。
- 編集するルートの編集アイコン（  ）をクリックします。

ルートが不要になったら、ルートの [ごみ箱（trash can）] アイコンをクリックして削除します。

ステップ 4 ルート プロパティの設定

- [名前（Name）]：ルートの表示名です。
- [説明（Description）]：ルートの目的に関する任意の説明です。
- [インターフェイス（Interface）]：トラフィックの送信経路となるインターフェイスを選択します。ゲートウェイ アドレスは、このインターフェイスを介してアクセス可能である必要があります。

  ブリッジ グループの場合、メンバー 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（BVI）のルートを設定します。

  仮想ルーティングと転送を有効にしている場合は、別の仮想ルータに属するインターフェイスを選択できます。別の仮想ルータのインターフェイスについて、仮想ルータでスタティックルートを作成すると、そのルートは仮想ルータの境界を越え、この仮想ルータからのトラフィックが別の仮想ルータにリークするリスクがあります。望ましい結果である可能性もありますが、このルートリークが必要かどうかを慎重に判断してください。インターフェイスを選択すると、インターフェイスが属する仮想ルータの名前がインターフェイスの右側に表示されます。
- [プロトコル（Protocol）]：ルートが **IPv4** アドレス用か **IPv6** アドレス用かを選択します。
- [ネットワーク（Networks）]：このルートでゲートウェイを使用する必要のある宛先ネットワークまたは宛先ホストを識別するネットワークオブジェクトを選択します。

デフォルト ルートを定義するには、事前定義された any-ipv4 または any-ipv6set ネットワーク オブジェクトを使用するか、または 0.0.0.0/0（IPv4）または ::/0（IPv6）ネットワークのオブジェクトを作成します。

- [ゲートウェイ（Gateway）]：ゲートウェイの IP アドレスを識別するホスト ネットワーク オブジェクトを選択します。トラフィックはこのアドレスに送信されます。複数のインターフェイス上のルートには同じゲートウェイを使用できません。

  仮想ルータでルートを定義し、そのインターフェイスが別の仮想ルータに属している場合は、ゲートウェイを空のままにしておく必要があります。これらのネットワークへのトラフィックは他の仮想ルータにルーティングされ、ターゲット仮想ルータのルーティング テーブルを使用してゲートウェイが決定されます。

- [メトリック（Metric）]：ルートのアドミニストレーティブ ディスタンス。1 ～ 254 の範囲で指定します。スタティックルートのデフォルト値は 1 です。インターフェイスとゲートウェイの間に追加ルータがある場合、アドミニストレーティブディスタンスとしてホップ数を入力します。

  アドミニストレーティブディスタンスは、ルートを比較するために使用されるパラメータです。番号が低いほど、ルートに高い優先順位が与えられます。接続されたルート（デバイスのインターフェイスに直接接続されているネットワーク）は、スタティック ルートよりも常に優先されます。

ステップ 5 （任意、IPv4 ルートのみ）このルートの有効性を追跡する [SLAモニター（SLA Monitor）] を選択します。

SLA モニターでは、ターゲットネットワーク上の常時利用可能なホストが到達可能であることを確認できます。到達不能になった場合、システムはバックアップルートをインストールできます。したがって、SLA モニターを設定する場合は、このネットワークに対してより大きなメトリックを持つ別のスタティックルートも設定する必要があります。たとえば、このルートのメトリックが 1 である場合は、メトリック 10 のバックアップルートを作成します。詳細については、「スタティック ルートのバックアップとスタティック ルートのトラッキング （394 ページ）」を参照してください。

SLA モニター オブジェクトがまだ存在しない場合は、リストの下部にある [SLAモニターの作成（Create SLA Monitor）] リンクをクリックしてここで作成します。

（注） モニター対象のアドレスを ping できないことが原因でモニター対象のルートが削除された場合、このルートは、ルートが到達不能であることを示す警告とともにスタティックルートテーブルに示されます。問題が一時的なものであるのか、またはルートを再設定する必要があるのかを確認します。ルートが有効でも、モニター対象のアドレスが十分に信頼できない可能性もあります。

ステップ 6 [OK] をクリックします。

SLA モニター オブジェクトの設定

スタティックルートとともに使用するためのサービスレベル契約（SLA）モニターオブジェクトを設定します。SLA モニターを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。ルート トラッキングの詳細については、スタティック ルートのバックアップとスタティック ルートのトラッキング（394 ページ）を参照してください。

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。ターゲットには、ホスト ネットワーク オブジェクトで定義された任意の IP アドレスを指定できますが、次の使用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）。
- システム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 IP アドレス。夜間にシャットダウンされる可能性のあるワークステーションは、適切な選択肢ではありません。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [SLAモニタ（SLA Monitors）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 SLA モニターの必須オプションを定義します。

- [モニターアドレス（Monitor Address）]：宛先ネットワークでモニターするアドレスを定義するホスト ネットワーク オブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。

  このアドレスは、SLA モニタをスタティックルートに接続している場合にのみモニタされます。

- [ターゲットインターフェイス（Target Interface）]：エコー要求パケットを送信するインターフェイスを選択します。これは通常、スタティックルートを定義するインターフェイスになります。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。

ステップ 5 （オプション）[IP ICMPエコーオプション（IP ICMP Echo Options）] を調整します。

すべてのICMPオプションには、ほとんどの場合に適合するデフォルト値がありますが、要件に合わせて調整できます。

- [しきい値（Threshold）]：宣言する上昇しきい値（ミリ秒）（0 ～ 2147483647 の間）。デフォルトは5000（5秒）です。この値は、タイムアウトに設定された値以下にする必要があります。しきい値は、しきい値超過イベントを示すためだけに使用され、到達可能性には影響しません。しきい値イベントの頻度を使用すると、タイムアウトの設定を評価できます。
- [タイムアウト（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（ミリ秒）（0 ～ 604800000 ミリ秒（7 日間）の間）。デフォルト値は 5,000 ミリ秒（5 秒）です。モニターがこの期間中に少なくとも 1 つのエコー要求への応答を受信しなかった場合、プロセスはバックアップルートをインストールします。
- [頻度（Frequency）]：SLA プローブ間のミリ秒数（1,000 ～ 604,800,000、1,000 の倍数単位）。タイムアウト値未満の頻度は設定できません。デフォルトは60,000ミリ秒（60秒）です。
- [サービスタイプ（Service Type）]：ICMP エコー要求パケットの IP ヘッダーの Type of Service（ToS）タイプを定義する整数（0 ～ 255 の間）。デフォルトは 0 です。
- [パケットの数（Number of Packets）]：各ポーリングを送信するパケットの数（1 ～ 100 の間）。デフォルトは 1 パケットです。
- [データサイズ（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（0 ～ 16384 バイトの間）。デフォルト値は 28 です。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。

ステップ 6 [OK] をクリックします。

これで、スタティック ルートで SLA モニター オブジェクトを使用することができます。

ECMP トラフィックゾーンの設定

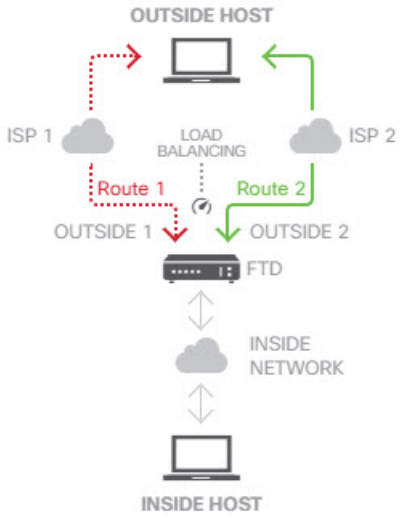
通常、同じルートメトリックを使用して特定のネットワークプレフィックスに複数のルートを設定するには、同じインターフェイスでルートを設定する必要があります。そのため、システムは、等コストマルチパス（ECMP）ルーティング計算を使用して、インターフェイス経由でゲートウェイに送信されるトラフィックのロードバランシングを実現します。

たとえば、次のように、異なるゲートウェイを指定する複数のデフォルトルートを外部インターフェイスに設定でき、この設定は追加の変更なしで許可されます。

```
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
```

また、ECMPを使用して、同じネットワークプレフィックスおよびルートメトリックの複数のインターフェイス（仮想ルータ内）間でトラフィックのバランシングを実現することもできます。この設定は、複数の個別インターフェイスを介してゲートウェイにアクセスできる場合に必要です。たとえば、ISP が 2 つあり、ISP 間でロードバランシングを行いたいものの、ISP ゲートウェイ間で内部アドレス空間を分割したくないとします。一方の ISP には outside1 インターフェイスを介してアクセスでき、もう一方の ISP には outside2 インターフェイスを介してアクセスできます。これを実現するには、outside1 インターフェイスと outside2 インターフェイスを含むルーティング トラフィック ゾーンを作成する必要があります。

```
isp-zone containing outside1 and outside2
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 10.1.1.3
```



（注） ECMP ルーティング トラフィック ゾーンはセキュリティゾーンに関連していません。outside1 インターフェイスと outside2 インターフェイスを含むセキュリティゾーンを作成しても、ECMP ルーティング用のトラフィックゾーンは実装されません。

次の手順で、インターフェイス間で ECMP 処理を利用するように ECMP ゾーンを設定する方法について説明します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーにあるリンクをクリックします。

ステップ 2 仮想ルータを有効にした場合は、スタティック ルートを設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [ECMPトラフィックゾーン（ECMP Traffic Zones）] タブをクリックします。

ステップ 4 [ECMPトラフィックゾーン（ECMP Traffic Zones）] ページで、次のいずれかを実行します。

- 新しいゾーンを追加するには、[+] または [ECMP トラフィックゾーンの追加（Add ECMP Traffic Zone）] をクリックします。
- 編集するゾーンの編集アイコン（  ）をクリックします。

ゾーンが不要になった場合は、ゾーンのごみ箱アイコンをクリックして削除します。ゾーンを削除する前に、そのゾーンに依存するすべての静的ルートを削除する必要があります。

ステップ 5 ゾーンの [名前（Name）] を入力し、必要に応じて説明を入力します。

ステップ 6 [インターフェイス（Interfaces）] で、ゾーンに含める最大 8 つのインターフェイス選択します。

- [+] をクリックして、インターフェイスを追加します。
- 削除するには、インターフェイスの右横にある [x] をクリックします。

インターフェイスを選択する際は、次の制限事項に注意してください。

- 物理インターフェイス、サブインターフェイス、および EtherChannel を選択できます。
- ECMP トラフィックゾーンに含めることのできないインターフェイスのタイプは、ブリッジグループ（BVI）やそのメンバー、Etherchannel メンバーインターフェイス、HA インターフェイス（フェールオーバーリンクまたはステートリンク）、管理専用インターフェイス、仮想トンネルインターフェイス（VTI）、または VPN 管理アクセス用に設定されたインターフェイスです。
- リモートアクセスまたはサイト間 VPN 接続で使用されるインターフェイスを含めることはできません。
- DHCP リレーが有効になっているインターフェイスは、サーバーまたはエージェントとして選択できません。
- インターフェイスは同じ仮想ルータに割り当てる必要があります。
- 1 つのインターフェイスは 1 つのトラフィックゾーンにのみ含まれます。

ステップ 7 [OK] をクリック

次のタスク

これで、[スタティックルート（Static Routes）] タブに移動し、これらのインターフェイスを介した同じ宛先への等コストルートを作成できます。または、動的ルーティングプロトコルがシステムを通じて配布される場合、等コストルートを自動的に設定できます。

ルーティングのモニタリング

ルーティングをモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。また、[ルーティング

（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

- **show route** はデータインターフェイスのルーティングテーブルを表示します。直接接続されたネットワークのルートが含まれます。
- **show ipv6 route** はデータインターフェイスの IPv6 ルーティングテーブルを表示します。直接接続されたネットワークのルートが含まれます。
- **show network** は管理インターフェイスの設定を表示します。管理ゲートウェイが含まれます。管理インターフェイスを介したルーティングは、データインターフェイスを管理ゲートウェイとして指定しない限り、データ インターフェイス ルーティング テーブルによって処理されません。
- **show network-static-routes** は、**configure network static-routes** コマンドを使用して、管理インターフェイスに対して設定されたスタティックルートを表示します。通常、ほとんどの場合、管理ゲートウェイは管理ルーティングに対して十分機能するため、スタティックルートは存在しません。これらのルートは、データインターフェイス上のトラフィックには使用できません。このコマンドは、CLI コンソールでは使用できません。
- **show ospf** は OSPF プロセスと学習ルートに関する情報を表示します。OSPF に関する特定の情報を表示するために含めることができるオプションのリストを取得するには、**show ospf ?** を使用します。
- **show bgp** は BGP プロセスと学習ルートに関する情報を表示します。BGP に関する特定の情報を表示するために含めることができるオプションのリストを取得するには、**show bgp ?** を使用します。
- **show eigrp** *option* は EIGRP プロセスと学習ルートに関する情報を表示します。含めることができるオプションのリストを取得するには、**show eigrp ?** を使用します。オプションを指定する必要があります。
- **show isis** *option* は IS-IS プロセスと学習ルートに関する情報を表示します。含めることができるオプションのリストを取得するには、**show isis ?** を使用します。オプションを指定する必要があります。
- **show rip database** は RIP プロセスと学習ルートに関する情報を表示します。
- **show vrf** は、システムで定義されている仮想ルータの情報を表示します。
- **show zone** は ECMP トラフィックゾーンに関する情報（各ゾーンに含まれるインターフェイスなど）を表示します。

第 13 章

仮想ルータ

仮想ルータを作成して、インターフェイスのサブセットのトラフィックを相互に分離することができます。

仮想ルータと Virtual Routing and Forwarding（VRF）について

複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。

これにより、共通のネットワーク機器のセットを使用して、2 件以上のお客様にサポートを提供できます。また、仮想ルータを使用して、独自のネットワーク要素をより明確に分離することもできます。たとえば、開発ネットワークを汎用企業ネットワークから分離することができます。

仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。

仮想ルータを作成するときに、インターフェイスをルータに割り当てます。特定のインターフェイスを 1 つのみの仮想ルータに割り当てることができます。次に、スタティックルートを定義し、各仮想ルータに OSPF や BGP などのルーティングプロトコルを設定します。また、ネットワーク全体で個別のルーティングプロセスを設定し、すべての参加デバイス上のルーティングテーブルが、仮想ルータごとの同じルーティングプロセスとテーブルを使用するようにします。仮想ルータを使用して、同じ物理ネットワーク上に論理的に分離されたネットワークを作成し、各仮想ルータを通過するトラフィックのプライバシーを確保します。

ルーティングテーブルは個別にあるため、仮想ルータ全体で同じ、または重複するアドレス空間を使用できます。たとえば、2 つの別個の物理インターフェイスでサポートされている 2 つの別個の仮想ルータ用に、192.168.1.0/24 アドレス空間を使用できます。

仮想ルータごとに個別の管理およびデータのルーティングテーブルがあることに注意してください。たとえば、管理専用インターフェイスを仮想ルータに割り当てると、そのインターフェイスのルーティングテーブルは、仮想ルータに割り当てられたデータインターフェイスとは別のものになります。

ポリシーを仮想ルータ対応にするための設定

仮想ルータを作成する場合、その仮想ルータのルーティングテーブルは、グローバル仮想ルータまたは他の仮想ルータから自動的に分離されます。ただし、セキュリティポリシーは自動的に仮想ルータ対応にはなりません。

たとえば、「任意の」送信元または宛先のセキュリティゾーンに適用されるアクセス制御ルールを作成する場合、ルールはすべての仮想ルータのすべてのインターフェイスに適用されます。実はこれがまさに必要な機能かもしれません。たとえば、すべてのお客様が、同じリストの好ましくない URL カテゴリへのアクセスをブロックしたい場合があります。

ただし、いずれかの仮想ルータにのみポリシーを適用する必要がある場合は、その 1 つの仮想ルータからのインターフェイスのみを含むセキュリティゾーンを作成する必要があります。その後、セキュリティポリシーの送信元と宛先の条件に、仮想ルータが制約されたセキュリティゾーンを使用します。

メンバーシップが 1 つの仮想ルータに割り当てられたインターフェイスに制限されたセキュリティゾーンを使用することにより、次のポリシーで仮想ルータ対応ルールを作成できます。

- アクセス コントロール ポリシー
- 侵入およびファイルポリシー。
- SSL 復号ポリシー。
- アイデンティティポリシーと、ユーザーから IP アドレスへのマッピング。仮想ルータで重複するアドレス空間を使用する場合は、仮想ルータごとに個別のレルムを作成し、アイデンティティ ポリシー ルールでそれらを正しく適用してください。

仮想ルータで重複するアドレス空間を使用する場合は、適切なポリシーが適用されるようにセキュリティゾーンを使用する必要があります。たとえば、2 つの個別の仮想ルータで 192.168.1.0/24 アドレス空間を使用する場合、192.168.1.0/24 ネットワークを指定するだけのアクセスコントロールルールは、両方の仮想ルータのトラフィックに適用されます。これが求める結果ではない場合は、1 つの仮想ルータのみに対して送信元/宛先セキュリティゾーンも指定することで、ルールの適用を制限できます。

NAT などのセキュリティゾーンを使用しないポリシーでは、1 つの仮想ルータに割り当てられたインターフェイスを送信元インターフェイスと宛先インターフェイスとして選択することによって、仮想ルータ固有のルールを作成できます。2 つの個別の仮想ルータから送信元インターフェイスと宛先インターフェイスを選択する場合は、ルールが機能するよう、仮想ルータ間に適切なルートがあることを確認する必要があります。

仮想ルータ間のルーティング

仮想ルータ間でトラフィックをルーティングするようにスタティックルートを設定できます。

たとえば、グローバル仮想ルータに外部インターフェイスがある場合、外部インターフェイスにトラフィックを送信するために、他の各仮想ルータでスタティック デフォルト ルートを設定できます。その後、特定の仮想ルータ内でルーティングできないトラフィックは、その後のルーティングのためにグローバルルータに送信されます。

仮想ルータ間のスタティックルートは、別の仮想ルータにトラフィックをリークしているため、ルートリークと呼ばれます。ルートをリークしている場合（VR2 への VR1 ルートなど）、VR2 から VR1 のみへの接続を開始できます。トラフィックが VR1 から VR2 に流れるようにするには、逆ルートを設定する必要があります。別の仮想ルータのインターフェイスへのスタティックルートを作成する場合は、ゲートウェイアドレスを指定する必要はありません。単純に宛先インターフェイスを選択します。

仮想ルータ間ルートの場合、システムは送信元の仮想ルータ内で宛先インターフェイスルックアップを行います。次に、宛先の仮想ルータでネクストホップの MAC アドレスを検索します。したがって、宛先の仮想ルータには、宛先アドレスに対して選択されたインターフェイスのダイナミック（学習済み）ルートまたはスタティックルートのいずれかが設定されている必要があります。

異なる仮想ルータで送信元インターフェイスと宛先インターフェイスを使用する NAT ルールを設定すると、仮想ルータ間でトラフィックをルーティングすることもできます。ルートルックアップを実行するために NAT のオプションを選択しない場合、宛先の変換が発生するたびに、NAT 変換アドレスを使用して宛先インターフェイスからトラフィックが送信されます。ただし、宛先の仮想ルータには、ネクストホップルックアップが成功するように、変換後の宛先 IP アドレスのルートが設定されている必要があります。

デバイスモデルごとの仮想ルータの最大数

作成できる仮想ルータの最大数は、デバイスモデルによって異なります。次の表に、上限を示します。**show vrf counters** コマンドを入力して、システムでダブルチェックできます。これにより、グローバル仮想ルータを含まない、そのプラットフォームのユーザー定義仮想ルータの最大数が表示されます。次の表の数字には、ユーザールータとグローバルルータが含まれています。Firepower 4100/9300 の場合、これらの数字はネイティブモードに適用されます。

Firepower 4100/9300 などのマルチインスタンス機能をサポートするプラットフォームでは、仮想ルータの最大数をデバイス上のコア数で割ってから、インスタンスに割り当てられたコア数を乗じて最も近い整数に丸めることにより、コンテナインスタンスごとの仮想ルータの最大数を決定します。たとえば、プラットフォームが最大 100 の仮想ルータをサポートする環境で、70 のコアが存在する場合、各コアは最大 1.43（切り上げた数）の仮想ルータをサポートします。したがって、6 つのコアが割り当てられたインスタンスは、8.58 の仮想ルータをサポートします（この数は 8 に切り下げる）。10 のコアが割り当てられたインスタンスは、14.3 の仮想ルータをサポートします（この数は 14 に切り下げる）。

デバイス モデル	最大仮想ルータ数
Firepower 1010	このモデルでは仮想ルータはサポートされていません。
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Cisco Secure Firewall 3105	10
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Firepower 9300 appliance、すべてのモデル	100
Threat Defense Virtual、すべてのプラットフォーム	30
ISA 3000	10

仮想ルータのガイドライン

デバイスモデルのガイドライン

次を除くすべての対応デバイスモデルで、仮想ルータを設定できます。

- Firepower 1010

その他のガイドライン

- 次の機能は、グローバル仮想ルータでのみ設定できます。
  - OSPFv3
  - RIP
  - EIGRP
  - IS-IS
  - BGPv6
  - 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
  - [VPN]
- 次の機能は、仮想ルータごとに個別に設定できます。
  - スタティックルートとその SLA モニター。
  - OSPFv2
  - BGPv4
- 次の機能は、リモートシステムに対してクエリまたは通信を行うときに（from-the-box トラフィック）、システムによって使用されます。これらの機能は、グローバル仮想ルータのインターフェイスのみを使用します。この機能のインターフェイスを設定する場合、そのインターフェイスはグローバル仮想ルータに属している必要があります。一般的なルールとして、システムがその管理の目的で外部サーバーに到達するためにルートを特定する必要がある場合は、グローバル仮想ルータでルートルックアップが行われます。
  - アクセス制御ルールで使用される完全修飾名を解決する場合、または **ping** コマンドの名前解決に使用されるDNSサーバー。DNSサーバーのインターフェイスとして**any**を指定すると、グローバル仮想ルータのインターフェイスのみ考慮されます。
  - AAA サーバーまたはアイデンティティレルム（VPN で使用する場合）。VPN はグローバル仮想ルータのインターフェイスでのみ設定できるため、VPNに使用される外部 AAA サーバー（Active Directory など）が、グローバル仮想ルータのインターフェイスを介して到達可能である必要があります。
  - Syslog サーバー。
  - SNMP。
- NAT では、異なる仮想ルータに割り当てられた送信元インターフェイスと宛先インターフェイスを指定すると、NAT ルールにより、ある仮想ルータから別の仮想ルータにトラフィックが転送されます。NAT ルール内のインターフェイスが意図せず混在していないことを確認します。通常は送信元と宛先のインターフェイスが使用され、ルーティングテーブルは無視され、手動 NAT での宛先変換も無視されます。ただし、NAT ルールでルートルックアップを実行する必要がある場合、インバウンド インターフェイスの VRF

テーブルでのみルックアップが実行されます。必要に応じて、宛先インターフェイスに対して送信元仮想ルータでスタティックルートを定義します。インターフェイスを [任意（any）] のままにした場合は、仮想ルータのメンバーシップに関係なく、すべてのインターフェイスにルールが適用されることに注意してください。仮想ルータを使用する場合は、NAT ルールを慎重にテストして、想定どおりに動作することを確認します。必要なルートリークを定義しておかないと、場合によっては、ルールが適合すると予想されるすべてのトラフィックにルールが適合せず、変換が適用されません。

- 仮想ルータ間のルートを設定する場合（ある仮想ルータから2番目の仮想ルータへのルートをリークする場合など）、システムは送信元の仮想ルータで宛先インターフェイスルックアップを実行します。次に、宛先の仮想ルータでネクストホップの MAC アドレスを検索します。したがって、宛先の仮想ルータには、宛先アドレスに対して選択されたインターフェイスのダイナミック（学習済み）ルートまたはスタティックルートのいずれかが設定されている必要があります。
- たとえば、仮想ルータ 1 から仮想ルータ 2 への仮想ルータ間ルート（リークルート）を使用する場合は、リターントラフィックを許可するために仮想ルータ 2 にミラー（リバース）ルートを設定する必要はありません。ただし、どちらの方向でも接続を開始できるようにする場合は、仮想ルータ 1 から 2、および仮想ルータ 2 から 1 の両方の方向にルートがリークしていることを確認します。
- ある仮想ルータから別の仮想ルータにインターフェイスを移動すると、そのインターフェイスに設定されているすべての機能が保持されます。設定を調べて、スタティックルート、IP アドレス、およびその他のポリシーが新しい仮想ルータのコンテキスト内で有効なことを確認します。
- 複数の仮想ルータで重複するアドレス空間を使用する場合は、Cisco Identity Services Engine（ISE）からダウンロードした IP アドレスマッピングへのスタティック セキュリティ グループ タグ（SGT）は仮想ルータに対応していないことに注意してください。仮想ルータごとに異なる SGT マッピングを作成する必要がある場合は、仮想ルータごとに個別のアイデンティティレルムを設定します。これは、各仮想ルータで同じ IP アドレスを同じ SGT 番号にマッピングする場合には必要ありません。
- 複数の仮想ルータで重複するアドレス空間を使用すると、ダッシュボードデータが紛らわしくなる可能性があります。同じ IP アドレスの接続は集約されます。そのため、同じ IP アドレスが 2 つ以上のエンドポイントで共有されている場合は、そのアドレスで送受信されるトラフィックが増加したように見えます。個別のアイデンティティレルムを使用してアイデンティティポリシーを慎重に作成すると、ユーザーベースの統計情報はより正確になります。
- オーバーラップしている DHCP アドレスプールは、別の仮想ルータでは使用できません。
- DHCP サーバーの自動設定は、グローバル仮想ルータのインターフェイスでのみ使用できます。自動設定は、ユーザ定義の仮想ルータに割り当てられているインターフェイスではサポートされていません。
- グローバル仮想ルータから新しいルータへの移動を含め、仮想ルータ間でインターフェイスを移動すると、そのインターフェイスを介した既存の接続はすべて切断されます。

- セキュリティ インテリジェンス ポリシーは、仮想ルータに対応していません。IP アドレス、URL、または DNS 名をブロックリストに追加すると、すべての仮想ルータに対してブロックされます。

仮想ルータの管理

仮想ルータと呼ばれる複数の Virtual Routing and Forwarding（VRF）インスタンスを作成して、インターフェイスのグループに対して個別のルーティングテーブルを維持できます。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。

これにより、共通のネットワーク機器のセットを使用して、2 件以上のお客様にサポートを提供できます。また、仮想ルータを使用して、独自のネットワーク要素をより明確に分離することもできます。たとえば、開発ネットワークを汎用企業ネットワークから分離することができます。

デフォルトでは、仮想ルーティングは無効になっています。すべてのデバイスで、データ（通過）および管理（ボックス間）トラフィック用に、1 つのグローバル ルーティング テーブルのセットが使用されます。

仮想ルーティングを有効にすると、最初のルーティングページは、システムで定義されている仮想ルータの一覧になります。仮想ルータを有効にしない場合、最初のルーティングページは、システムで定義されているスタティックルートの一覧になります。

グローバル仮想ルータは、常に存在します。グローバルルータは、個別の仮想ルータに割り当てられていないすべてのインターフェイスを保持します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーにあるリンクをクリックします。

ステップ 2 まだ仮想ルータを有効にしていない場合は、[複数の仮想ルータの追加（Add Multiple Virtual Routers）] リンクをクリックし、次に [最初のカスタム仮想ルータの作成（Create First Custom Virtual Router）] をクリックします。

最初の仮想ルータの作成は、基本的に、追加の仮想ルータの作成と同じです。詳細については、「仮想ルータの作成またはインターフェイス割り当ての編集（412 ページ）」を参照してください。

ステップ 3 次のいずれかを実行します。

- すべての仮想ルータに適用されるグローバル BGP を設定するには、[BGPグローバル設定（BGP Global Settings）] ボタンをクリックします。これらの設定は、スマート CLI を使用して行います。これについては、Smart CLI オブジェクトの設定（1041 ページ）で説明しています。1 つ以上の仮想ルータで BGP を設定する場合にのみ、グローバル BGP 設定を設定します。

- 新しいルータを作成するには、仮想ルータのリストの上にある [+] ボタンをクリックします。
- たとえば、スタティックルートを作成したり、ルーティングプロセスを定義したりするために、仮想ルータのルーティングプロパティを編集するには、仮想ルータの [アクション（Action）] セルの表示アイコン（）をクリックします。
- 仮想ルータの名前、説明、またはインターフェイスの割り当てを編集するには、仮想ルータの [アクション（Action）] セルの表示アイコン（）をクリックし、[仮想ルータのプロパティ（Virtual Router Properties）] タブを選択します。
- 仮想ルータの表示を切り替えるには、仮想ルータ名の横（ルーティングテーブルの上）にある下向き矢印をクリックし、目的の仮想ルータを選択します。[仮想ルータに戻る（Go Back To Virtual router）] 矢印（）をクリックすると、リストページに戻ることができます。
- 仮想ルータを削除するには、仮想ルータの [アクション（Action）] セルの削除アイコン（）をクリックするか、仮想ルータの内容を表示するときに仮想ルータ名の横に表示される削除アイコンをクリックします。最後の仮想ルータ（削除できないグローバルルータ以外）を削除すると、VRF は無効になります。
- 仮想ルータのルーティングをモニターするには、その仮想ルータのテーブル内のいずれかの **show** コマンドのリンクをクリックします。コマンドをクリックすると CLI コンソールが開き、CLI コマンドの出力を調べることができます。ルート、OSPF、および OSPF ネイバーに関する情報を表示できます。コマンド出力は展開された設定に基づいていることに注意してください。展開されていない編集内容は表示されません。

  これらのコマンドは、仮想ルータを表示するときに [コマンド（Commands）] ドロップダウンリストから選択して実行することもできます。

仮想ルータの作成またはインターフェイス割り当ての編集

仮想ルータでスタティックルートまたはルーティングプロセスを設定するには、その前にルータを作成し、インターフェイスを割り当てる必要があります。

始める前に

[インターフェイス（Interface）] ページに移動し、仮想ルータに追加する各インターフェイスに名前が付いていることを確認します。仮想ルータに名前を付けるまでは、仮想ルータにインターフェイスを追加できません。

手順

ステップ 1 **[デバイス（Device）]** > **[ルーティング（Routing）]** をクリックします。

ステップ 2 次のいずれかを実行します。

- まだ仮想ルータを作成していない場合は、[複数の仮想ルータの追加（Add Multiple Virtual Routers）] リンクをクリックし、次に [最初のカスタム仮想ルータの作成（Create First Custom Virtual Router）] をクリックします。
- 仮想ルータのリストの上にある [+] ボタンをクリックして、新しいルータを作成します。
- 仮想ルータの編集アイコン（  ）をクリックして、そのプロパティとインターフェイスリストを編集します。
- 仮想ルータを表示している場合は、[仮想ルータのプロパティ（Virtual Router Properties）] タブをクリックして、表示している仮想ルータのプロパティを編集します。
- 仮想ルータを表示している場合は、仮想ルータ名の横にある下矢印をクリックし、[仮想ルータの新規作成（Create New Virtual Router）] をクリックします。

ステップ 3 仮想ルータのプロパティを設定します。

- [名前（Name）]：仮想ルータの名前。
- [説明（Description）]：仮想ルータの説明（任意）。
- [インターフェイス（Interfaces）]：[+] をクリックして、仮想ルータの一部となる各インターフェイスを選択します。インターフェイスを削除するには、インターフェイス上にカーソルを合わせ、インターフェイスカードの右側にある [X] をクリックします。仮想ルータには物理インターフェイス、サブインターフェイス、ブリッジグループ、および EtherChannel を割り当てられますが、VLAN は割り当てられません。

  他のインターフェイスへのルートを意図的に仮想ルーティングテーブルにリークしない限り、ルーティングテーブルはこれらのインターフェイスに制限されます。

ステップ 4 [OK] または [保存（Save）] をクリックします。

この仮想ルータのビューが表示されます。ここでスタティックルートまたはルーティングプロセスを設定できます。

仮想ルータのスタティックルートとルーティングプロセスの設定

各仮想ルータには、個別のスタティックルートとルーティングプロセスがあります。これは、他の仮想ルータに定義されているルートおよびルーティングプロセスとは別に動作します。

スタティックルートを設定する場合は、仮想ルータの外部にある宛先インターフェイスを選択できます。これにより、宛先インターフェイスを含むルートが仮想ルータにリークされます。他の仮想ルータに必要以上のトラフィックを送信しないように、リークが必要なルートだけをリークするようにします。たとえば、インターネットへのパスが 1 つの場合、インターネット宛てのトラフィックについて、各仮想ルータからインターネットに接する仮想ルータへのルートをリークすることが理にかなっています。

手順

ステップ 1 **[デバイス（Device）]** > **[ルーティング（Routing）]** を選択します。

ステップ 2 仮想ルータを開くには、ルータの [アクション（Action）] セルにある表示アイコン（  ）をクリックします。

ステップ 3 次のいずれかを実行します。

- スタティックルートを設定するには、[スタティックルーティング（Static Routing）] タブをクリックしてから、ルートを作成または編集します。詳細については、スタティックルートの設定 （396 ページ）を参照してください。
- 等コストマルチパス（ECMP）トラフィックゾーンを設定するには、[ECMPトラフィックゾーン（ECMP Traffic Zones）] タブをクリックし、ゾーンを作成します。詳細については、ECMP トラフィックゾーンの設定 （400 ページ）を参照してください。
- BGPルーティングプロセスを設定するには、[BGP] タブをクリックし、プロセスを定義するために必要なスマートCLIオブジェクトを作成します。詳細については、ボーダー ゲートウェイ プロトコル（BGP） （505 ページ）を参照してください。

  すべての仮想ルータに適用されるBGPのグローバル設定もあります。これらのプロパティを設定するには、仮想ルータのリストページに戻り、[BGPグローバル設定（BGP Global Settings）] ボタンをクリックします。
- OSPF ルーティングプロセスを設定するには、[OSPF] タブをクリックしてから、最大2つのプロセスを定義するために必要なスマートCLIオブジェクトを作成し、それらに関連付けられたインターフェイス設定を作成します。詳細については、Open Shortest Path First （OSPF） （457 ページ）を参照してください。
- （グローバル仮想ルータのみ）EIGRP ルーティングプロセスを設定するには、[EIGRP] タブをクリックし、単一プロセスを定義するために必要な Smart CLI オブジェクトを作成します。詳細については、Enhanced Interior Gateway Routing Protocol（EIGRP） （483 ページ）を参照してください。

仮想ルータの削除

仮想ルータが不要になった場合は、削除できます。グローバル仮想ルータを削除することはできません。

仮想ルータを削除すると、その仮想ルータ内で設定されているすべてのスタティックルートとルーティングプロセスも削除されます。

仮想ルータに割り当てられたすべてのインターフェイスは、グローバルルータに再割り当てされます。

手順

ステップ 1 **[デバイス（Device）]** > **[ルーティング（Routing）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 仮想ルータのリストで、仮想ルータの[アクション（Action）]列にある削除アイコン（）をクリックします。
- 削除する仮想ルータを表示している場合、ルータ名の横にある削除アイコン（）をクリックします。

仮想ルータを削除することの確認を求められます。

ステップ 3 [OK] をクリックして削除を実行します。

仮想ルータの例

次のトピックでは、仮想ルータの実装例を示します。

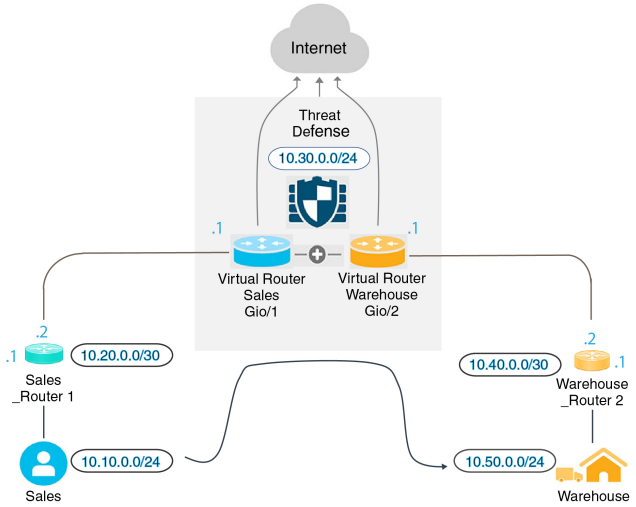
関連トピック

サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法 （823 ページ）
異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法 （913 ページ）

複数の仮想ルータを介して遠隔サーバーにルーティングする方法

仮想ルータを使用する場合、1 つの仮想ルータのユーザーが、別の仮想ルータを介してのみ到達可能なサーバーにアクセスする必要がある場合があります。

次の図を考えてみましょう。セールスチームのワークステーションは、Sales 仮想ルータに接続されています。ウェアハウスサーバーは、Warehouse 仮想ルータを介して接続されます。販売チームが、IP アドレスが 10.50.0.5/24 であるウェアハウスサーバーの情報を検索する必要がある場合は、Sales 仮想ルータからのルートを Warehouse 仮想ルータにリークする必要があります。また、Warehouse 仮想ルータは、Warehouse Router 2 から数ホップ離れたウェアハウスサーバーへのルートも持っている必要があります。



始める前に

この例では、すでに以下の設定が実施されていることを前提としています。

- Threat Defense デバイスの Sales と Warehouse の両方の仮想ルータで、GigabitEthernet 0/1 が Sales に割り当てられ、GigabitEthernet 0/2 が Warehouse に割り当てられています。
- Sales Router 1 には、10.20.0.1/30 インターフェイスから 10.50.0.5/24 にトラフィックを送信するスタティックルートまたはダイナミックルートのいずれかが含まれています。

手順

ステップ 1 10.50.0.5/24 または 10.50.0.0/24 のネットワークオブジェクトを作成します。また、ゲートウェイ（10.40.0.2/30）のオブジェクトを作成します。

ルートをウェアハウスサーバーの単一の IP アドレスに制限する場合は、ホストオブジェクトを使用して 10.50.0.5 を定義します。または、販売チームが倉庫内の他のシステムにアクセスできるようにするには、10.50.0.0/24 ネットワークのネットワークオブジェクトを作成します。この例では、ホスト IP アドレスのルートを作成します。

a) [オブジェクト（Objects）] を選択し、目次から [ネットワーク（Networks）] を選択します。

b) [+] をクリックし、次にウェアハウスサーバーのオブジェクトプロパティを入力します。

c) [OK] をクリック

d) [+] をクリックし、次にウェアハウスネットワークへのルータゲートウェイのオブジェクトプロパティを入力します。

e) [OK] をクリック

ステップ 2 Warehouse 仮想ルータの Gi0/2 インターフェイスをポイントする、Sales でのルートリークを定義します。

この例では、Gi0/1 に inside という名前が付けられており、Gi0/2 には inside-2 という名前が付けられています。

a) [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] のサマリーで [設定の表示（View Configuration）] をクリックします。

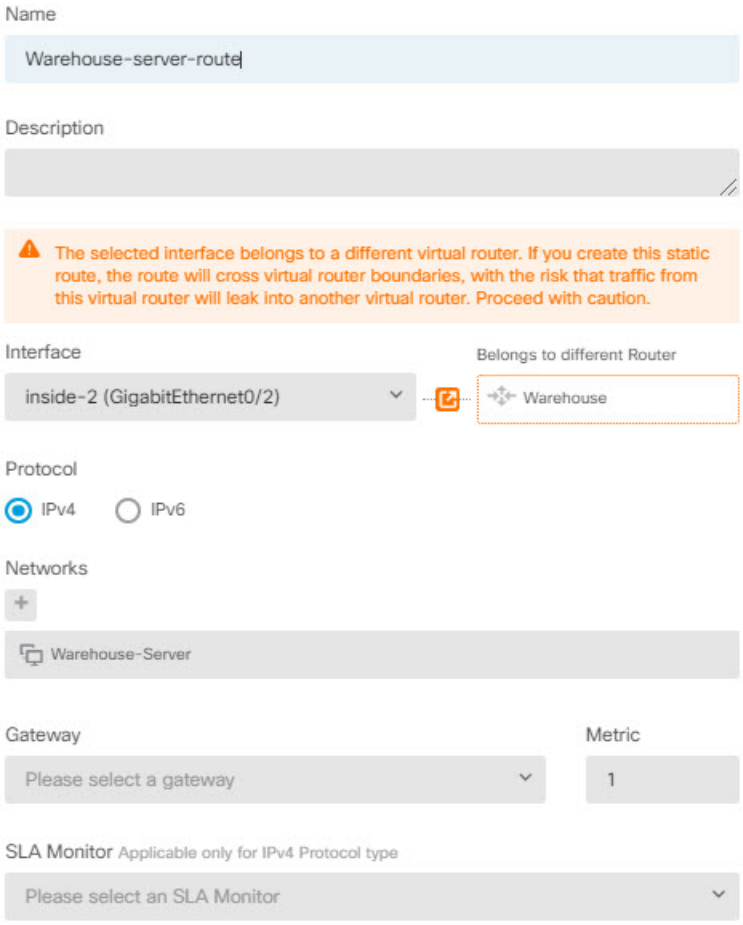
b) 仮想ルータのリストで、Sales 仮想ルータの [アクション（Action）] 列にある [表示（view）] アイコン（ ）をクリックします。

c) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：Warehouse-server-route など、任意の名前が付けられます。

- [インターフェイス（Interface）]：**inside-2** を選択します。インターフェイスが別のルータにあり、ルートリークを作成しているという警告が表示されます。これを今から実行します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。または、IPv6 アドレスを使用してこの例を実装することもできます。
- [ネットワーク（Networks）]：Warehouse-Server オブジェクトを選択します。
- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。

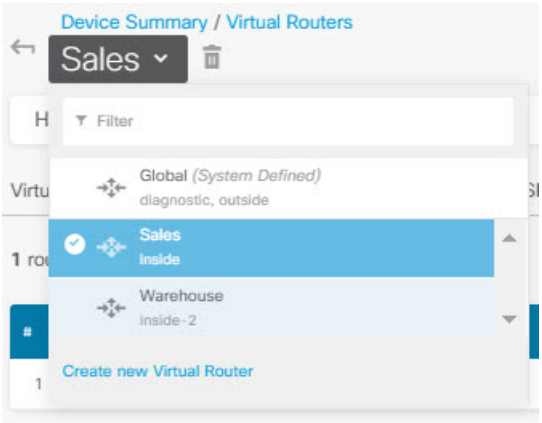


d) [OK] をクリック

ステップ 3 Warehouse 仮想ルータで、Warehouse Router 2 のゲートウェイを指すルートを定義します。

または、Warehouse Router 2 からルートを動的に検出するルーティングプロトコルを設定することで、これを行うことができます。この例では、スタティックルートを定義します。

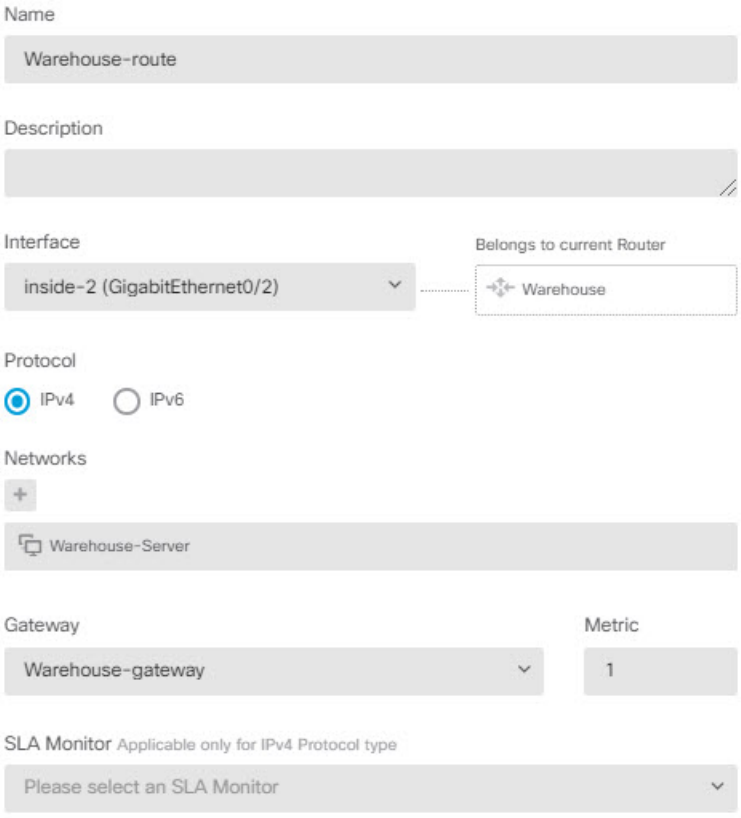
a) 現在 Sales と示されている仮想ルータのドロップダウンから、Warehouse 仮想ルータを選択してルータを切り替えます。



b) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：Warehouse-route など、任意の名前が付けられます。
- [インターフェイス（Interface）]：**inside-2** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]：Warehouse-Server オブジェクトを選択します。
- [ゲートウェイ（Gateway）]：Warehouse-gateway オブジェクトを選択します。

次のようなダイアログが表示されるはずです。

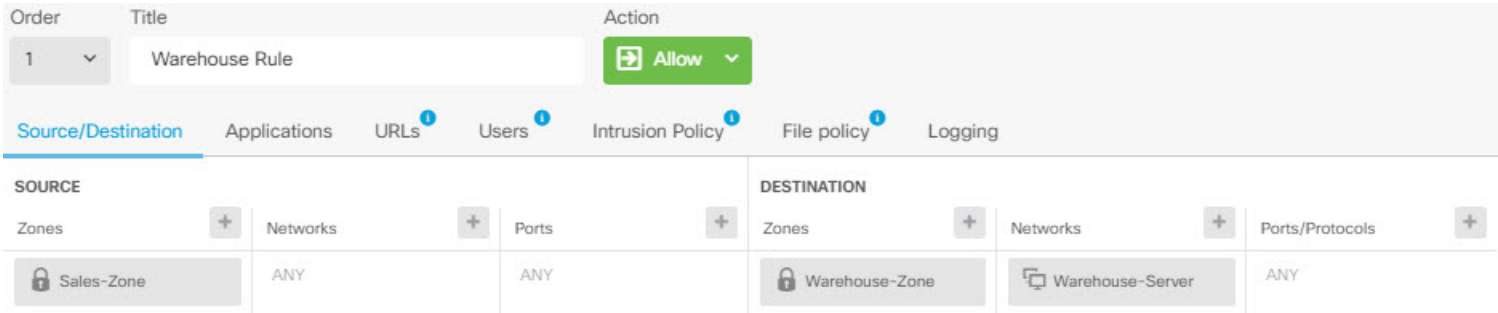


c) [OK] をクリック

ステップ 4 ウェアハウスサーバーへのアクセスを許可するアクセス制御ルールがあることを確認します。

最も単純なルールは、Sales 仮想ルータの送信元インターフェイスから、宛先 Warehouse-Server ネットワークオブジェクトの Warehouse 仮想ルータ内の宛先インターフェイスへのトラフィックを許可するものです。適切な侵入インスペクションをトラフィックに適用できます。

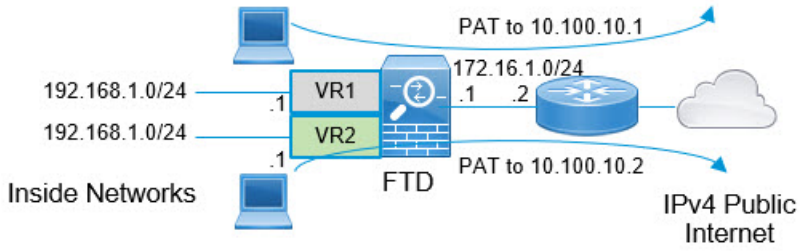
たとえば、Sales のインターフェイスが Sales-Zone セキュリティゾーンにあり、Warehouse のインターフェイスが Warehouse-Zone セキュリティゾーンにある場合、アクセスコントロールルールは次のようになります。



重複するアドレス空間を持つ複数の仮想ルータへのインターネットアクセスを提供する方法

仮想ルータを使用する場合、別のルータに存在するインターフェイスに対して同じネットワークアドレスを設定できます。たとえば、inside および inside-2 のインターフェイスをどちらも IP アドレス 192.168.1.1/24 を使用するように定義し、192.168.1.0/24 ネットワーク内のセグメント上のエンドポイントを管理することができます。ただし、これらの個別の仮想ルータでルーティングされる IP アドレスは同じであるため、リターントラフィックが正しい宛先に到達するように、仮想ルータから発信されるトラフィックを慎重に処理する必要があります。

たとえば、同じアドレス空間を使用する 2 つの仮想ルータからのインターネットアクセスを許可するには、NAT ルールを各仮想ルータ内のインターフェイスに個別に適用する必要があります。それぞれ別の NAT または PAT プールを使用することが理想的です。PAT を使用して、仮想ルータ 1 の送信元アドレスを 10.100.10.1 に変換し、仮想ルータ 2 の送信元アドレスを 10.100.10.2 に変換することができます。次の図は、インターネット側の外部インターフェイスがグローバルルータの一部である場合の設定を示しています。送信元インターフェイスを明示的に選択した NAT/PAT ルールを定義する必要があります。これは、送信元インターフェイスとして「any」を使用すると、同じ IP アドレスが 2 つの異なるインターフェイスに存在する可能性があるため、システムが正しい送信元を識別できなくなるからです。



（注） この例では、各仮想ルータに 1 つのインターフェイスが含まれています。「inside」仮想ルータに複数のインターフェイスがある場合は、「inside」インターフェイスごとに NAT ルールを作成する必要があります。重複するアドレス空間を使用しない仮想ルータ内にいくつかのインターフェイスがある場合でも、NAT ルールで送信元インターフェイスを明示的に特定することでトラブルシューティングが容易になり、インターネットにバインドされた仮想ルータからのトラフィックを確実に分離できるようになります。

手順

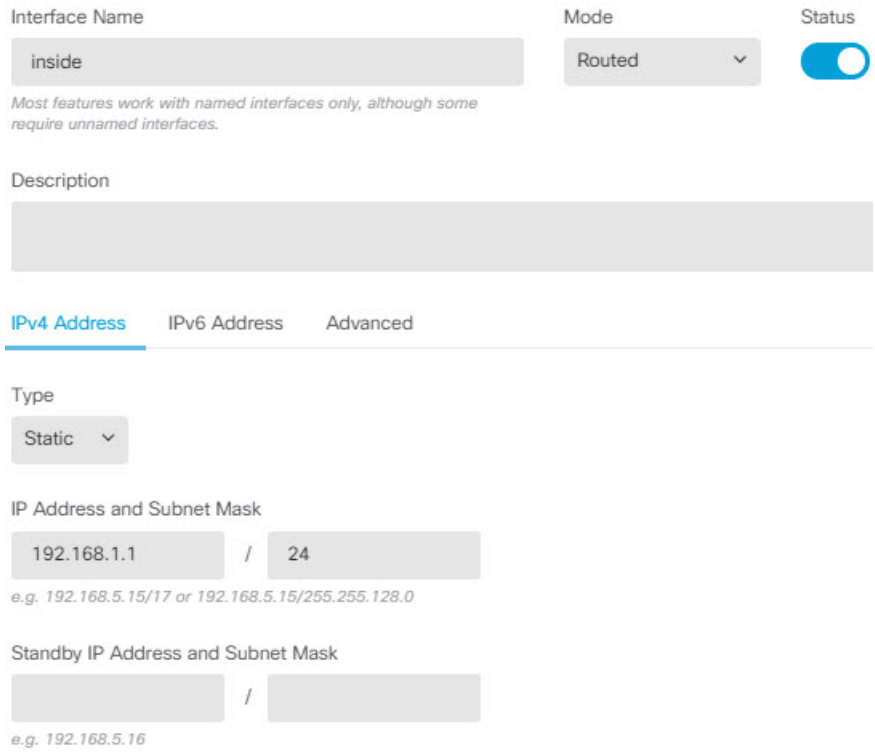
ステップ 1 仮想ルータ 1（VR 1）の内部インターフェイスを設定します。

a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

b) VR 1 に割り当てるインターフェイスの [アクション（Action）] 列にある編集アイコン（）をクリックします。

c) 少なくとも次のプロパティを設定します。

- [名前（Name）]：この例では **inside**。
- [モード（Mode）]：[ルーテッド（Routed）] を選択します。
- [ステータス（Status）]：インターフェイスを有効にします。
- [IPv4アドレスタイプ（IPv4 Address Type）]：[スタティック（Static）] を選択します。
- [IPv4アドレスとサブネットマスク（IPv4 Address and Subnet Mask）]：192.168.1.1/24 と入力します。



d) [OK] をクリック

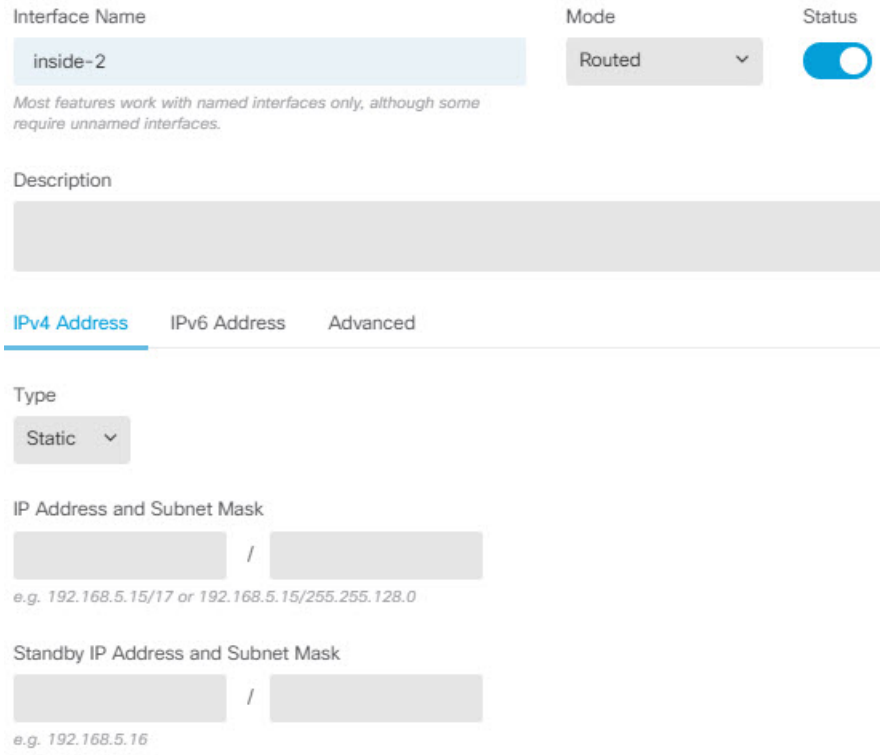
ステップ 2 仮想ルータ 2（VR2）の inside-2 インターフェイスを設定しますが、IP アドレスは指定しないでください。

a) [インターフェイス（Interface）] リストページで、VR2 に割り当てるインターフェイスの [アクション（Action）] 列にある編集アイコン（）をクリックします。

b) 少なくとも次のプロパティを設定します。

- [名前（Name）]：この例では **inside-2**。
- [モード（Mode）]：[ルーテッド（Routed）] を選択します。
- [ステータス（Status）]：インターフェイスを有効にします。
- [IPv4アドレスタイプ（IPv4 Address Type）]：[スタティック（Static）] を選択します。

- [IPv4アドレスとサブネットマスク（IPv4 Address and Subnet Mask）]：これらのフィールドは空欄のままにします。この時点で inside インターフェイスと同じアドレスを設定しようとすると、システムによってエラーメッセージが表示され、機能しない設定は作成できなくなります。同じルータ内の異なるインターフェイスを介して同じアドレス空間にルーティングすることはできません。



c) [OK] をクリック

ステップ 3 外部インターフェイスへのスタティック デフォルト ルート リークを含む、仮想ルータ VR1 を設定します。

a) [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] のサマリーで [設定の表示（View Configuration）] をクリックします。

b) ルーティングページの上部にある [複数の仮想ルータの追加（Add Multiple Virtual Router）] をクリックします。

c) 説明パネルの右下にある [最初のカスタム仮想ルータの作成（Create First Custom Virtual Router）] をクリックします。

d) 仮想ルータ VR1 のプロパティを入力します。

- [名前（Name）]：VR1 または選択した別の名前を入力します。
- [インターフェイス（Interfaces）]：[+] をクリックし、**inside** を選択して [OK] をクリックします。

e) [OK] をクリック

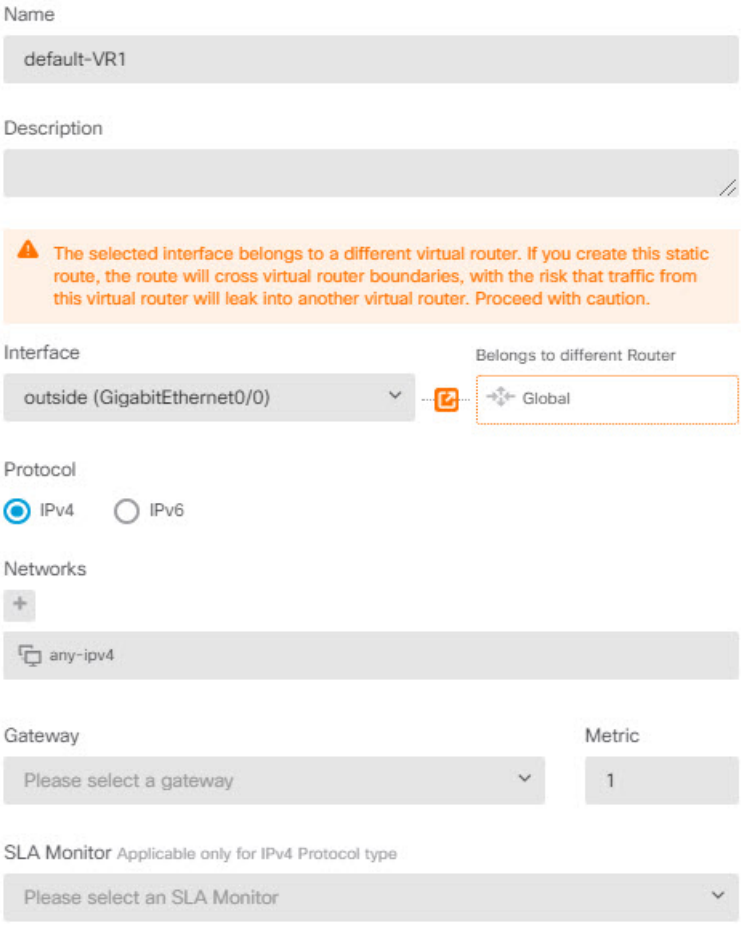
ダイアログボックスが閉じ、仮想ルータのリストが表示されます。

f) 仮想ルータのリストで、VR1 仮想ルータの [アクション（Action）] 列にある [表示（view）] アイコン（ ）をクリックします。

g) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：**default-VR1** などの任意の名前を指定します。
- [インターフェイス（Interface）]：**outside** を選択します。インターフェイスが別のルータにあり、ルートリークを作成しているという警告が表示されます。これを今から実行します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。
- [ネットワーク（Networks）]：**any-ipv4** オブジェクトを選択します。これは、VR1 内でルーティングできないすべてのトラフィックのデフォルトルートになります。
- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



h) [OK] をクリック

ステップ 4 外部インターフェイスへのスタティック デフォルト ルート リークを含む、仮想ルータ VR2 を設定します。

a) VR1 を表示している場合は、戻るボタン（⮌）をクリックして仮想ルータのリストに戻ります。

b) リストの先頭にある [+] をクリックします。

c) 仮想ルータ VR2 のプロパティを入力します。

- [名前（Name）]：VR2 または選択した別の名前を入力します。
- [インターフェイス（Interfaces）]：[+] をクリックし、**inside-2** を選択して [OK] をクリックします。

d) [OK] をクリック

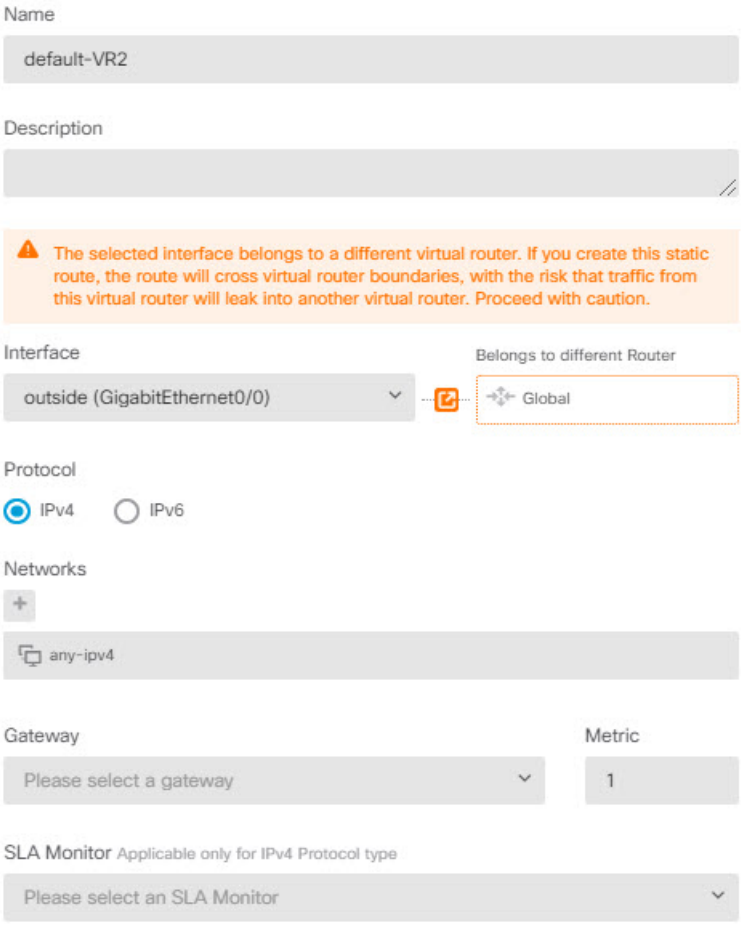
ダイアログボックスが閉じ、仮想ルータのリストが表示されます。

e) 仮想ルータのリストで、VR2 仮想ルータの [アクション（Action）] 列にある [表示（view）] アイコン（）をクリックします。

f) [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：**default-VR2** などの任意の名前を指定します。
- [インターフェイス（Interface）]：**outside** を選択します。インターフェイスが別のルータにあり、ルートリークを作成しているという警告が表示されます。これを今から実行します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。
- [ネットワーク（Networks）]：**any-ipv4** オブジェクトを選択します。これは、VR2 内でルーティングできないすべてのトラフィックのデフォルトルートになります。
- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。

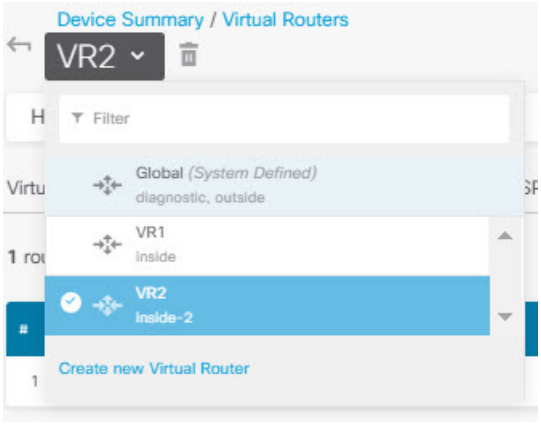


g) [OK] をクリック

ステップ 5 外部インターフェイスへのグローバルルータのデフォルトルートを作成します。

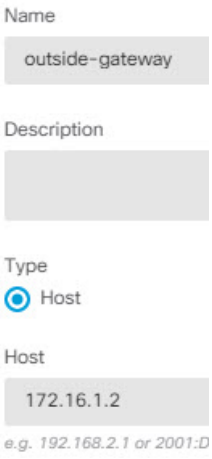
このルートの目的は、2 つの仮想ルータからグローバルルータの外部インターフェイスへのトラフィックリークに適切なゲートウェイを割り当てることです。

a) VR2 を表示している場合は、ページの上部にある VR2 の名前をクリックして仮想ルータのリストを開き、グローバルルータを選択します。

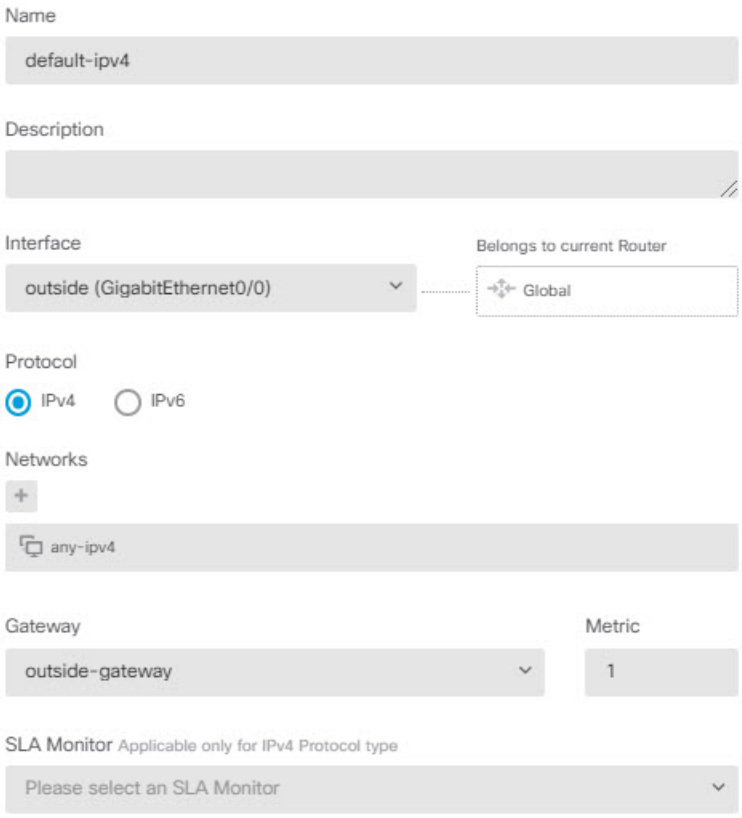


b) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：default-ipv4 などの任意の名前を指定します。
- [インターフェイス（Interface）]：**outside** を選択します。
- [プロトコル（Protocol）]：この例では、**IPv4** を使用します。
- [ネットワーク（Networks）]：**any-ipv4** オブジェクトを選択します。これは、任意の IPv4 トラフィックのデフォルトルートになります。
- [ゲートウェイ（Gateway）]：オブジェクトがまだ存在していないと仮定して、[新規ネットワークオブジェクトの作成（Create New Network Object）] をクリックし、外部インターフェイス（この場合は 172.16.1.2）のネットワークリンクの反対側にあるゲートウェイの IP アドレスに対してホストオブジェクトを定義します。オブジェクトを作成したら、そのオブジェクトをスタティックルートの [ゲートウェイ（Gateway）] フィールドで選択します。



次のようなダイアログが表示されるはずです。



c) [OK] をクリック

ステップ 6 [インターフェイス（Interface）] ページに戻り、inside-2 に IP アドレスを追加します。

a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。

b) VR2 に割り当てる inside-2 インターフェイスの [アクション（Action）] 列にある編集アイコン（）をクリックします。

c) [IPv4アドレス（IPv4 Address）] タブで、IP アドレスとサブネットマスクとして 192.168.1.1/24 と入力します。

d) [OK] をクリック

この時点では、inside および inside-2 インターフェイスが別の仮想ルータにあるため、重複する IP アドレスに対するエラーは発生しません。

ステップ 7 inside to outside トラフィックの 10.100.10.1 への PAT を実行する NAT ルールを作成します。

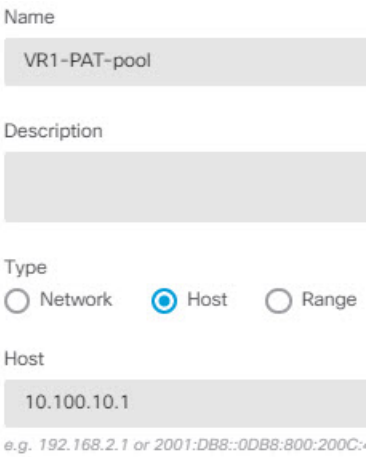
a) [ポリシー（Policies）] を選択し、[NAT] をクリックします。

b) 内部から外部インターフェイスに InsideOutsideNatRule という名前の手動 NAT ルールがすでに存在する場合、インターフェイス PAT を適用するには、ルールの編集アイコン（）をクリックします。そうでない場合は、[+] をクリックして新しいルールを作成します。

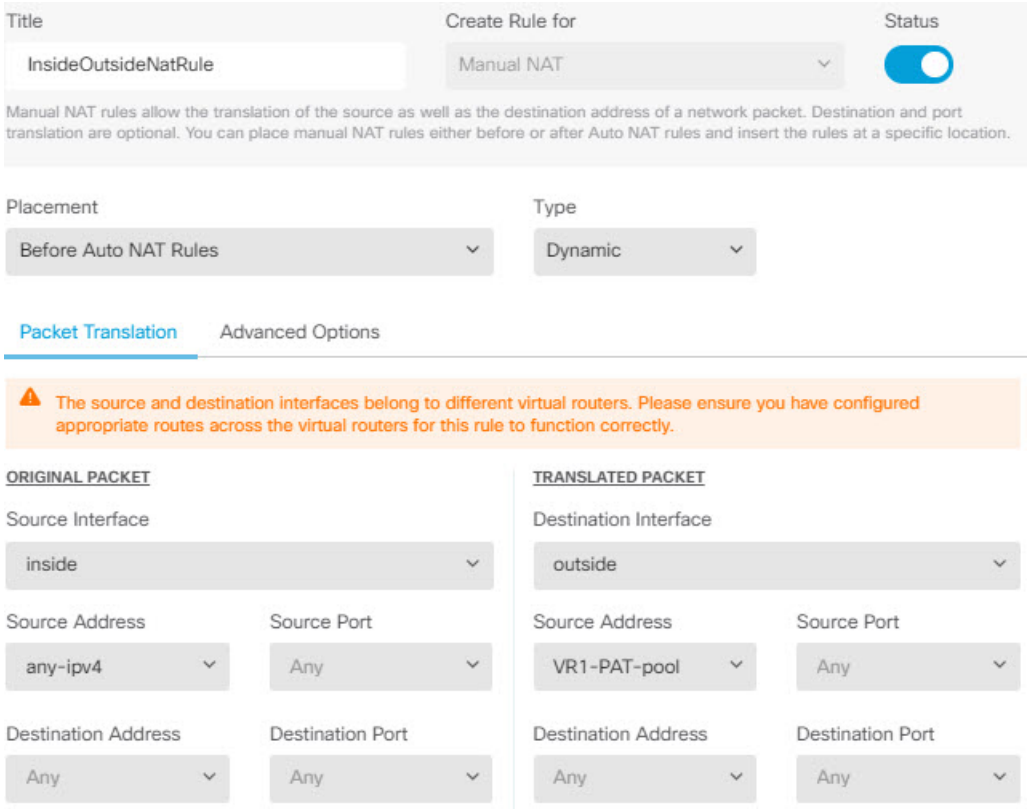
既存のルールを編集する場合は、送信元インターフェイスと宛先インターフェイスが異なる仮想ルータにあり、ルートを定義する必要があることを示す警告が表示されることに注意してください。これは、前の手順で行ったものです。

c) 既存のルールを編集する場合は、**[変換済みパケット（Translated Packet）]** > **[送信元アドレス（Source Address）]** のドロップダウン矢印をクリックし、[新規ネットワークの作成（Create New Network）] をクリックします（10.100.10.1 を定義しているホストオブジェクトがない場合）。

d) PAT アドレスのホスト ネットワーク オブジェクトを設定します。オブジェクトは次のようになります。



e) **[変換済みパケット（Translated Packet）]** > **[送信元アドレス（Source Address）]** として新しいオブジェクトを選択します。NAT ルールは次のようになります。



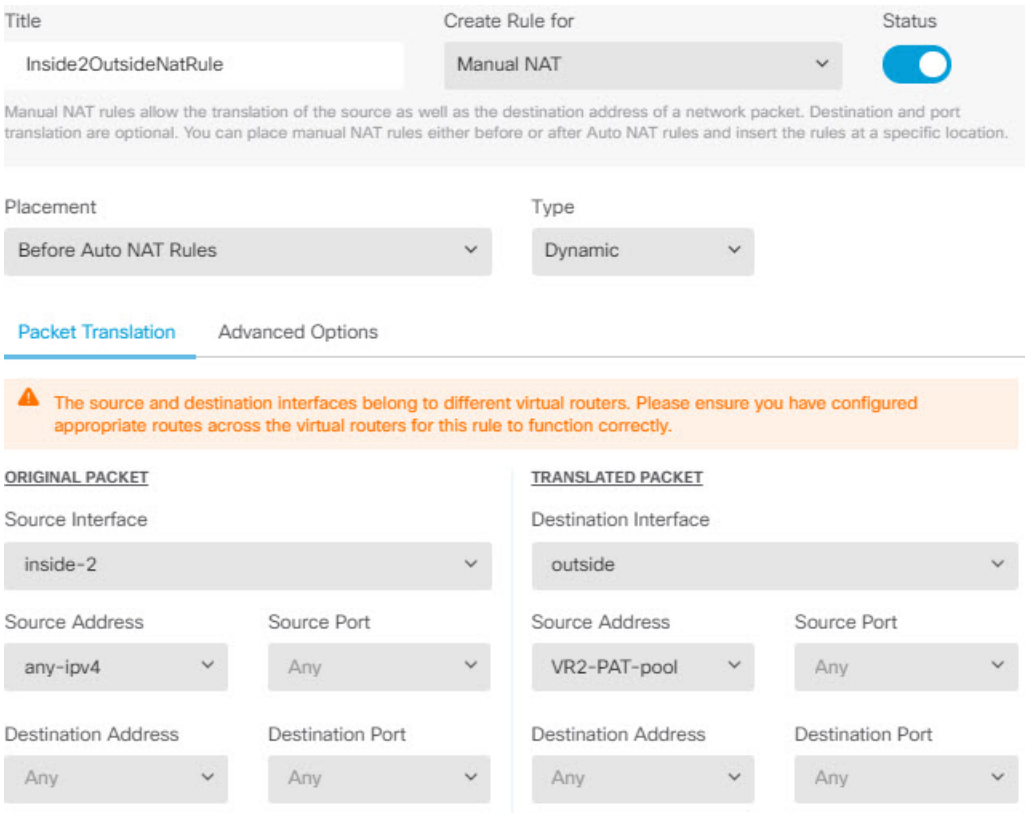
f) [OK] をクリック

ステップ 8 NAT ルールを作成して、inside-2 to outside トラフィックの 10.100.10.2 PAT を実行します。

このルールは、VR1 のルールとまったく同じように表示されますが、次の例外があります。

- [名前（Name）]：一意である必要があります（たとえば、Inside2OutsideNatRule）。
- **[元のパケット（Original Packet）]** > **[送信元インターフェイス（Source Interface）]**：inside-2 を選択します。
- **[変換済みパケット（Translated Packet）]** > **[送信元アドレス（Source Address）]**：10.100.10.2 の新しいホスト ネットワーク オブジェクトを作成します。

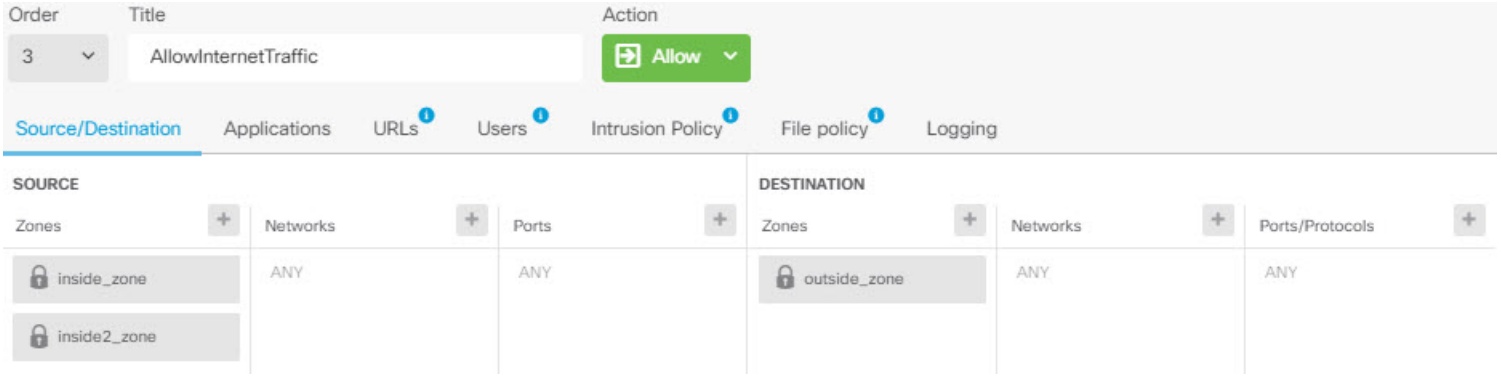
ルールは次のようになります。



ステップ 9 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択し、inside_zone および inside2_zone からのトラフィックを outside_zone に許可するアクセス制御ルールを設定します。

最後に、inside インターフェイスと inside-2 インターフェイスから outside インターフェイスへのトラフィックを許可するようにアクセス コントロール ポリシーを設定する必要があります。アクセス制御ルールではセキュリティゾーンを使用する必要があるため、これらのインターフェイスごとにゾーンを作成する必要があります。または、inside と inside-2 の両方を保持する単一のゾーンを作成することもできますが、これらのルータでトラフィックがどのように処理されるかを区別するために、このポリシーまたは他のポリシーで追加のルールを作成することになるでしょう。

インターフェイスの名前が付けられたゾーンを作成したとすると、すべてのトラフィックがインターネットに流れることを許可する基本ルールは、次のようになります。このルールには、適切な侵入ポリシーを適用できます。たとえば、URL フィルタリングを実装するために、不要なトラフィックをブロックする追加のルールを定義できます。



仮想ルータのモニタリング

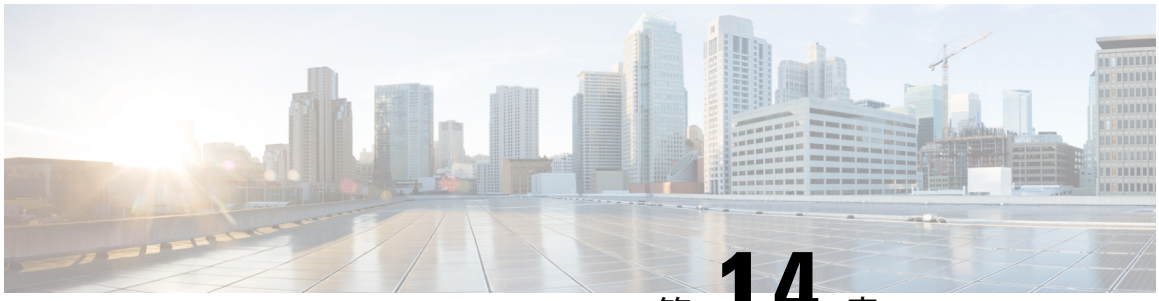
仮想ルータをモニターし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。また、[ルーティング（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

- **show vrf** は、システムで定義されている仮想ルータの情報を表示します。
- **show ospf** ［**vrf** *name* | **all**］

  仮想ルータの OSPF プロセスに関する情報を表示します。仮想ルータを指定して、その仮想ルータ内のプロセスに関する情報のみを表示するか、オプションを省略して、すべての仮想ルータにわたる VRF に関する情報を表示することができます。追加オプションを表示するには、**show ospf ?** を使用します。
- **show bgp** ［**vrf** *name* | **all**］

  仮想ルータの BGP プロセスに関する情報を表示します。仮想ルータを指定して、その仮想ルータ内のプロセスに関する情報のみを表示するか、オプションを省略して、すべての仮想ルータにわたる VRF に関する情報を表示することができます。追加オプションを表示するには、**show bgp ?** を使用します。
- **show eigrp** *option*

  EIGRP プロセスに関する情報を表示します。使用可能なオプションを表示するには、**show eigrp ?** を使用します。



第 14 章

ルートチューニングのためのルートマップおよびその他のオブジェクト

さまざまなルーティングプロトコルにより、ルートの配布や集約などのアクティビティを微調整できます。一部のチューニング機能では、ルートマップまたはその他のオブジェクトを使用して、チューニングポリシーの対象となるルートを識別します。ルートマップには、一致するルートに関するオプションを設定する追加機能があります。これにより、ネクストホップルータがカスタム動作を適用するために使用できるルートに変更を加えることができます。

これらのオブジェクトを作成する必要があるかどうかは、実装するルーティングプロトコルの動作を微調整するために必要なものに基づいて決まります。最初に要件を評価することによって、設定する調整コマンドに必要なオブジェクトのタイプを決定します。

ルートマップの設定

ルートマップはさまざまな目的で使用でき、一部のルーティングプロトコルは他のプロトコルよりも多くの用途をサポートしています。最も一般的な用途は、別のルーティングプロトコルへのルート再配布を微調整することです。

ルートマップの permit 句と deny 句

ルートマップは、1 つ以上の **permit** 句または **deny** 句で構成されます。これらの句の順序は重要です。ルートはマップのトップダウンで評価され、最初の一致が優先されます。ルートがどの句とも一致しない場合、ルートマップと一致しないと見なされます。

各 permit 句には、0 個以上の **match** ステートメントおよび **set** ステートメントを含めることができます。**match** ステートメントはどのルートが句と一致するのかを決定しますが、**set** ステートメントはルートのいくつかの特性（ルートメトリックなど）を変更します。set ステートメントは必要ありません。ルートを変更することなく、再配布（または別のサービス）のためにルートを照合できます。

各 deny 句には、0 個以上の match ステートメントを含めることができます。ただし、「拒否された」ルートは単にルートマップと一致しないため、set アクションを適用できないことから、set 句を含めても意味がありません。

ルートマップの match ステートメントと set ステートメント

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、ルートの一部の属性を変更します。

たとえば、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。ルートが基準に一致する場合、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ます。permit 句と一致する場合、ルートの属性の一部は、set コマンドからの値によって変更される可能性があります。ルートが基準に一致しない場合、この句はルートに適用されず、システム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。一致する句がない場合、ルートはルートマップに一致しないと見なされます（拒否アクションと同等）。

1 つの句内の match ステートメントおよび set ステートメントについては、次のようになります。

- 複数の match ステートメントは AND 演算されます。つまり、ルートが句に一致するには、そのルートが各ステートメントを満たす必要があります。
- 1 つの match ステートメントに含まれる複数の値は OR 演算されます。つまり、ルートがある match 句内のいずれかの値と一致する場合、そのルートはその句と全体として一致すると見なされます。
- match ステートメントがない場合、すべてのルートが句と一致します。
- ルートマップの permit 句に set ステートメントがない場合、機能（再配布など）は、ルートの現在の属性を変更せずに、ルートに適用されます。
- deny 句内の set ステートメントは無視されます。「拒否された」ルートは単にルートマップと一致しないため、set アクションを適用できないことから、set 句を含めても意味がありません。
- match ステートメントまたは set ステートメントがない空の句は、それより前の句と一致しなかったすべてのルートと一致します。次に例を示します。

- 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、残りのルートを再配布できません。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場合のデフォルトアクションです。

ルートマップの設定

ルートマップはさまざまな目的で使用でき、一部のルーティングプロトコルは他のプロトコルよりも多くの用途をサポートしています。最も一般的な用途は、別のルーティングプロトコルへのルート再配布を微調整することです。

ルートマップは、1 つ以上の **permit** 句または **deny** 句で構成されます。これらの句の順序は重要です。ルートはマップのトップダウンで評価され、最初の一致が優先されます。ルートがどの句とも一致しない場合、ルートマップと一致しないと見なされます。

各 permit 句には、0 個以上の **match** ステートメントおよび **set** ステートメントを含めることができます。**match** ステートメントはどのルートが句と一致するのかを決定しますが、**set** ステートメントはルートのいくつかの特性（ルートメトリックなど）を変更します。set ステートメントは必要ありません。ルートを変更することなく、再配布（または別のサービス）のためにルートを照合できます。

各 deny 句には、0 個以上の match ステートメントを含めることができます。ただし、「拒否された」ルートは単にルートマップと一致しないため、setアクションを適用できないことから、set 句を含めても意味がありません。

match ステートメントと set ステートメントの評価方法の詳細については、ルートマップの match ステートメントと set ステートメント （436 ページ） を注意深く参照してください。

始める前に

アクセスリスト、ASパスアクセスリスト、コミュニティリスト、ポリシーリスト、プレフィックスリストといった他のさまざまなオブジェクトをルートマップで使用して、一致基準を定義することができます。ルートマップを作成する前に、これらのオブジェクトを作成する必要があります。

ACL 照合の場合、IPv4 アドレスには標準 ACL または拡張 ACL を使用できますが、IPv6 アドレスに使用できるのは拡張 ACL のみです。match 句は IPv4 または IPv6 のみに基づいているため、ACL に match ステートメントの正しいアドレススキームがあることを確認してください。

また、他のルーティングプロトコルと比較すると BGP の一致および設定基準が異なることに注意してください。ルートマップを使用するルーティングプロセスに関して正しい一致/設定基準を選択していることを確認してください。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLI テンプレート（CLI Template）] として [ルートマップ（Route Map）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入入力します。この名前は、CLI テンプレートの最初の行（**route-map** コマンド内）のルートマップ名としても入力されることに注意してください。

ステップ 6 最初の句を作成します。

a) [redistribution] 変数をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、このルートマップを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) **sequence-number** 変数をクリックし、句の番号を 1 ー 65535 の範囲で入力します。

この番号は、ルートマップ内の他の番号付き句に関連しています。一般的な方法は、カウントを 10 ずつスキップし（つまり、10、20、30）、将来新しい句を挿入する余地を残すことです。

ステップ 7 [無効を表示（Show Disabled）] をクリックし、句の **match** ステートメントを設定します。

a) **configure** *clause* コマンドを有効にするには、コマンドの横にある [+] をクリックします。

b) [clause] をクリックし、**bgp-match-clause**（BGP ルートマップの場合）または **match-clause**（他のすべてのルーティングプロトコルの場合）を選択します。

c) （BGP ルートマップ）次の **match** ステートメントの任意の組み合わせを設定して、この句でターゲットとする特定のルートを識別します。設定しないコマンドについては、必ず、[-] アイコンをクリックして無効にしてください。

- **match as-path**：変数をクリックし、照合する自律システム番号を定義する AS パスオブジェクトを選択します。

- **match community**を使用して無効にすることができます。変数をクリックし、照合するコミュニティを定義するコミュニティ リスト オブジェクトを選択します。
- **match policy-list**を使用して無効にすることができます。変数をクリックし、句の一致基準を定義するポリシーリストオブジェクトを選択します。
- **match tag**を使用して無効にすることができます。変数をクリックし、照合するルートタグ値を 0 ー 4294967295 の範囲で入力します。

d) （他のすべてのルーティングプロトコル）次の **match** ステートメントの任意の組み合わせを設定して、この句でターゲットとする特定のルートを識別します。設定しないコマンドについては、必ず、[-]アイコンをクリックして無効にしてください。これらのコマンドの一部を有効にするには、[+] をクリックする必要がある場合があります。

- **match interface**を使用して無効にすることができます。変数をクリックし、照合するルート内のすべてのインターフェイスを選択します。
- **configure match ipv4/ipv6 ip address** *list-type*：IP バージョンに適したコマンドを有効にします。次に、[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートの IP アドレスを照合するかどうかを選択します。これにより **match ipv4/ipv6 address** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義するアクセスリストまたはプレフィックスリストを選択することができます。
- **configure match ipv4/ipv6 ip next-hop** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートのネクストホップルータの IP アドレスを照合するかどうかを選択します。これにより **match ipv4/ipv6 next-hop** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義するアクセスリストまたはプレフィックスリストを選択することができます。
- **configure match ipv4/ipv6 ip route-source** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートのルート送信元の IP アドレスを照合するかどうかを選択します。これにより **match ipv4/ipv6 route-source** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義するアクセスリストまたはプレフィックスリストを選択することができます。
- **match metric**：変数をクリックし、照合するルーティングメトリックを 1 ー 4294967295 の範囲で入力します。
- **match route-type**：（OSPF、EIGRP）変数をクリックし、ルートタイプを選択します。
  - **external-1**、**external-2**：OSPF または EIGRP の外部タイプ 1 またはタイプ 2 ルート。
  - **internal**を使用して無効にすることができます。OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート
  - **local**を使用して無効にすることができます。ローカルに生成された BGP ルート。
  - **nssa-external-1**、**nssa-external-2**：外部 Not So Stubby Area（NSSA）タイプ 1 またはタイプ 2 ルート。

ステップ 8 （任意、permit 句のみ）許可された（つまり、一致した）ルートについて、**set** ステートメントを設定してルート属性を変更できます。ルートを変更する必要はありません。たとえば、ルートを変更せずに再配布することができます。

a) **[...] > [複製（Duplicate）]**（permit 句内の configure match-clause コマンドまたは **configure bgp-match-clause** コマンドの左横）をクリックします。新しい **configure** *clause* コマンドが permit 句の最後に追加されます。

b) [clause] をクリックし、match 句に対して選択したものに基づいて **bgp-set-clause** または **set-clause** を選択します。

c) （BGP ルートマップ）一致するルートの属性を変更するには、次の **set** ステートメントの任意の組み合わせを設定します。設定しないコマンドについては、必ず、[-]アイコンをクリックして無効にしてください。

- **configure set as-path** *options*：[options] をクリックし、**properties** を選択すると、設定する必要がある次のコマンドが追加されます。パスに項目を追加すると、AS 番号が重複していても、パスが長くなり、そのルートが最適なルートとして選択される可能性が低くなります。
  - **set as-path prepend** *as-path*：[as-path] をクリックし、ルートの AS_PATH 属性の先頭に追加する最大 10 個の自律システム番号を入力します。この変更は、アウトバウンド BGP ルートマップに適用されます。
  - **set as-path prepend last-as** *value*：[value] をクリックし、システムが AS_PATH 変数の先頭にアドバタイジングネイバーの自律システム番号を付加する回数を入力します。この変更は、インバウンド BGP ルートマップに適用されます。
  - **set as-path tag**を使用して無効にすることができます。ルートのタグを自律システム パスに変換します。BGP にルートを再配布するときのみ適用されます。
- **set community** *community-number properties*：[community-number] をクリックし、ルートのコミュニティを 1 ～ 4694967295 の範囲で入力します。必要に応じて、[properties] をクリックし、次のいずれかを追加できます。
  - **internet**：このコミュニティのあるルートは、すべてのピア（内部および外部）にアドバタイズされます。
  - **no-advertise**：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。
  - **no-export**：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。
- **set local-preference**を使用して無効にすることができます。変数をクリックし、自律システムパスのプリファレンス値を 0 ー 4294967295 の範囲で入力します。グローバル BGP オプションで変更しないかぎり、BGP ルートのデフォルトプリファレンスは 100 です。プリファレンス値が最大のルートが優先されます。

- **set weight**を使用して無効にすることができます。変数をクリックし、ルートの重み 0 ～ 65535 の範囲で入力します。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。
- **set origin** *options*：BGP ルートの起点は、メイン IP ルーティングテーブルのルートのパス情報に基づいています。これを変更するには、[options] をクリックし、BGP 送信元コードの設定方法を選択します。
  - **igp**を使用して無効にすることができます。送信元を内部ゲートウェイプロトコル（IGP）のリモートシステムに設定します。
  - **incomplete**を使用して無効にすることができます。送信元を不明な継承として設定します。
- **configure next-hop ipv4/ipv6** *options*：これらは個別のコマンドです。適切な IP バージョンの [options] をクリックし、次のいずれかを選択します。ネクストホップゲートウェイの設定は、通常、ポリシーベースのルーティングを実装するときに行います。
  - **specific-ip**を使用して無効にすることができます。このルートのネクストホップゲートウェイの IP アドレスを明示的に設定する場合は、このオプションを選択します。**set ip/ipv6 next-hop ip-address** コマンドが追加されます。変数をクリックし、ネクストホップゲートウェイの IP アドレスを入力します。スペースで区切ることにより、複数の IP アドレスを追加できます。最初のゲートウェイのアドレスに到達できない場合は次のアドレスが試行され、以降同様です。
  - **user-peer-address**を使用して無効にすることができます。ネクストホップゲートウェイを BGP ピアの IP アドレスとして設定する場合は、このオプションを選択します。このオプションを BGP ピアのアウトバウンドルートマップで使用すると、アドバタイズされた一致するルートのネクストホップをローカルルータのピアアドレスに設定し、ネクストホップ計算をディセーブルにします。このコマンドについては、追加設定は必要ありません。
- **set ipv4/ipv6 address** *prefix-list*：これらは個別のコマンドです。選択したプレフィックスリストの内容に基づいて、ルートの IP アドレスを変更します。
- **set automatic-tag**を使用して無効にすることができます。システムにルートのタグ値を自動的に計算させます。

d) （他のすべてのルーティングプロトコル）一致するルートの属性を変更するには、次の**set** ステートメントの任意の組み合わせを設定します。設定しないコマンドについては、必ず、[-] アイコンをクリックして無効にしてください。

- **set metric**を使用して無効にすることができます。変数をクリックし、メトリック値を 0 ー 4294967295 の範囲で入力します。この値は EIGRP では使用されません。
- **set metric-type**を使用して無効にすることができます。変数をクリックし、メトリックのタイプを選択します。
  - **type-1**、**type-2**：OSPF の外部ルートのタイプ。デフォルトは type-2 です。

- **internal**を使用して無効にすることができます。ルートのネクストホップの内部ゲートウェイプロトコル（IGP）メトリックと一致するように、外部BGP（eBGP）ネイバーにアドバタイズされるプレフィックスのMulti-Exit識別子（MED）値を設定します。これは、生成された内部BGP（iBGP）生成ルートおよびeBGP生成ルートに適用されます。

ステップ 9 permit/deny 句を追加してルートマップを完成させます。

句を追加するには、**[...]** > **[複製（Duplicate）]**（**permit** 行または **deny** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックした句の直後に新しい *redistribution sequence-number* 句が追加されます。

ルートマップの句は、オブジェクトに表示される順序ではなく、シーケンス番号の順序で評価されますが、新しい句を順番に挿入することで、オブジェクトの編集が容易になります。オブジェクト内で句を移動することはできません。

句を複製すると新しい空の句が挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

ルートマップを必要とする機能のために、ルーティングプロセス設定（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

アクセスリストの設定

アクセス リスト オブジェクトは、アクセス コントロール リスト（ACL）とも呼ばれ、トラフィックに適用されるサービスを選択します。アクセス リスト オブジェクトを使って、ルート マップなどの機能を設定します。ACL で許可されたトラフィックはサービスを利用できますが、「ブロックされた」トラフィックはサービスから除外されます。サービスから除外されたトラフィックが必ずしも完全にドロップされるわけではありません。

次のタイプの ACL を設定できます。

- 拡張：送信元と宛先アドレスおよびポートに基づいてトラフィックを識別します。IPv4アドレスと IPv6 アドレスをサポートしています。
- 標準：宛先アドレスのみに基づいてトラフィックを識別します。IPv4のみサポートしています。

ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）またはルールで構成されます。ACE の順番は重要です。パケットを「許可」 ACE と照合して ACL を評価する際、ACL に登録されているACEの順番どおりに照合します。一致が見つかると、ACEはそれ以上チェックされません。たとえば、10.100.10.1 と一致させ、10.100.10.0/24 の残りを除外する場合、10.100.10.1 の許可エントリは 10.100.10.0/24 の拒否エントリの前に配置する必要があります。通常、具体性の高いルールを ACL の上部に置きます。

許可エントリに一致しないパケットは、拒否されるか、照合から除外されると見なされます。

次に、ACL オブジェクトの設定方法について説明します。

拡張アクセスリストの設定

送信元および宛先アドレス、プロトコル、およびポートに基づいて、あるいはトラフィックが IPv6 の場合にトラフィックを照合するには、拡張 ACL オブジェクトを使用します。

始める前に

オブジェクトに作成する ACE に必要なネットワークオブジェクトまたはポートオブジェクトを作成します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [拡張アクセスリスト（Extended Access List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**access list** コマンド内）の ACL 名としても入力されることに注意してください。

ステップ 6 ACL の最上位のルールとなる ACE を作成します。

1 つの **configure access list entry** コマンドに含まれるコマンドの各リストは基本的に 1 つの ACE ですが、展開すると、特に複数のネットワークオブジェクトを含める場合、システムがコマンドを一連の ACE に分割することがあります。

a) configure access list entry コマンドで、[action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。この ACE に一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。この ACE に一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであること

に注意してください。たとえば、ルートマップでは、この ACL を使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) **permit/deny network** コマンドで、変数をクリックし、接続の送信元 IP アドレスと宛先 IP アドレスを定義するネットワークオブジェクトを選択します。複数のオブジェクトを選択できます。「任意の」アドレスを指定するには、any-ipv4 オブジェクトおよび any-ipv6 オブジェクトを選択します。

c) **configure permit/deny port** コマンドで、[options] をクリックし、次のいずれかを選択します。これにより、関連付けられた permit/deny コマンドがテンプレートに追加されます。

- **any**：ポートが問題ではない場合に使用します。つまり、任意のタイプの IP トラフィックが照合されます。
- **any-source**：送信元 TCP/UDP ポートは問題ではないが、宛先ポートを指定する場合に使用します。**permit/deny port** コマンドの [destination-port] 変数をクリックし、ポートオブジェクトを選択します。
- **any-destination**：宛先 TCP/UDP ポートは問題ではないが、送信元ポートを指定する場合に使用します。**permit/deny port** コマンドの [source-port] 変数をクリックし、ポートオブジェクトを選択します。
- **source-destination**：送信元 TCP/UDP ポートと宛先 TCP/UDP ポートの両方が問題である場合に使用します。**permit/deny port** コマンドで [source-port] 変数と [destination-port] 変数をクリックし、ポートオブジェクトを選択します。

d) **configure logging** コマンドで、**disabled** を選択します。ロギングはアクセス制御に使用される ACL に適用され、これらのオブジェクトをアクセス制御に使用することはできません。そのため、ロギングオプションは選択内容に関係なく無視されます。

ステップ 7 ACE を追加して ACL を完成させます。

ACE を追加するには、**[...]** > **[複製（Duplicate）]**（**configure access list entry** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックした ACE の直後に新しい ACE グループが追加されます。

そのため、オブジェクトに多数の ACE がある場合は、「複製」する ACE を慎重に選択してください。オブジェクト内では ACE を移動できないため、間違えた場合は、ACE を正しい場所で手動で再作成する必要があります。

ACE を複製すると新しい空の ACE が挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

拡張 ACL を必要とする機能のために、ルートマップオブジェクト（または FlexConfig オブジェクト）でオブジェクトを使用できるようになりました。

標準アクセスリストの設定

宛先 IPv4 アドレスのみに基づいてトラフィックを照合する場合や、設定している機能が標準 ACL をサポートする場合は、標準 ACL オブジェクトを使用します。それ以外の場合は、拡張 ACL を使用します。

始める前に

オブジェクトに作成する ACE に必要なネットワークオブジェクトを作成します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [標準アクセスリスト（Standard Access List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**access list** コマンド内）の ACL 名としても入力されることに注意してください。

ステップ 6 ACL の最上位のルールとなる ACE を作成します。

1 つの **configure action** コマンドに含まれるコマンドの各リストは、1 つの ACE です。

a) **configure action** コマンドで、[action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。この ACE に一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。この ACE に一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、この ACL を使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) **permit/deny host** コマンドで、変数をクリックし、接続の宛先 IP アドレスを定義するネットワークオブジェクトを選択します。このオブジェクトは、ネットワークまたはホストアドレスを指定できます。**permit/deny host** コマンドごとに 1 つのオブジェクトを選択できます。コマンドで **[...]** > **[複製（Duplicate）]** をクリックして追加のアドレスを指定すると、

同じアクションを持つ一意の ACE になります。「任意の」アドレスを指定するには、any-ipv4 オブジェクトを選択します。

ステップ 7 ACE を追加して ACL を完成させます。

ACE を追加するには、**[...]** > **[複製（Duplicate）]**（**configure action** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックした ACE の直後に新しい ACE グループが追加されます。

そのため、オブジェクトに多数の ACE がある場合は、「複製」する ACE を慎重に選択してください。オブジェクト内では ACE を移動できないため、間違えた場合は、ACE を正しい場所で手動で再作成する必要があります。

ACE を複製すると新しい空の ACE が挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

標準ACLを必要とする機能のために、ルートマップオブジェクト（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

AS パスアクセスリストの設定

AS パスアクセスリストを使用して、BGP ネイバーの更新を、更新内の自律システム番号に基づいてフィルタ処理できます。許可された AS 番号の場合は更新が受け入れられますが、拒否された AS 番号の場合は更新が拒否されます（つまり、更新はルーティングテーブルに追加されない）。

また、アウトバウンド方向に AS パスフィルタ処理を適用して、ネイバーに送信する更新をフィルタ処理することもできます。

さらに、BGP アドレス集約のルートマップで AS パスオブジェクトを使用できます。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [ASパス（ASPath）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、1 ー 500 の範囲の数値にする必要があります。この名前は、CLIテンプレートの最初の行（**as-path** コマンド内）の AS パスアクセスリスト名としても入力されることに注意してください。

ステップ 6 AS パスエントリを設定します。

各エントリは、*action* オプションで始まる単一の行に含まれます。

a) [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このオブジェクトを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) [regex] をクリックし、このエントリに一致する AS 番号を定義する正規表現を入力します。

最も単純な形式では、正規表現は単に完全な AS パス番号であり、単一の自律システムからのルート更新を許可または拒否します。

AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。システムは、RFC 5396 で定義されている asplain および asdot 表記をサポートしています。使用する必要がある表記は、BGP グローバル設定で **bgp asnotation dot** コマンドを有効にするかどうかによって異なります。

ステップ 7 エントリを追加して AS パスアクセスリストを完成させます。

エントリを追加するには、**[...]**>**[複製（Duplicate）]**（*action* 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックしたエントリの直後に新しいエントリが追加されます。

そのため、オブジェクトに多数のエントリがある場合は、「複製」するエントリを慎重に選択してください。オブジェクト内ではエントリを移動できないため、間違えた場合は、エントリを正しい場所で手動で再作成する必要があります。ルールはトップダウンで評価され、最初の一致が優先されます。

エントリを複製すると新しい空のエントリが挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ASパスアクセスリストを必要とする機能のために、BGPオブジェクト、ルートマップオブジェクト（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

コミュニティリストの設定

BGPプロセスでコミュニティ情報を送信できるようにすると、ルートマップでコミュニティリストをmatch句として使用して、一致するルートで属性を設定できます。たとえば、特定のコミュニティのルート優先度を変更できます。

コミュニティとは、共通するいくつかの属性を共有する宛先グループに関してアドバタイズされたルートにサービスプロバイダーが添付するオプションの属性またはラベルです。特定のコミュニティ番号はISPがアドバタイズするものであり、それらの番号とその意味をISPから取得し、ルートマップを使用してそれらを処理する方法を選択する必要があります。

コミュニティリストは順序付けられており、一致は、アクセスリストやプレフィックスリストと同様に、トップダウン（最初の一致が優先される）方式によって決定されます。

コミュニティリストには次の2つのタイプがあります。

- 標準：特定の既知のコミュニティ（サービスプロバイダーから取得したコミュニティなど）を対象とする場合は、標準リストを使用します。
- 拡張：正規表現照合に基づいて一連のコミュニティを照合する場合は、拡張リストを使用します。

手順

ステップ1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ2 コンテンツテーブルから **[スマートCLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ4 [CLIテンプレート（CLI Template）] として [標準コミュニティリスト（Standard Community List）] または [拡張コミュニティリスト（Expanded Community List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**community-list** コマンド内）のコミュニティリスト名としても入力されることに注意してください。

ステップ 6 （標準リスト）コミュニティリストエントリを設定します。

各エントリは、*action* オプションで始まる単一の行に含まれます。

a) [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このルートを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) [community-number] をクリックし、最大 10 個のコミュニティをスペースで区切って入力します。1 つのルールに含まれる複数のコミュニティは AND 演算されるため、ルート内のすべてのコミュニティが一致する場合にのみ一致します。

BGP プロセスに関して有効になっている番号付け方法に基づいてコミュニティを 10 進形式（1 ～ 4294967295）または AA:NN 形式（各値は 1 ～ 66535）で入力します。これらの番号は、ISP またはその他の BGP ネイバーから取得してください。

c) （オプション）[properties] をクリックし、他の既知のコミュニティをルールに追加します。

- **internet**：このコミュニティのあるルートは、すべてのピア（内部および外部）にアドバタイズされます。
- **no-advertise**：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。
- **no-export**：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 （拡張リスト）コミュニティリストエントリを設定します。

a) [action] をクリックし、**permit** または **deny** を選択します。これらのアクションについては、前述しています。

b) [regex] をクリックし、このエントリに一致するコミュニティを定義する正規表現を入力します。

***** または **+** の文字を使用した照合の順序は、最長のコンストラクトが最初になります。入れ子のコンストラクトは外側から内側へと照合されます。連結コンストラクトは左側から順に照合されます。ある正規表現が、1 つの入力ストリングの異なる 2 つの部分と一致する可能性がある場合、早く入力された部分が最初に一致します。正規表現の表記の詳細に

ついては、『Cisco IOS Terminal Services Configuration Guide』の付録「Regular Expressions」を参照してください。

ステップ 8 エントリを追加してコミュニティリストを完成させます。

エントリを追加するには、**[...]** > **[複製（Duplicate）]**（*action* 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックしたエントリの直後に新しいエントリが追加されます。

そのため、オブジェクトに多数のエントリがある場合は、「複製」するエントリを慎重に選択してください。オブジェクト内ではエントリを移動できないため、間違えた場合は、エントリを正しい場所で手動で再作成する必要があります。

エントリを複製すると新しい空のエントリが挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 9 [OK] をクリックしてオブジェクトを保存します。

コミュニティリストを必要とする機能のために、ルートマップやルーティングプロセス（または FlexConfig オブジェクト）でオブジェクトを使用できるようになりました。

ポリシー リストの設定

ルートマップではポリシーリストを 1 つ以上の match 句の代わりに使用できます。そのため、再利用したい一連の match 句がある場合、ポリシーマップによって設定が簡素化され、各ルートマップで match 句を繰り返す必要がなくなります。BGP のポリシーリストを参照するルートマップを使用できます。

ルートマップ内には、ポリシーリストに加えて他の match 句を含めることができます。ポリシーリストの match 句は、着信属性でのみ照合されます。

ポリシーリストは IPv4 アドレスの照合のみをサポートします。IPv6 アドレスは照合できません。

ポリシーマップ内の match 句については、次のようになります。

- 複数の match 句は AND 演算されます。つまり、ルートがポリシーリストに一致するには、そのルートが各句を満たす必要があります。
- 1 つの match 句内の複数の値は OR 演算されます。つまり、ルートがある match 句内のいずれかの値と一致する場合、そのルートはその句と全体として一致すると見なされます。

始める前に

アクセスリスト、プレフィックスリスト、または AS パスアクセスリストに関する match 句を設定する場合は、ポリシーリストを作成する前にそれらのオブジェクトを作成する必要があります。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLI テンプレート（CLI Template）] として [ポリシーリスト（Policy List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**policy-list** コマンド内）のポリシーリスト名としても入力されることに注意してください。

ステップ 6 **policy-list** コマンドで [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このリストに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このリストに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このオブジェクトを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

ステップ 7 テンプレートの上にある [無効を表示（Show Disabled）] をクリックして match コマンドを表示します。有効にする match ステートメントの左側にある [+] アイコンをクリックする必要があります。次の match ステートメントの任意の組み合わせを設定して、ターゲットとするルートを定義します。

- **match as-path**を使用して無効にすることができます。変数をクリックし、照合する自律システム番号を定義する AS パスオブジェクトを選択します。
- **configure match ip address** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートの IP アドレスを照合するかどうかを選択します。これにより **match ip address** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義する標準アクセスリストまたは IPv4 プレフィックスリストを選択することができます。
- **configure match ip next-hop** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートのネクストホップルータの IP アドレスを照合するかどうかを選択します。これにより **match ip next-hop** コマンドが追加されます。このコマンドの変

数をクリックし、照合する IP アドレスを定義する標準アクセスリストまたは IPv4 プレフィックスリストを選択することができます。

- **configure match ip route-source** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートのルート送信元の IP アドレスを照合するかどうかを選択します。これにより **match ip route-source** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義する標準アクセスリストまたは IPv4 プレフィックスリストを選択することができます。
- **match community** *community-list options*：[community-list] 変数をクリックし、照合するコミュニティを定義するコミュニティ リスト オブジェクトを選択します。リスト内のすべてのコミュニティが一致した場合にのみルートをコミュニティリストと一致させる場合は、[options] をクリックし、**exact-match** を選択します。
- **match interface**を使用して無効にすることができます。変数をクリックし、照合するルート内のすべてのインターフェイスを選択します。
- **match metric**を使用して無効にすることができます。変数をクリックし、照合するルーティング Multi-Exit 識別子（MED）メトリックを 1 ー 4294967295 の範囲で入力します。
- **match tag**を使用して無効にすることができます。変数をクリックし、照合するルートタグ値を 0 ー 4294967295 の範囲で入力します。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

BGP ルーティングで使用するためにオブジェクトをルートマップオブジェクトで使用できるようになりました。

プレフィックス リストの設定

プレフィックスリストはアクセス制御リストと似ています。プレフィックスリストは、許可/拒否ルールの順序付きリストです。ここで、「許可」はリストと一致する必要があるアドレスプレフィックスを示し、「拒否」はリストと一致してはならないアドレスプレフィックスを示します。システムは一致をトップダウン方式で評価し、必ずしも最も一致したルールに基づかず、最初に一致したルールに基づいてアクションを割り当てます。そのため、必要な一致を確実に得るには、シーケンス番号を慎重に指定する必要があります。

OSPF フィルタリングや BGP、OSPF、または EIGRP ルートマップのプレフィックスリストを使用して、ルートの再配布または注入、あるいは BGP ネイバーフィルタ処理を行うことができます。

IPv4 アドレス用と IPv6 アドレス用の個別のプレフィックスリストがありますが、リストの構造は同じです。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [IPv4プレフィックスリスト（IPv4 Prefix List）] または [IPv6プレフィックスリスト（IPv6 Prefix List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**prefix-list** コマンド内）のプレフィックスリスト名としても入力されることに注意してください。

ステップ 6 プレフィックス リスト エントリを設定します（**seq** コマンドライン）。

各エントリは、**seq** オプションで始まる単一の行に含まれます。

a) **seq** で、[sequence-number] をクリックし、このルールの番号を 1 ー 4294967294 の範囲で入力します。この番号は、他のルールのシーケンス番号に関連し、1 のルールが最初に評価されます。一般的な方法では、カウントを 5 ずつスキップします（つまり 5、10、15 など）。これにより、他のルールのシーケンス番号を変更することなく新しいルールを挿入する余地が残ります。

b) [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このルートを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

c) [ip-address-mask] をクリックし、ネットワークアドレスおよびマスク（IPv4 の場合 CIDR 形式）または IPv6 の場合はプレフィックス長を入力します。たとえば、10.100.10.0/24（IPv4）または 2001:DB8:0:CD30::/60（IPv6）と入力します。

ge オプションまたは **le** オプションのいずれかを含めないかぎり、システムは、このアドレス/マスクの完全一致を使用します。たとえば、ルールに **ge 9** を含めないかぎり、10.100.10.10/8 は 10.100.10.0/24 と一致しません。

マスクまたはプレフィックス長は次のように設定できます。

- IPv4 = 0 ～ 32
- IPv6 = 0 ～ 128

d) （オプション）**ge** キーワードおよび **le** キーワードを使用して、IP アドレスおよびマスク/プレフィックス長よりも具体的なプレフィックスに対して一致するプレフィックス長の範囲を指定できます。これらのキーワードがないときは、完全一致の場合にのみルールに一致すると見なされます。

ge *min-prefix-length* では、照合する最小プレフィックス長を指定します。この最小値は、マスク/プレフィックス長より大きく、**le** オプションで定義されている最大値以下である（存在する場合）必要があります。

le *max-prefix-length* では、照合する最大プレフィックス長を指定します。この最大値は、最小値以上である（存在する場合）か、マスク/プレフィックス長より大きい（最小値が定義されていない場合）必要があります。

上記の相対的な長さの制限に加えて、これらのオプションの長さには、次の外的制限があります。

- IPv4 = 1 ～ 32
- IPv6 = 0 ～ 128

ステップ 7 エントリを追加してプレフィックスリストを完成させます。

エントリを追加するには、**[...]**>**[複製（Duplicate）]**（**seq** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックしたエントリの直後に新しいエントリが追加されます。

便宜上、エントリを順番に保持することをお勧めします。ただし、オブジェクト内で混ざっていても、展開するとプレフィックスリストは順番に書き換えられます。

エントリを複製すると新しい空のエントリが挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

プレフィックスリストを必要とする機能のために、ルートマップやルーティングプロセス（または FlexConfig オブジェクト）でオブジェクトを使用できるようになりました。

例

以下に、プレフィックスリストを使用してプレフィックスを照合する方法の例を示します。分かりやすくするために例ではシーケンス番号を省いています。各ルールの実際の動作は、対象のアドレス空間のサブセットに一致するルールがそれよりも前にある場合は、それによって変更されます。

- デフォルトルート 0.0.0.0/0 を拒否する：

```
deny 0.0.0.0/0
```

- プレフィックス 10.0.0.0/8 を許可する：

```
permit 10.0.0.0/8
```

- プレフィックス 192/8 のルートで最大 24 ビットのマスク長を許可する：

```
permit 192.168.0.0/8 le 24
```

- プレフィックス 192/8 のルートで 25 ビットよりも大きいマスク長を拒否する：

```
deny 192.168.0.0/8 ge 25
```

- すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する：

```
permit 0.0.0.0/0 ge 8 le 24
```

- すべてのアドレス空間で 25 ビットよりも大きいマスク長を拒否する：

```
deny 0.0.0.0/0 ge 25
```

- プレフィックス 10/8 のすべてのルートを拒否する：

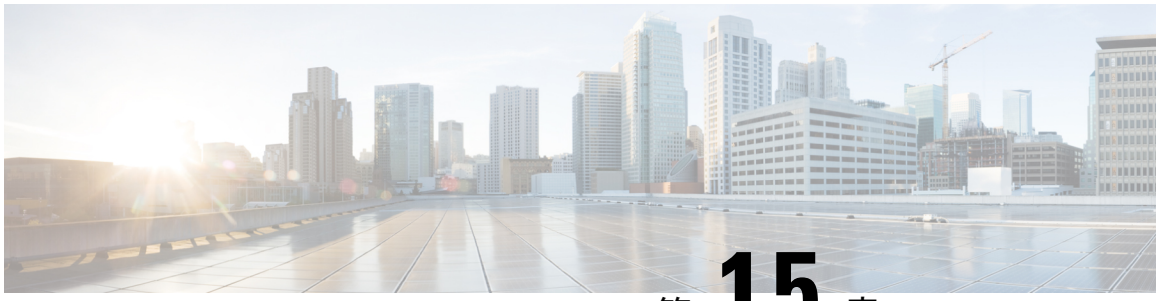
```
deny 10.0.0.0/8 le 32
```

- プレフィックス 192.168.1/24 のルートで 25 ビットよりも大きいすべてのマスクを拒否する：

```
deny 192.168.1.0/24 ge 25
```

- プレフィックス 0/0 のすべてのルートを許可する：

```
permit 0.0.0.0/0 le 32
```



第 15 章

Open Shortest Path First（OSPF）

Open Shortest Path First（OSPF）は、リンクステート内部ゲートウェイプロトコルです。OSPF ルータは、リンクステート情報を隣接ルータにフラッディングし、OSPF エリア内のすべてのルータがネットワークトポロジを完全に把握できるようにします。

IPv4 ネットワークの場合は OSPFv2、IPv6 ネットワークの場合は OSPFv3 など、IP バージョンに基づいて、個別の OSPF バージョンがあります。これらのバージョンは独立していて、OSPFv3 は OSPFv2 に代わるものではありません。

スマート CLI オブジェクトを使用して OSPFv2 を設定し、デバイスを OSPFv2 ネットワークトポロジに統合することができます。OSPFv3 は設定できません。

OSPFv2 プロセスとエリアの設定

脅威に対する防御で最大 2 つの OSPFv2 プロセスを設定できます。プロセス番号は純粋に内部的なインジケータです。他のデバイスで使用されているプロセス番号と一致させる必要はありませんが、独自のトラッキングを目的として番号を一致させることもできます。

プライベートネットワークの番号（192.168.1.0/24 など）を内部ネットワークに使用する場合は、プライベートアドレスをパブリックアドレスから分離し、これらの内部ネットワークに対して 1 つの OSPFv2 プロセスを使用し、外部の公的にアドレス可能なネットワークに対して 2 番目のプロセスを使用することが必要になる場合があります。プライベート番号を使用しない場合でも、1 つのプロセスを内部で実行し、別のプロセスを外部で実行して、2 つのプロセス間でルートのサブセットを再配布することができます。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。

一方、エリア番号はネットワーク内に存在するため、他の隣接ルータで使用されているものと同じ番号を使用する必要があります。シングルエリアネットワークを設定する場合は、エリア

0（バックボーンエリアとも呼ばれる）を使用します。階層型ネットワーク設計の複数エリアネットワークの場合は、ネットワークで定義されたエリアを理解し、このデバイスをどのエリアに参加させるかを把握する必要があります。

仮想ルータを使用している場合は、仮想ルータごとに 2 つの OSPFv2 プロセスを作成できます。

次の手順で、1 つの OSPFv2 プロセスを作成する方法を説明します。2 番目のプロセスを作成するには、この手順を繰り返します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいプロセスを作成するには、**[+]** > **[OSPF]** をクリックするか、**[OSPFオブジェクトの作成（Create OSPF Object）]** > **[OSPF]** ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

プロセスが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 6 基本的なプロセスのプロパティを設定します。

- **router ospf** *process-id*：*process-id* をクリックし、1 ～ 65535 の番号を入力します。この番号は、このデバイス内のみで意味を持つもので、他のルータで設定されているプロセス番号と一致している必要はありません。この番号は仮想ルータ内で一意である必要があります。
- **log-adj-changes** *log-state*：*log-state* をクリックし、次のいずれかのオプションを選択します。
  - **enable**（推奨）：OSPFv2 ネイバーがアップまたはダウンすると、システムは syslog メッセージを生成します。このオプションを選択すると、追加の **log-adj-changes** *log-type* 行がオブジェクトに追加されます。ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信したい場合、*log-type* をクリックして **detail** を選択します。

    詳細なメッセージが表示されないようにするには、*log-type* をオプションのままにします 。オブジェクトからこの行を削除しないでください。

- **disable**：syslog メッセージは生成されません。**no log-adj-changes** 行がオブジェクトに追加されます。この行は削除しないでください。

ステップ 7 オブジェクト本文の上にある [無効を表示（Show Disabled）] リンクをクリックして、その他のすべての設定行を追加します。

ステップ 8 エリア番号を設定します。

a) **area** *area-id* 行の左にある [+] をクリックして、コマンドを有効にします。コマンドは有効にするまで設定できません。

b) *area-id* をクリックし、エリアの番号を入力します。このエリア番号は、OSPFv2 エリアを定義する他のルータで使用されている番号と同じである必要があります。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

ステップ 9 エリア内でルーティングする必要があるネットワークとインターフェイスを設定します。

a) **configure area** *area-id options* 行の左にある [+] をクリックします。

b) *area-id* をクリックし、 **area** コマンドと同じエリア番号を入力します。

c) *options* をクリックして、**properties** を選択します。このアクションにより複数の行が追加されます。これには、デフォルトで有効になっている行、**network** コマンドが含まれます。

d) **network** コマンドで *network-object* をクリックし、この領域に含めるネットワークを定義するオブジェクトを選択します。通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

e) （オプション）**network** コマンドで *tag-interface* をクリックして、ネットワークにホストまたはルーティングするインターフェイスを選択します。このインターフェイスを選択すると、それがルーティングプロセスで使用されるため、インターフェイス上のアドレスを変更できなくなる場合があります。この場合、インターフェイスアドレッシングへの変更がルーティング設定に影響を与える可能性があることがわかります。

ここでインターフェイスを選択した場合は、インターフェイス上のアドレスを変更する前に、まずルーティングプロセスからインターフェイスを削除する必要があります。次に、IP アドレスを変更した後、必ずここに戻り、新しいネットワークとインターフェイスを選択して、ルーティングプロセスが正しく設定されていることを確認します。

f) その他の新しいエリア行はすべてオプションで、デフォルトでは無効になっています。これらのサービスが必要な場合にのみ設定してください。詳細については、OSPF プロセスとエリア特性のカスタマイズ （460 ページ）を参照してください。

ステップ 10 複数エリアネットワークのプロセスを設定する場合は、**area** と **configure area** の行の丸で囲まれた [-] の左側の領域にカーソルを合わせ、**[...]** > **duplicate** をクリックします。次に、前述のように、新しいエリアとそのネットワークを設定します。このルーティングプロセスが参加する必要があるすべてのエリアを定義するまで、このプロセスを繰り返します。

ステップ 11 [OK] をクリックします。

OSPF プロセスとエリア特性のカスタマイズ

OSPF には、デフォルト値を持つ多くのオプションが含まれています。これらの値は、多くのネットワークで適切に機能します。ただし、必要とする動作を正確に得るために、設定を1つ以上調整する必要がある場合があります。以降のトピックでは、OSPFv2 ルーティングプロセスをカスタマイズするためのさまざまな方法について説明します。

OSPF プロセスの詳細設定の構成

OSPFv2 プロセスの全体的な動作を制御する複数の設定を構成できます。これには、ディスタンスメトリック、タイマー、グレースフルリスタート、リンク ステート アドバタイズメントやその他のルーティングアップデートの送信に使用されるルータ ID などがあります。これらの設定の多くには、ほとんどのネットワークに適しているデフォルト設定があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 **setup ospf** 行を見つけます。

オブジェクトを追加する場合は、[無効を表示（Show Disabled）] リンクをクリックして、この行を表示する必要があります。次に、コマンドの [+] をクリックして有効にし、*configuration* をクリックして、**advanced** を選択します。デフォルトで有効になっているコマンドは、デフォルト値を使用してすでに有効になっています。

オブジェクトを編集するときには、その行はすでに有効になっています。

この手順の残りの部分では、[無効を表示（Show Disabled）] をクリックしたことを前提としています。コマンドが表示されない場合は、無効なコマンドが表示されるようになっていることを確認してください。

ステップ 6 （オプション）ルータ ID を設定します。

[+] をクリックして **router-id** コマンドを有効にし、変数をクリックして、このデバイスからルータアップデートを送信するときに使用する IPv4 アドレスを入力します。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできないため、ID がエリア内で一意であることを確認してください。

プロセスに対してルータ ID を明示的に指定しない場合、システムはアクティブインターフェイスに割り当てられている最も大きい IP アドレスを使用します。そのため、選択したインター

フェイスを無効にするか、アドレスを変更すると、ルータ ID が変更される場合があります。ルータ ID を明示的に割り当てることにより、プロセスの一貫性を確保することができます。

ステップ 7 （オプション）サマリールートコストを計算する際に、RFC 1583 互換性を設定します。

[+] をクリックして **configure summary-route-cost** コマンドを有効にし、変数をクリックして、**any**（RFC 1583 互換性をオフにする）、または **rfc1583**（RFC 1583 互換性をオンにする）をクリックします。

OSPF オブジェクトではこのコマンドはデフォルトで有効になっていませんが、実際は RFC 1583 互換性が、サマリールートのコストを計算するときに使用されるデフォルトの方法となっています。定義された設定を CLI で確認すると、無効になっている設定のみが表示されます。

RFC 1583 の互換性が有効な場合、ルーティング ループが発生することがあります。ルーティング ループを防止するには、これを無効にします。RFC 1583 互換性は、OSPF ルーティング ドメイン内のすべての OSPF ルータで同じに設定するようにしてください。

ステップ 8 （オプション）マルチキャスト OSPF（MOSPF）リンク ステート アドバタイズメント（LSA）の syslog メッセージを抑制します。

[+] をクリックして、**ignore lsa mospf** コマンドを有効にします。

システムは、LSA タイプ 6 MOSPF パケットをサポートしていません。このコマンドを有効にすると、システムがこれらのパケットを受信したときに syslog メッセージが送信されないようにできるため、syslog サーバーのノイズを削減できます。

ステップ 9 ディスタンスメトリックを設定します。

次の **distance** コマンドは、デフォルトで有効になっています。ルートのタイプに基づいて、OSPF ルート アドミニストレーティブ ディスタンスを変更できます。距離は 1 ～ 255 で、数値が高いほど信頼度が低下します。これらのメトリックは、異なるプロセスからの類似したルートを比較する際に、学習したルートの相対値を判断するために使用されます。

- **distance ospf inter-area 110**を使用して無効にすることができます。数値をクリックして、あるエリアから別のエリアまでのすべてのルートの距離を設定します。
- **distance ospf intra-area 110**を使用して無効にすることができます。数値をクリックして、エリア内のすべてのルートの距離を設定します。
- **distance ospf external 110**を使用して無効にすることができます。数値をクリックして、再配布によって取得した他のルーティングドメインからのルートの距離を設定します。

ステップ 10 OSPF プロセスのルート計算タイマーを設定します。

次のタイマーコマンドは、これらのデフォルト値で有効になっています。

- **timers lsa arrival 1000**を使用して無効にすることができます。数値をクリックして、システムが OSPF ネイバーから同じリンク ステート アドバタイズメント（LSA）を受け入れる最小間隔を設定します（0 ～ 600000 ミリ秒）。このコマンドを使用して、ネイバーから着信する同じ LSA を受信する間に経過する必要がある最小間隔を指定します。この最小時間より前に着信した LSA は無視されます。

- **timers pacing flood 33**を使用して無効にすることができます。数値をクリックして、フラッディングキュー内の LSA がアップデートの合間にペーシング処理される時間を設定します（5 ～ 100 ミリ秒）。
- **timers pacing lsp-group 240**を使用して無効にすることができます。数値をクリックして、OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を設定します（10 ～ 1800 秒）。
- **timers pacing retransmission 66**を使用して無効にすることができます。数値をクリックして、再送信キュー内の LSA がペーシング処理される時間間隔を設定します（5 ～ 200 ミリ秒）。OSPF パケットフラッディングの要件を満たす他のオプションをすべて使用した場合に限り、パケット再送信ペーシングタイマーを変更することが推奨されます。特に、デフォルトのフラッディングタイマーを変更する前に、集約、スタブエリアの使用方法、キューの調整、およびバッファの調整を設定してください。
- **timers throttle lsa 0 5000 5000**を使用して無効にすることができます。数値をクリックして、Open Shortest Path First（OSPF）のリンクステート アドバタイズメント（LSA）生成に対するレート制限値を設定します。LSA および SPF スロットリングは、ネットワークが不安定になっている間に OSPF の LSA 更新頻度を低下させて、より高速な OSPF コンバージェンスを可能にするダイナミックメカニズムを提供します。値は次のとおりです。
  - [インターバル（開始）（Start Interval）]（最初の数値）：LSA の最初のオカレンスを生成する最小遅延（1 ～ 600000 ミリ秒）。LSA の最初のインスタンスは、ローカル OSPF トポロジの変更直後に生成されます。次の LSA は、この開始インターバルの後にのみ生成されます。遅延なしで LSA が生成されるようにするには、0 を指定します。
  - [ホールド時間（Hold Time）]（2 番目の数値）：LSA を再生成する最小遅延（1 ～ 600000 ミリ秒）。この値は、LSA 生成の時間を制限する従属レートを計算するために使用されます。
  - [最大インターバル（Maximum Interval）]（3 番目の数値）：LSA を再生成する最大遅延（1 ～ 600000 ミリ秒）。
- **timers throttle spf 5000 10000 10000**を使用して無効にすることができます。数値をクリックして、最短パス優先（SPF）生成のレート制限値を設定します。値は次のとおりです。
  - [インターバル（開始）（Start Interval）]（最初の数値）：SPF 計算の変更を受信するまでの遅延（1 ～ 600000 ミリ秒）。
  - [ホールド時間（Hold Time）]（2 番目の数値）：1 回目の SPF 計算と 2 回目の SPF 計算の間の遅延（1 ～ 600000 ミリ秒）。
  - [最大インターバル（Maximum Interval）]（3 番目の数値）：SPF 計算の最大待機時間（1 ～ 600000 ミリ秒）。

ステップ 11　（オプション）デフォルトの外部ルートを OSPF ルーティングドメインに生成します。

+ をクリックして、**default-information originate** コマンドを有効にします。次のコマンドを有効にして設定し、機能を微調整することができます（オプション）。

- **default-information originate always**を使用して無効にすることができます。デフォルトルートがない場合でも、常にデフォルトルートをアドバタイズします。
- **default-information originate metric 1 metric-type** *metric-type-value*。デフォルトルートを生成するためのメトリックのタイプと値。
  - **metric** の数値をクリックして、OSPF のデフォルトメトリック値を入力します（0 ～ 16777214）。別の値が必要であることがわかっている場合を除き、「10」と入力します。
  - **metric-type** の数値をクリックして、OSPF 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る外部リンクタイプを選択します（1または2）。デフォルトは 2 です。
- **default-information originate route-map** *route-map*。ルーティングプロセスを指定するルートマップを選択します。このルートマップが一致した場合、このルーティングプロセスによりデフォルトルートが生成されます。

ステップ 12 （オプション）デバイスが高可用性（HA）用に設定されている場合、Non-Stop Forwarding（NSF）グレースフルリスタートを設定します。

システムでは、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。この機能は、コンポーネントに障害が発生した場合（たとえば、HA でアクティブ装置がスタンバイ装置にフェールオーバーした場合や、クラスタのプライマリユニットに障害が発生してセカンダリユニットが新しいプライマリとして選出された場合）、またはスケジュールされたヒットレス ソフトウェア アップグレードがある場合に役立ちます。

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。

デバイスは NSF 対応または NSF 認識として設定できます。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、動作中のモードに関係なく、NSF 認識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、デバイスが高可用性（フェールオーバー）であるかスパンド EtherChannel（L2）クラスタモードである必要があります。

（注） グレースフルリスタートも設定する場合は、fast hello パケットを使用するように OSPF プロセスを設定しないでください。fast hello パケットを使用するとグレースフルリスタートは発生しません。これは、アクティブユニットとスタンバイユニット間のロール変更にかかる時間が、設定されている dead 間隔を超えるためです。

グレースフルリスタートを設定するには、次の手順を実行します。

a) + をクリックして、**configure nsf graceful-restart** コマンドを有効にします。
b) *mechanism* 変数をクリックして、次のいずれかを選択します。

- **cisco** Cisco RFC 4811 および RFC 4812 に従って NSF 対応デバイスを設定します。
- **ietf** IETF RFC 3623 に従って NSF 対応デバイスを設定します。
- **both** NSF 対応デバイスではなく NSF 認識ヘルパーとしてデバイスを設定します。
- **none** グレースフルリスタートを無効にします（事前に設定している場合）。

c) 前の手順での選択内容により、仕様に従ってグレースフルリスタートを実装するために必要なコマンドが追加されます。これらのコマンドは無効にしないでください。必要に応じて詳細な設定が必要となるコマンドが 1 つだけあります。次に、追加されたコマンドの説明を示します。このコマンドの **no** 形式は、関連する機能をオフにします。

- **nsf cisco helper**を使用して無効にすることができます。Cisco Nonstop Forwarding（NSF）ヘルパーモードを有効にします。NSF 対応 Threat Defense デバイスがグレースフルリスタートを実行しているときに、ヘルパー Threat Defense デバイスはそのノンストップ フォワーディングの復帰プロセスを支援します。
- **nsf ietf helper** *mode-option*。IETF ノンストップ フォワーディング（NSF）ヘルパーモードを有効にします。NSF 対応 Threat Defense デバイスがグレースフルリスタートを実行しているときに、ヘルパー Threat Defense デバイスはそのノンストップ フォワーディングの復帰プロセスを支援します。オプションで、*mode-option* をクリックして、厳密なリンクステートアドバタイズメント（LSA）チェックを有効にすることができます。厳密な LSA チェックを有効にすると、再起動しているシステムにフラッディングする可能性がある LSA の変更があることをヘルパーシステムが検出した場合、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、再起動しているシステムの再送リスト内に変更された LSA がある場合、ヘルパーシステムは再起動しているシステムのプロセスの支援を終了します。
- **capability lls**を使用して無効にすることができます。シスコ グレースフルリスタートに必要なリンクローカルシグナリング（LLS）を有効にします。
- **capability opaque**を使用して無効にすることができます。IETF グレースフルリスタートに必要な Opaque リンクステート アドバタイズメント（LSA) を有効にします。

ステップ 13 [OK] をクリックします。

OSPF エリアプロパティの設定

複数の OSPF エリア パラメータを設定できます。エリア内でアドバタイズするネットワークに加えて、フィルタリングと仮想リンクを定義できます。さらに、これらのエリアパラメータには、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。

エリアパラメータを設定する場合は、システムがエリア内でどのように機能するかを把握しておく必要があります。

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 はリンクステート アドバタイズメント（LSA）を使用して、使用可能なルータ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すると、ABR として機能するシステムを使用して、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。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 エリア番号を設定します。

a) **area** *area-id* 行の左にある [+] をクリックして、コマンドを有効にします。コマンドは有効にするまで設定できません。

b) *area-id* をクリックし、エリアの番号を入力します。このエリア番号は、OSPFv2 エリアを定義する他のルータで使用されている番号と同じである必要があります。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

ステップ 6 エリア内でルーティングする必要があるネットワークとインターフェイスを設定します。

a) **configure area** *area-id options* 行の左にある [+] をクリックします。

b) *area-id* をクリックし、 **area** コマンドと同じエリア番号を入力します。

c) *options* をクリックして、**properties** を選択します。このアクションにより複数の行が追加されます。これには、デフォルトで有効になっている行、**network** コマンドが含まれます。

d) **network** コマンドで *network-object* をクリックし、この領域に含めるネットワークを定義するオブジェクトを選択します。通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

e) （オプション）**network** コマンドで *tag-interface* をクリックして、ネットワークにホストまたはルーティングするインターフェイスを選択します。このインターフェイスを選択す

ると、それがルーティングプロセスで使用されるため、インターフェイス上のアドレスを変更できなくなる場合があります。この場合、インターフェイスアドレッシングへの変更がルーティング設定に影響を与える可能性があることがわかります。

ここでインターフェイスを選択した場合は、インターフェイス上のアドレスを変更する前に、まずルーティングプロセスからインターフェイスを削除する必要があります。次に、IPアドレスを変更した後、必ずここに戻り、新しいネットワークとインターフェイスを選択して、ルーティングプロセスが正しく設定されていることを確認します。

ステップ 7 （オプション）スタブエリアまたはNot-So-Stubby Area（NSSA）に送信されるデフォルトサマリールートのコストを設定します。

このオプションは、次に説明するように、エリアをスタブまたはNSSAとして設定した場合にのみ有効です。[+] をクリックして、エリアプロパティの次のコマンドを有効にします。

area *area-id* **default-cost 1**

必要に応じて、正しいエリア ID を入力します。次に、番号をクリックして、ルートの相対コストを 0 ～ 16777214 の範囲で入力します。デフォルトは 1 です。数値が大きいほど、宛先に適用される別のルートでルートが使用される可能性が低くなります。

ステップ 8 （オプション）エリアのプレフィックス フィルタリングを設定します。

エリアボーダールータ（ABR）のOSPFv2エリア間のタイプ3リンクステートアドバタイズメント（LSA）でアドバタイズされたプレフィックスをフィルタ処理することができます。プレフィックスの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。プレフィックスのフィルタリングでは、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。

このコマンドを設定する前に、**[デバイス（Device）] > [詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトであるプレフィックスリストを作成する必要があります。インバウンドまたはアウトバウンドアドバタイズメントに対して個別のプレフィックスリストを設定できます。フィルタ方向パラメータの方向を選択します。

area *area-id* **filter-list prefix** *prefix-list filter-direction*

ステップ 9 （オプション）エリアをスタブエリアとして設定します。

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。適切に動作させるには、スタブエリアでデフォルトルーティングを使用する必要があります。スタブエリアに送信される LSA の数をさらに減らすには、ABR で実行する **area stub** コマンドに **no-summary** キーワードを設定して、スタブエリアにサマリー リンク アドバタイズメント（LSA タイプ 3）が送信されないようにします。

エリアをスタブとして設定するには、以下を実行します。

a) [setup area-id as type] 行の左にある [+] をクリックします。
b) [type] をクリックし、**stub** を選択します。これにより、セットアップ行の後に area stub コマンドが追加されます。

c) オプションで、**area stub** コマンドで [stub-parameters] をクリックし、**no-summary** を選択します。

ステップ 10 （オプション）エリアを Not-So-Stubby Area（NSSA）に設定します。

Not-So-Stubby Area（NSSA）は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 のエリア境界ルータ（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。

OSPF 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、接続エリアに NSSA を利用することによって管理を簡略化できます。スタブエリアにはリモートサイトのルートが再配布されないため、企業サイトの境界ルータとリモートルータ間の接続に OSPFv2 スタブエリアを利用できず、2 つのルーティングプロトコルを維持する必要がありました。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。

エリアを NSSA として設定するには、以下を実行します。

a) **setup** *[area-id]* **as** *[type]* 行の左にある [+] をクリックします。
b) [type] をクリックし、**nssa** を選択します。これにより、setup 行の後に、**area nssa** コマンドを含む複数のコマンドが追加されます。このコマンドはイネーブルのままにする必要があります。
c) （オプション）NSSA にタイプ 7 のデフォルトルートを生成するには、[+] をクリックして次のコマンドを有効にします。

   area *area-id* **nssa default-information-originate metric 1 metric-type 2**

   オプションで、次の値を調整できます。

   - **metric** の数値をクリックして、OSPF のデフォルトメトリック値を入力します（0 ～ 16777214）。別の値が必要であることがわかっている場合を除き、「10」と入力します。
   - **metric-type** の数値をクリックして、OSPF 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る外部リンクタイプを選択します（1 または 2）。デフォルトは 2 です。

d) （オプション）システムが ABR であり、他のルーティングプロトコルから再配布して、NSSA ではなく通常のエリアにのみルートをインポートする場合は、[+] をクリックして次のコマンドを有効にします。

area *area-id* **nssa no-redistribution**

e) （オプション）サマリールートを NSSA に挿入しない場合は、[+] をクリックして次のコマンドを有効にします。

area *area-id* **nssa no-summary**

ステップ 11 （オプション）エリアの仮想リンクを設定します。

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。バックボーンエリアに接続されているルータへの仮想リンクを設定できます。

a) **configure area** *[area-id]* **virtual-link** *[ip_address option]* 行の左にある [+] をクリックします。

b) [ip_address] をクリックして、仮想リンクを確立するルータのルータ ID を入力します。

c) （オプション）[option] をクリックして **properties** を選択し、次の属性を調整します。これらの属性はすべて、ほとんどのネットワークに適したデフォルト値になっています。これらのコマンドの最初の部分は、同じコマンドのパラメータであるため、省略されています。

- **authentication** *auth-type*。[+] をクリックしてコマンドを有効にし、[auth-type] をクリックして **none**、**password**、または **message-digest** を選択します。[none] 以外の項目を選択した場合は、キーオプションを設定します。このオプションは、OSPFv2 インターフェイスと OSPF 認証の設定（475 ページ） で説明されているように、OSPF インターフェイスで設定するものと同じです。他のルータが認証を使用している場合にのみ、認証を設定します。
- **hello-interval 10**を使用して無効にすることができます。番号をクリックし、インターフェイスで送信される hello パケットの間隔を 1 ～ 65535 秒の範囲で入力します。
- **retransmit-interval 5**を使用して無効にすることができます。番号をクリックし、仮想リンクの LSA 再送信間の時間を 1 ～ 65535 秒の範囲で入力します。
- **transmit-delay 1**を使用して無効にすることができます。番号をクリックし、OSPF がトポロジ変更を受信してから最短パス優先（SPF）計算を開始するまでの遅延時間を 0 ～ 65535 秒の範囲で入力します。

d) 別の仮想リンクを定義するには、**[...]** > **[重複（Duplicate）]**（**configure area virtual-link** コマンドの横）をクリックします。必要な数だけ定義します。

ステップ 12 （オプション）システムがエリア境界ルータ（ABR）の場合は、エリアのルートを統合または集約するための範囲を設定します。

area range コマンドを設定すると、その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は、「経路集約」と

呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。このように、OSPF は多くの異なるアドレス範囲セットのアドレスを集約できます。

ルート集約を設定するには、以下を実行します。

a) **area** *[area-id]* **range** *[network-object range-parameters]* 行の左側にある [+] をクリックします。
b) [network-object] をクリックし、集約するルートのアドレス範囲を定義するネットワークオブジェクトを選択します。
c) （オプション）[range-parameters] をクリックし、次のいずれかの属性を選択します。
   - **advertise**を使用して無効にすることができます。アドバタイズするアドレス範囲ステータスを設定し、タイプ 3 サマリー リンクステート アドバタイズメント（LSA）を生成します。これは、[no] オプションを選択した場合のデフォルトです。
   - **not-advertise**を使用して無効にすることができます。アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。
d) 別のルート集約を定義するには、**[...]** > **[重複（Duplicate）]**（**area range** コマンドの横）をクリックします。必要な数だけ定義します。

ステップ 13 マルチエリアネットワークのプロセスを設定する場合は、**area** と **configure area** の行の丸で囲まれた [-] の左側の領域にカーソルを合わせ、**[...]** > **[重複（Duplicate）]** をクリックします。次に、前述のように、新しいエリアとそのネットワークを設定します。このルーティングプロセスが参加する必要があるすべてのエリアを定義するまで、このプロセスを繰り返します。

ステップ 14 [OK] をクリックします。

スタティック OSPF ネイバーの設定

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、つまり、VPN トンネルを介して OSPF 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。

通常のブロードキャスト ネットワークのルータは隣接関係を形成できるため、それらのネットワーク上にあるスタティックネイバーを定義する必要はありません。

始める前に

システムがネイバーに到達するために使用するインターフェイスを決定します。ネイバールータを定義する前に、このインターフェイスの OSPF 設定を設定する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF インターフェイス オブジェクトを追加または編集し、選択したインターフェイスに対して **ospf network point-to-point non-broadcast** コマンドを有効にします。変更を保存します。

ステップ 5 OSPF プロセスオブジェクトを追加または編集します。

ステップ 6 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **neighbor** コマンドを有効にします。

ステップ 7 ネイバーアドレスを設定します。

neighbor *ip-address* **interface** *interface*

- [ip-address] をクリックし、ネイバールータの IP アドレスを入力します。
- [interface] をクリックして、システムがルータに到達するために使用するインターフェイスを選択します。

ステップ 8 必要に応じて、ネイバールータのスタティックルートを設定します。

ルータの IP アドレスが、選択したインターフェイスと同じネットワーク上にある場合、スタティックルートは必要ありません。たとえば、IP アドレスが 10.100.10.1/24 であるインターフェイスを選択し、ネイバーアドレスが 10.100.10.2/24 の場合、スタティックルートは必要ありません。

ステップ 9 **[...]** > **[重複（Duplicate）]**（**neighbor** コマンドの横）をクリックして、別のスタティックネイバーを定義できます。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

OSPF サマリー アドレスの設定

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。ただし、再配布されるルートのうち、指定のネットワークアドレスとマスクに含まれるすべてのものを 1 つのルートで表し、そのルートだけをアドバタイズするようにシステム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廃止できます。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。他のルーティングプロトコルから学習したルートを集約できます。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。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。

始める前に

集約するすべてのアドレスのネットワークオブジェクトを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 [Show Disabled] をクリックしてすべてのコマンドを公開し、[+] をクリックして **configure** *network-object* **as** *option* **summary-address** コマンドを有効にします。

ステップ 6 [network-object] をクリックし、集約するアドレス空間を定義するオブジェクトを選択します。

ステップ 7 [options] をクリックし、次のいずれかを選択します。

- **advertising**を使用して無効にすることができます。アドレスに一致するルートをアドバタイズします。
- **non-advertising**を使用して無効にすることができます。アドレスに一致するルートを抑制します。

ステップ 8 （オプション）集約されたルートにタグ値を追加するには、[+] をクリックして **summary-address tag** コマンドを有効にし、[tag-number] 変数をクリックして、タグ番号（0 ～ 4294967295）を入力します。

この値は OSPF 自体には使用されません。自律システム境界ルータ（ASBR）間で情報を通信するために使用できます。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、その他のプロトコルには 0 が使用されます。

タグ値を使用する主な理由は、タグ番号に基づいて再配布を制御することです。再配布ルートマップでタグ値を使用しない場合は、ここで設定する必要はありません。

ステップ 9 別のルート集約を定義するには、**[...] > [重複（Duplicate）]**（**configure summary-address** コマンドの横）をクリックします。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

OSPF のフィルタ ルールの設定

各フィルタルールに必要なスマート CLI 標準アクセスリストオブジェクトを作成します。拒否アクセス制御エントリ（ACE）を使用してエントリに一致するルートを除外し、更新する必要があるルートの ACE を許可します。

始める前に

エリア境界ルータ（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。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 [無効を表示（Show Disabled）] をクリックしてすべてのコマンドを表示し、[+] をクリックして **configure filter-rules** *direction* コマンドを有効にします。

ステップ 6 [direction] をクリックし、**in**（インバウンドアップデートをフィルタ処理する場合）または **out**（アウトバウンドアップデートをフィルタ処理する場合）を選択します。

ステップ 7 インバウンドフィルタの場合は、必要に応じて、アップデートをフィルタ処理するインターフェイスを指定できます。インターフェイスを指定しない場合、フィルタは任意のインターフェイスで受信されるすべてのアップデートに適用されます。

a) [+] をクリックして **distribute-list** *acl-name* **in interface** *interface* コマンドを有効にします。

b) [interface] 変数をクリックし、インターフェイスを選択します。

ステップ 8 アウトバウンドフィルタの場合は、必要に応じて、プロトコルを指定して、そのルーティングプロセスにアドバタイズされたルートにフィルタを制限できます。

distribute-list out コマンドには 2 つの形式があります。一方には [protocol] 変数の後に [identifier] 識別子があり、もう一方には [identifier] 識別子がありません。次のプロトコルを選択できますが、追加の識別子情報を提供する必要があるかどうかに基づいて、これらのコマンドのバージョン間でプロトコルが分けられます。

- **connected**を使用して無効にすることができます。システムのインターフェイスに直接接続されているネットワークに対して確立されたルート用です。
- **static**を使用して無効にすることができます。手動で作成したスタティックルート用です。
- **rip**を使用して無効にすることができます。RIP にアドバタイズされたルート用です。
- **bgp** *automonous-system*：BGP にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている BGP プロセスの自律システム番号を入力します。
- **eigrp** *automonous-system*：EIGRP にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている EIGRP プロセスの自律システム番号を入力します。

- **ospf** *process-id*：OSPF にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている他の OSPF プロセスのプロセス ID を入力します。

ステップ 9 **[...] > [重複（Duplicate）]**（**configure filter-rules** コマンドの横）をクリックして、別のフィルタルールを定義します。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

OSPF 再配布の設定

他のルーティングプロトコル、接続されたルート、およびスタティックルートからの OSPF プロセスへのルートの再配布を制御できます。

始める前に

OSPF への再配布を設定する前に、ルートを再配布するルーティングプロセスを設定し、変更を展開することがベストプラクティスです。

ルートマップを適用して、再配布されるルートを微調整する場合は、Smart CLI ルートマップオブジェクトを作成します。ルートマップに一致するルートが再配布され、一致しないルートはすべて再配布されません。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **configure redistribution** コマンドを有効にします。

ステップ 6 [protocol] 変数をクリックし、ルートの再配布元となる送信元プロセスを選択します。**connected** および **static** のルート、あるいは **bgp**、**eigrp**、**isis**、**ospf**、または **rip** のいずれかによって生成されたルートを再配布できます。

ステップ 7 ルーティングプロセスを選択した場合は、[identifier] 変数をクリックして、必要な値を入力します。

- **bgp**、**eigrp**：自律システムの番号を入力します。
- **ospf**を使用して無効にすることができます。プロセス ID 番号を入力します。
- **connected**、**static**、**isis**、**rip**。**none** を入力します。別の値を入力しても、無視されます。

ステップ 8 （任意：IS のみ）**redistribute isis level-2** コマンドで、**level-2** をクリックして、IS-IS エリア（**level-1**）内でのみ学習したルートを再配布するか、IS-IS エリア（**level-2**）間、または両方（**level-1-2**）で再配布するかを選択します。

ステップ 9 （任意：すべてのプロトコル）再配布を制御するためにタグをルートに適用する場合は、[+] をクリックして **redistribute tag** *tag-number* コマンドを有効にし、変数をクリックして、再配布するルートに関連付けられているタグを入力します。タグ番号の範囲は 0 ～ 4294967295 です。

ステップ 10 （任意：すべてのプロトコル）標準クラスに準拠するものだけでなく、すべてのサブネットのルートを再配布する場合は、[+] をクリックして **redistribute subnets** コマンドを有効にします。

たとえば、このコマンドを有効にしない場合、10.100.10.0/24 の特定のルートは再配布されず、代わりに、10.0.0.0/8 のルートのみが再配布されます。

ステップ 11 （任意：すべてのプロトコル）ルートマップに基づいて再配布されるルートを微調整するには、[+] をクリックして **redistribute** *route-map* コマンドを有効にし、変数をクリックして、制限を定義するルートマップを選択します。

ルートマップを適用しない場合は、（再配布用に設定された他のコマンドに適合する）プロセスのすべてのルートが再配布されます。

ステップ 12 （任意：すべてのプロトコル）再配布されたルートのメトリックを微調整するには、[+] をクリックして次のコマンドを有効にし、オプションを設定します。

redistribute *protocol* **metric** *metric-value* **metric-type** *metric-type-value*

変数をクリックして、次のように設定します。

- **metric**を使用して無効にすることができます。配布されているルートのメトリック値（0 ～ 16777214）。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に渡されます。他のプロセスを OSPF プロセスに再配布する場合、デフォルトのメトリックは 20 です。
- **metric-type**を使用して無効にすることができます。メトリックタイプは、OSPF 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。デフォルトは 2 です。

ステップ 13 （任意：OSPF のみ）別の OSPF プロセスからルートを再配布する場合、次のコマンドはデフォルトで有効になっています。[-] をクリックして、不要なコマンドを無効化できます。

これらのコマンドで、OSPF ルートを他のルーティングドメインに再配布する条件を指定します。

- **redistribute ospf match external 1**を使用して無効にすることができます。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。
- **redistribute ospf match external 2**を使用して無効にすることができます。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。

- **redistribute ospf match internal**を使用して無効にすることができます。特定の自律システムの内部ルート。
- **redistribute ospf match nssa-external 1**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。
- **redistribute ospf match nssa-external 2**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。

ステップ 14 **[...]** > **[重複（Duplicate）]**（**configure redistribution** コマンドの横）をクリックして、別のプロトコルの再配布を設定できます。ネットワークに適したプロトコルごとの再配布を設定します。

ステップ 15 [OK] をクリックします。

OSPFv2 インターフェイスと OSPF 認証の設定

ネイバー OSPF ルータに面しているインターフェイスは、hello パケットなどの方法を用いてルータと通信して、ネイバーの正常性を確認し、ルーティングの更新を共有します。これらの特性の一部にはデフォルト設定がありますが、ベストプラクティスは、OSPF インターフェイス設定オブジェクトを使用してオプションを明示的に設定する方法です。OSPF ネイバールータに隣接する各インターフェイスのオブジェクトを作成します。

（注） ネットワーク上の各ルータは、認証および失われたネイバー検出の hello と dead 間隔について同じ値を持つ必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいオブジェクトを作成するには、**[+]** > **[OSPFインターフェイス設定（OSPF Interface Settings）]** をクリックするか、**[OSPFオブジェクトの作成（Create OSPF Object）]** > **[OSPFインターフェイス設定（OSPF Interface Settings）]** ボタンをクリックします。

- 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

インターフェイス設定オブジェクトが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 6 インターフェイスの認証を設定します。

configure authentication *auth-type*

OSPF 認証を設定するには、各 OSPF インターフェイスでパスワードまたは認証キーを設定してから、そのエリア自体で認証を有効にする必要があります。インターフェイスとエリアで同じ認証方式を選択する必要があります。

auth-type をクリックして、次のオプションを選択できます。

- **none**：OSPF 認証を使用しない。リンクで動作するすべての OSPF ルータは、このルータとの隣接関係を確立できます。オブジェクトにコマンド **ospf authentication null** が追加されます。
- **password**：共有パスワードを使用して OSPF 接続を認証する。インターフェイス単位で各ネットワークに個別のパスワードを設定できます。とはいえ、OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータに同じパスワードを設定する必要があります。

  このオプションを選択すると、2 つのコマンド（**ospf authentication** および **ospf authentication-key** *key*）が追加されます。変数をクリックして、次のように設定します。

  - *key*：パスワードが格納されている秘密鍵オブジェクトを選択します。パスワードは最大 8 文字です。2 文字間にブランクを含めることができます。パスワードの先頭または末尾のブランクは無視されます。オブジェクトがまだ存在しない場合、リストの下部にある [新しい秘密鍵の作成（Create New Secret Key）] をクリックして作成します。

- **message-digest**：メッセージダイジェスト（MD5）を使用して OSPF 接続を認証します。MD5 認証は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。両方のルータで同じ MD5 キーが使用されるように設定する必要があります。

  このオプションを選択すると、2 つのコマンド（**ospf authentication message-digest** および **ospf message-digest-key** *key-id* **md5** *key*）が追加されます。変数をクリックして、次のように設定します。

  - *key-id*：1 ～ 255 の認証キー ID 番号。同じキー ID および関連付けられた MD5 キーを使用して、ネイバールータを設定する必要があります。
  - *key*：MD5 キーが格納されている秘密鍵オブジェクトを選択します。キーは最大 16 文字の英数字のパスワードです。文字間にスペースを含めることができます。キーの先頭または末尾のスペースは無視されます。オブジェクトがまだ存在しない場合、リス

トの下部にある [新しい秘密鍵の作成（Create New Secret Key）] をクリックして作成します。

ステップ 7 （オプション）リンクステート アドバタイズメント（LSA）タイマーを設定します。

これらのタイマーにはデフォルト値があるため、ネットワークで別の設定が必要な場合にのみ変更する必要があります。次のコマンドを設定します。

- **ospf retransmit interval 5**：OSPF インターフェイスに属する隣接ルータに LSA を再送信する間隔の秒数。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秒数にする必要があります。範囲は 1 ～ 8192 秒です。デフォルト値は 5 秒です。5 をクリックし、新しい数値を入力して値を変更します。
- **ospf transmit-delay 1**：OSPF 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ために必要な推定秒数（1 ー 8192 秒）。デフォルト値は 1 秒です。1 をクリックし、新しい数値を入力して値を変更します。

ステップ 8 （オプション）他のすべての設定は、デフォルト値が設定されているか、オプションです。別の動作が必要な場合にのみ、それらを変更するか有効にします。オプションを表示するには、[無効を表示（Show Disabled）] リンクをクリックします。

次に、付加的なインターフェイス設定を示します。設定を有効にするには、コマンドの左側にある [+] をクリックして、コマンドを設定します（必要な場合）。

- **ospf cost** *value*：OSPF インターフェイスでパケットを送信するコスト（リンクステートメトリック）（1 ～ 65535）。値 1 は、インターフェイスに直接接続されているネットワークを表します。変数をクリックし、ネットワークで使用している番号に基づいてインターフェイスの性能を表すコストを入力します。

  値を決定する際、インターフェイスの帯域幅が大きいほど、そのインターフェイスでパケットを送信するための関連コストが低くなります。つまり、コストの値が大きければインターフェイス帯域幅が小さく、コストの値が小さければインターフェイス帯域幅が大きいということになります。選択した特定の数値には固有の意味はありません。この値は、OSPF エリア全体でインターフェイスに設定したその他の値に相対的なものです。これらの値は、接続先への最適ルートの計算に影響します。

  脅威に対する防御デバイスでの OSPF インターフェイスのデフォルトのコストは 10 です。このデフォルトは、Cisco IOS ソフトウェアとは異なります。Cisco IOS ソフトウェアの場合、デフォルトのコストはファストイーサネットおよびギガビットイーサネットでは 1、10BaseT では 10 です。ネットワークで ECMP を使用している場合には、このことを考慮に入れることが重要です。

- **ospf database-filter all out**：同期およびフラッディング中の OSPF インターフェイスへのすべての発信 LSA をフィルタで除外します。
- **ospf mtu-ignore**：受信データベースパケットの OSPF 最大伝送ユニット（MTU）不一致検出を無効にします。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、ネイバーがデータベース記述子（DBD）パケットを交換するときに実行されます。DBD パケット内の受信 MTU が着信インター

フェイスに設定されている MTU より高い場合、OSPF の隣接性は確立されません。インターフェイス上の MTU 値を同じ値に修正できない場合は、MTU チェックを無効にすることができます。

- **ospf network point-to-point non-broadcast**：OSPF 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 ネットワークとして設定します。この設定により、VPN トンネルを介して OSPF ルートを送信できるようになります。このオプションを設定すると、ネイバーを動的に検出できなくなります。次の手順の実行も必要です。
  - このインターフェイスに対して 1 つのスタティックネイバーを定義するには、OSPF プロセスオブジェクトを更新します。また、ネイバールータの OSPF プロセスを更新して、このデバイスをスタティックネイバーとして定義します。
  - ネイバールータを指すスタティックルート（各ルータ上）を作成します。
- **ospf priority** *value*：ネットワーク内の他のルータと相対的なルータのプライオリティ（0 ～ 255）。デフォルトのプライオリティは 1 です。ネットワークにアタッチされている 2 つのルータがともに指定ルータになろうとした場合、ルータのプライオリティの高い方が優先されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。ルータのプライオリティがゼロに設定されているルータには、指定ルータまたはバックアップ指定ルータになる資格がありません。変数をクリックし、ネットワークで使用する相対的な番号付け方式に基づいて優先順位を選択します。
- **ospf lost-neighbor-detection** *detection-mechanism*：ネイバールータがダウンしているかどうかをシステムがどのように判断するかを定義します。OSPF は、OSPF ルータがダウンしていると宣言されるたびにルートを再計算する必要があります。失われたネイバー検出の設定の詳細については、OSPFv2 の失われたネイバー検出と fast hello パケットの設定（OSPF インターフェイス設定）（478 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。

OSPFv2 の失われたネイバー検出と fast hello パケットの設定（OSPF インターフェイス設定）

OSPF プロセスは定期的に各ネイバールータに hello パケットを送信し、ネイバーが応答できることを確認します。応答の継続的な失敗は、ネイバールータ（全インターフェイスまたは隣接するインターフェイスのみ）がルーティングに使用できないことを示し、OSPF はルートを再計算する必要があり、OSPF システムは更新されたルーティングテーブルへのコンバージェンスが必要となります。

次の値を調整して、ネットワークを微調整できます。理想的には、ネイバーがダウンしていると宣言され、ルートが再計算される頻度を最小限に抑える必要があります。一方、OSPF ルータ（またはインターフェイス）が実際にダウンしたときに、ネットワークが適切なルーティングテーブルに再コンバージェンスするのにかかる時間を最小限に抑える必要もあります。

- [hello間隔（Hello interval）]：hello パケットを送信する時間の間隔です。デフォルトは 10 秒ごとです。必要に応じて、hello が 1 秒未満の間隔で送信される fast hello パケットを設定できます。fast hello パケットを使用すると、ダウンしているネイバーの検出と、ルーティングテーブルの再コンバージェンスが最速になります。
- [dead間隔（Dead interval）]：ネイバーから hello パケットが検出されなかった場合に、ネイバーが dead と宣言されるまでの時間の長さ。デフォルトは 40 秒（デフォルトの hello 間隔の 4 倍）です。ただし、fast hello パケットを使用している場合を除きます（この場合 dead 間隔は常に 1 秒）。小さい dead 間隔を指定すると、ダウンしているネイバーの検出が速くなり、コンバージェンスが向上しますが、ルーティングが不安定になる可能性があります。どのような場合でも、dead 間隔は hello 間隔よりも大きい値に設定する必要があります。ネットワーク内のすべての OSPF ルータで同じ dead 間隔を設定する必要があります。

[OSPFインターフェイス設定（OSPF Interface Settings）] オブジェクトで、失われたネイバー検出を設定します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいオブジェクトを作成するには、**[+]** > **[OSPFインターフェイス設定（OSPF Interface Settings）]** をクリックするか、**[OSPFオブジェクトの作成（Create OSPF Object）]** > **[OSPFインターフェイス設定（OSPF Interface Settings）]** ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 **ospf lost-neighbor-detection** *detection-mechanism* コマンドが表示されない場合は、[無効を表示（Show Disabled）] リンクをクリックします。

ステップ 6 コマンドを有効にするには、コマンドの左側にある [+] をクリックします。

ステップ 7 *detection-mechanism* をクリックし、実装するメカニズムを選択します。

- **dead-interval**：標準の hello 間隔を秒単位で設定します。次のコマンドが追加されます。必要に応じて値を調整します。
  - **ospf hello-interval 10**：hello 間隔（1 ～ 8192 秒）。デフォルトは 10 です。この値は、dead 間隔より小さくする必要があります。値をクリックして、目的の数字を入力します。

- **ospf dead-interval 40**：dead 間隔（1 ～ 8192 秒）。推奨値は hello 間隔の 4 倍ですが、コンバージェンスを高速化するために短い時間を設定できます。

- **hello-multiplier**：1 秒未満の fast hello パケットを設定します。次のコマンドが追加されました。値を設定する必要があります。
  - **ospf dead-interval minimal hello-multiplier** *value*：変数をクリックし、1 秒間に送信する hello パケットの数を 3 ～ 20 の間で入力します。dead 間隔は、**minimal** キーワードによって 1 秒に設定されます。

ステップ 8 [OK] をクリックします。

OSPF のモニタリング

OSPF をモニターし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。また、[ルーティング（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

追加オプションのリストを取得するには、**show ospf ?** を使用します。たとえば、プロセス ID、エリア ID、および仮想ルータを指定して、表示する情報を制限することができます。また、探している情報だけを対象とするその他のオプションも指定できます。次のリストは概要のみです。

- **show ospf**

  OSPFv2 ルーティング プロセスに関する一般情報を表示します。

- **show ospf border-routers**

  ABR および ASBR までの内部 OSPFv2 ルーティング テーブル エントリを表示します。

- **show ospf database**

  特定のルータの OSPFv2 データベースに関係する情報のリストを表示します。

- **show ospf events**

  OSPF 内部イベント情報を表示します。

- **show ospf flood-list**

  OSPFv2 パケットペーシングの観察のために、インターフェイスへのフラッディングを待機している LSA のリストを表示します。OSPFv2 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。

ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv2 アップデートおよび再送信パケットの送信の効率をよくすることです。

- **show ospf interface**

  OSPFv2-related インターフェイスの情報を表示します。

- **show ospf neighbor**

  OSPFv2 ネイバー情報をインターフェイスごとに表示します。

- **show ospf nsf**

  OSPFv2 関連のノンストップ フォワーディング（NSF）情報を表示します。

- **show ospf request-list**

  ルータで要求されるすべての LSA のリストを表示します。

- **show ospf retransmission-list**

  再送信を待機しているすべての LSA のリストを表示します。

- **show ospf rib**

  OSPF ルータ情報ベース（RIB）を表示します。

- **show ospf statistics**

  さまざまな OSPF 統計（SPF が実行された回数、理由、期間など）を表示します。

- **show ospf summary-addresses**

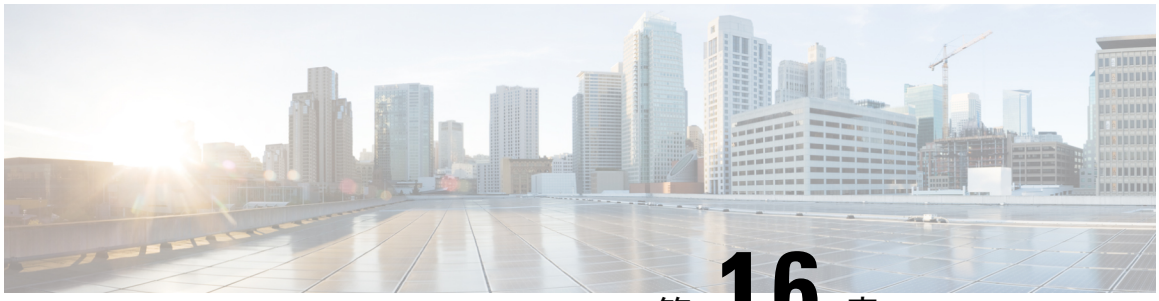
  OSPFv2 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。

- **show ospf traffic**

  特定の OSPFv2 インスタンスで送信または受信されたパケットのさまざまなタイプのリストを表示します。

- **show ospf virtual-links**

  OSPFv2-related 仮想リンク情報を表示します。



第 16 章

Enhanced Interior Gateway Routing Protocol（EIGRP）

Enhanced Interior Gateway Routing Protocol（EIGRP）は、ディスタンスベクターとリンクステートのハイブリッド内部ゲートウェイ ルーティング プロトコルです。当初はシスコが開発した独自のプロトコルでしたが、現在では RFC 7868 で定義されているオープン標準になっています。自律システム内の内部ルートを管理するように EIGRP を設定できます。

EIGRP のベストプラクティス

EIGRP の設定に関するいくつかのヒントを次に示します。

- デバイスを既存の EIGRP 自律システムに挿入する場合は、自律システム内の他のルータの設定を調べて、システム番号とその他のカスタマイズを確認します。追加する Threat Defense デバイスには、必ず、同じカスタマイズ（または少なくとも一貫性のあるカスタマイズ）を実装してください。
- 完全な EIGRP プロセスまたはスタブプロセスのどちらを設定するのかを決定します。
  - Threat Defense デバイスが自律システムの中央にあり、他の複数の EIGRP ルータに接続されている場合は、完全な EIGRP プロセスが必要です。完全なルーティングのための EIGRP プロセスの設定 （486 ページ） を参照してください。
  - Threat Defense デバイスが自律システムのエッジにあり、他の 1 つの EIGRP ルータにのみ接続されていて、それ以外は、接続されたネットワークのみをホストする場合は、それをスタブルータとして設定することが最も合理的である可能性があります。Threat Defense デバイスが接続されたルートに関する情報を EIGRP ネイバーに送信するようにスタブを設定して、自律システム内の他の EIGRP ルータが Threat Defense デ

バイスの接続されたネットワークへのルートを取得できるようにすることが可能です。スタブルーティングのための EIGRP プロセスの設定 （488 ページ） を参照してください。

- デフォルト設定はほとんどのネットワークで機能するため、自律システム内の他のEIGRPルータで設定を調整した場合にのみ設定を調整してください。自律システム番号を設定し、ルーティングするネットワークを指定するだけで、完全に機能する EIGRP プロセスを実現できます。
- ルータ ID を設定して、ルータを識別するために安定したアドレスが使用されるようにします。これにより、ルーティングに関する問題のトラブルシューティングが容易になります。EIGRP の詳細設定の設定 （491 ページ） を参照してください。
- ルーティングループが発生せず、ネットワークに何らかの利点をもたらすと判断される場合以外は、自動ルート集約（**auto-summary** コマンド）を有効にしないでください。自動集約がネットワークで機能するかどうかを判断する方法は、このドキュメントの範囲外です。

EIGRP について

Enhanced Interior Gateway Routing Protocol（EIGRP）は、ディスタンスベクターとリンクステートのハイブリッド内部ゲートウェイ ルーティング プロトコルです。EIGRP は同じ自律システム内のルータにルーティング更新を送信します。通常、EIGRPはマルチキャスト更新を使用してネイバールータを検出しますが、マルチキャスト境界の外側にある静的ネイバーを設定でき、これらの静的ネイバーはユニキャスト更新を取得します。

EIGRP のコンバージェンス テクノロジーは、Diffusing Update Algorithm（DUAL）と呼ばれるアルゴリズムに基づいています。このアルゴリズムは、ルート計算中のどの時点でもループが発生しないようにし、トポロジ変更に関与するすべてのデバイスを同期できるようにします。トポロジ変更の影響を受けないデバイスは、再計算に含まれません。

限られた範囲で、ルーティングメトリックを調整して、ルートの選択方法を制御できます。以下のトピックでは、これらの高度な概念の背景について説明します。

（注） これらのメトリックを調整する場合、自律システム内のすべてのルータに同じ調整を行う必要があります。そうしないと、ルーティングループが発生する可能性があります。

DUAL 有限状態マシン

DUAL 有限状態マシンには、すべてのルート計算の決定プロセスが組み込まれており、すべてのネイバーによってアドバタイズされたすべてのルートが追跡されます。DUAL は距離情報（メトリックともいう）を使用して、効率的な、ループのないパスを選択し、

さらに DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。サクセサは、宛先への最小コストパス（ルーティングループに関連しないことが保証されている）を持つ、パケット転送に使用される隣接デバイスです。

トポロジが変更されると、DUAL はフィージブルサクセサが存在するかどうかを確認します。フィージブルサクセサがある場合、DUAL は検出されたいずれかのフィージブルサクセサを使用して、不要な再計算を防止します。

フィージブルサクセサがなく、宛先にアドバタイズするネイバーだけがある場合は、再計算を行って新たなサクセサを決定する必要があります。ルートの再計算に必要な時間は、コンバージェンス時間に影響します。

EIGRP のメトリック重み

EIGRP は、ルーティングおよびメトリック計算でメトリックの重み（K 値と呼ばれる）を使用します。EIGRP メトリックのデフォルトは、大半のネットワークで最適なパフォーマンスを実現できるよう、慎重に選択されています。

IOS ルータとは異なり、Threat Defense デバイスで動作する EIGRP のデフォルトの K 値は調整できません。自律ネットワーク内のすべてのシステムで同じ K 値を使用する必要があるため、Threat Defense デバイスを含む自律システム内のすべてのルータでこれらの値を変更しないでください。

K 値の使用方法については、EIGRP コストメトリック （485 ページ）を参照してください。

EIGRP コストメトリック

EIGRP は、リンク特性に加えてメトリックの重み（K 値）を使用して、複合コストメトリックを計算します。リンク特性が変わった結果としてネットワーク内でチャーンが生じないようにするために、この計算で使用される値の一部を調整できます。

実際の計算は非常に複雑であり、5 つの K 値（乗数として）と 5 つのベクトル属性を使用します。ただし、3 つの K 値はデフォルトで 0 であり、K 値のデフォルトは変更できないため、実際の計算は大幅に簡素化されます。

コストメトリック = 256 *（帯域幅 + 遅延）

変更できるのは、EIGRP プロセスとの間で再配布されるルートの帯域幅と遅延の値です。具体的には、これらの値を **default-metric** コマンド（すべてのタイプの再配布ルートについてデフォルトを設定する）または **redistribute metric** コマンド（特定のタイプのルートについてメトリックを設定する）で調整できます。次の点に注意してください。

- 「帯域幅」はルートの最小帯域幅（キロビット/秒単位）です。1 ー 4294967295 キロバイト/秒を指定できます。この式の帯域幅は、次の式によってスケーリングおよび反転されます。

  （10^7/帯域幅（キロビット/秒単位））

- 「遅延」はルートの遅延（10 マイクロ秒単位）です。

Threat Defense で使用されないその他の特性は、遅延の信頼性、ルートの有効負荷、およびルートの最小 MTU（最大伝送ユニット）です。これらの値は使用されませんが、これらのコマンドを調整する場合は設定する必要があります。

EIGRP がコストメトリックを計算する方法の詳細については、『*IP Routing: EIGRP Configuration Guide*』を参照してください。例：https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-7/ire-xe-16-8-book/ire-enhanced-igrp.html。

EIGRP のガイドライン

IPv6 のガイドライン

IPv6 はサポートされません。

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。
- EIGRP プロセスの自律システム番号は変更できません。代わりに、プロセスを削除し、変更を展開してから、新しい自律システム番号を使用して新しいプロセスを設定してください。
- ブリッジ仮想インターフェイス（BVI）に属する EIGRP プロセスにネットワークを含めることはできません。
- 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。

コア EIGRP プロセスの設定

ここでは、デバイスで EIGRP を稼働状態にする方法について説明します。完全なルーティングプロセスを設定することも、EIGRP ルータとして自律ネットワークに完全に参加させないシステムのスタブプロセスとして設定することもできます。

完全なルーティングのための EIGRP プロセスの設定

1 つの EIGRP プロセスを設定できます。複数の仮想ルータを設定する場合、EIGRP はグローバル仮想ルータでのみサポートされます。

次の手順では、EIGRP ルーティングのすべてのデフォルト値を使用して、一連のネットワークの基本的な EIGRP ルーティングをセットアップします。デバイスで EIGRP を有効にするに

は、この手順を完了するだけで十分です。必要に応じて、他の手順を実行して EIGRP プロセスを微調整できます。

始める前に

ネットワークで EIGRP に使用している自律システム番号を確認します。

EIGRP 自律システム内でルーティングする各ネットワークを定義するネットワークオブジェクトを作成します。たとえば、192.168.1.0/24 ネットワークと 192.168.2.0/24 ネットワークに EIGRP を使用する場合は、各ネットワークに 1 つずつ、2 つのネットワークオブジェクトを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（  ）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいプロセスを作成するには、[+]をクリックするか、[EIGRPオブジェクトの作成（Create EIGRP Object）] ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

プロセスが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力し、任意で説明を入力します。

ステップ 6 基本的なプロセスのプロパティを設定します。

router eigrp *autonomous-system*

変数をクリックし、番号を 1 ー 65535 の範囲で入力します。このデバイスと同じルーティングドメイン内で動作する必要があるネットワーク内の他のルータで使用されている自律システム番号を使用してください。

ステップ 7 EIGRP 自律システム内でルーティングする必要があるネットワークとインターフェイスを設定します。

a) オブジェクト本文の上にある [無効を表示（Show Disabled）] リンクをクリックして、その他のすべての設定行を追加します。

b) **network** *network-object* 行の左横にある [+] をクリックします。

c) **network** コマンドで、変数をクリックし、この自律システムに含めるネットワークを定義するオブジェクトを選択します。

通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

直接接続されているネットワークと静的ネットワークが定義されたネットワークに含まれていれば、プロセスによってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

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、EIGRP パッシブ ルーティング インターフェイスの設定（494 ページ）を参照してください。

d) ルーティングする追加のネットワークがある場合は、**[...] > [複製（Duplicate）]**（**network** コマンドの左横）をクリックして新しいネットワークを追加します。ルーティングするすべてのネットワークを設定するまで、**network** 行の追加を継続します。

ステップ 8 （オプション）必要に応じて、最初に無効にした他のコマンドの設定を調整します。EIGRP プロセスのカスタマイズ （491 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。

スタブルーティングのための EIGRP プロセスの設定

EIGRP スタブルータになるようにデバイスを設定できます。スタブルーティングを使用すると、システムのメモリおよび処理要件を減らすことができます。スタブルータとして設定すると、システムはローカル以外のトラフィックをすべて配布ルータに転送するため、完全な EIGRP ルーティングテーブルを維持する必要はありません。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システムは、サマリー、接続されているルート、再配布された静的ルート、外部ルート、および内部ルートに対するクエリすべてに、応答として「inaccessible」というメッセージを返します。システムは、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。

始める前に

ネットワークで EIGRP に使用している自律システム番号を確認します。

EIGRP 自律システム内でルーティングする各ネットワークを定義するネットワークオブジェクトを作成します。たとえば、192.168.1.0/24 ネットワークと 192.168.2.0/24 ネットワークに EIGRP を使用する場合は、各ネットワークに 1 つずつ、2 つのネットワークオブジェクトを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいプロセスを作成するには、[+]をクリックするか、[EIGRPオブジェクトの作成（Create EIGRP Object）] ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

プロセスが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力し、任意で説明を入力します。

ステップ 6 基本的なプロセスのプロパティを設定します。

router eigrp *autonomous-system*

変数をクリックし、番号を 1 ー 65535 の範囲で入力します。このデバイスと同じルーティングドメイン内で動作する必要があるネットワーク内の他のルータで使用されている自律システム番号を使用してください。

ステップ 7 EIGRP 自律システム内でルーティングする必要があるネットワークとインターフェイスを設定します。

a) オブジェクト本文の上にある [無効を表示（Show Disabled）] リンクをクリックして、その他のすべての設定行を追加します。

b) **network** *network-object* 行の左横にある [+] をクリックします。

c) **network** コマンドで、変数をクリックし、この自律システムに含めるネットワークを定義するオブジェクトを選択します。

通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

直接接続されているネットワークと静的ネットワークが定義されたネットワークに含まれていれば、プロセスによってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

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、EIGRPパッシブルーティングインターフェイスの設定（494ページ）を参照してください。

d) ルーティングする追加のネットワークがある場合は、**[...]** > **[複製（Duplicate）]**（**network** コマンドの左横）をクリックして新しいネットワークを追加します。ルーティングするすべてのネットワークを設定するまで、**network** 行の追加を継続します。

ステップ 8 スタブ設定を指定します。

a) **setup eigrp** *configuration* 行の左にある [+] をクリックします。

b) 変数をクリックし、**advanced** を選択します。

c) **setup eigrp stub** *stub-options* コマンドの左側にある [+] をクリックします。

d) デバイスにEIGRPネイバールータからのみ更新を受信させるために、自律システム内の他のルータとルートを共有しないようにデバイスを制限するには、*stub-options* をクリックし、**receive** を選択します。その後、次のコマンドを設定します。

eigrp stub *stub-parameters*

変数をクリックし、**receive-only** を選択します。

e) デバイスが EIGRP ネイバールータにルートをアドバタイズできるようにするには、*stub-options* をクリックし、**other** を選択します。次に、次のコマンドを設定して、アドバタイズする必要があるルートのタイプを選択します。

eigrp stub *connected-parameter redistributed-parameter static-parameter summary-parameter*

変数をクリックして選択します。少なくとも 1 つのルートタイプを選択する必要がありますが、すべてまたは任意の組み合わせを選択できます。

- *connected-parameter*：接続ルートをアドバタイズするには、**connected** を選択します。接続ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスでの接続ルートの再配布の設定が必要となることがあります。
- *redistributed-parameter*：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再配布されるルートをアドバタイズするには、**redistributed** を選択します。
- *static-parameter*：静的ルートをアドバタイズするには、**static** を選択します。また、**configure redistribution** コマンドを有効にして、静的ルートの再配布を設定する必要もあります。
- *summary-parameter*：サマリールートをアドバタイズするには、**summary** を選択します。

ステップ 9 （オプション）必要に応じて、最初に無効にした他のコマンドの設定を調整します。EIGRPプロセスのカスタマイズ（491 ページ）を参照してください。

ステップ 10 [OK] をクリックします。

EIGRP プロセスのカスタマイズ

EIGRP には、デフォルト値を持つ多数のオプションが含まれています。これらの値は、多くのネットワークで適切に機能します。ただし、必要とする動作を正確に得るために、設定を 1 つ以上調整する必要がある場合があります。以下のトピックでは、EIGRP ルーティングプロセスをカスタマイズするさまざまな方法について説明します。

EIGRP の詳細設定の設定

EIGRP プロセスの全体的な動作を制御する複数の設定を指定することができます。これには、自動ルート集約、ディスタンスメトリック、ロギング、リンク ステート アドバタイズメントやその他のルーティング更新の送信に使用されるルータ ID などがあります。これらの設定の多くには、ほとんどのネットワークに適しているデフォルト設定があります。

始める前に

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

このプロセスを作成すると、特定の詳細オプションがデフォルトで有効になります。EIGRP オブジェクトを編集する際に、これらの有効なオプションが表示されます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（  ）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（  ）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 オブジェクト本文の上にある [無効を表示（Show Disabled）] をクリックして、その他のすべての設定行を追加します。

ステップ 6 **setup eigrp** *configuration* 行は、**setup eigrp advanced** のように、すでに有効になっているはずです。有効になっていない場合は、行の左横にある [+] をクリックして有効にしてから、変数をクリックし、**advanced** を選択します。

ステップ 7 （任意。推奨されません）ネットワーク番号境界上のルートを自動的に集約するには、**auto-summary** コマンドの横にある [+] をクリックします。

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 172.16.1.0、172.16.2.0、172.16.3.0 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 172.16.0.0 を作成します。さらにネットワーク 172.16.10.0 と 172.16.11.0 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 172.16.0.0 として集約されます。そのため、ルートを自動的に集約すると、トラフィックが誤ったルータにルーティングされます。

ステップ 8 （任意。推奨）ルータ ID を設定します。

[+] をクリックして **router-id** コマンドを有効にし、変数をクリックして、このデバイスからルータアップデートを送信するときに使用する IPv4 アドレスを入力します。EIGRP 自律システム内の 2 台のルータが同じルータ ID を持つことはできないため、ID がシステム内で一意であることを確認してください。

プロセスに対してルータ ID を明示的に指定しない場合、システムはアクティブインターフェイスに割り当てられている最も大きいIPアドレスを使用します。そのため、選択したインターフェイスを無効にするか、アドレスを変更すると、ルータ ID が変更される場合があります。ルータ ID を明示的に割り当てることにより、プロセスの一貫性を確保することができます。

ステップ 9 （オプション）内部および外部 EIGRP 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。

プロセスを設定すると、次のコマンドがデフォルトで有効になります。新しいオブジェクトを設定する際は、[+] をクリックしてコマンドを有効にする必要がある場合があります。

distance eigrp 90 170

各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいた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つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。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、システムが最適なパスの選択に使用するルートパラメータです。

EIGRP のアドミニストレーティブ ディスタンスの範囲は 1 ー 255 です。これらの数値は、システムが最適なルートを選択したときに他のルーティングプロセスに割り当てられる管理値との相対的な値です。通常は、値が大きいほど、信頼性の格付けが下がります。デフォルト値は、ほとんどのネットワークで機能します。EIGRP ルートを優先させるか、EIGRP ルートが使用される可能性を低減させる場合は、それらを調整します。

数値は、次を意味します。

- 最初の値（90）：**内部距離**。EIGRP 内部ルートのアドミニストレーティブディスタンス。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。
- 2 番目の値（170）：**外部距離**。EIGRP 外部ルートのアドミニストレーティブ ディスタンス。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです

ステップ 10 **default-metric** コマンドは、他のルーティングプロセスからルートを再配布するときに使用されます。これは、再配布も設定する場合にのみ設定します。詳細は、EIGRP のルート再配布の設定 （500 ページ）を参照してください。

ステップ 11 ネイバーロギングを設定します。

プロセスを設定すると、次のコマンドがデフォルトで有効になります。新しいオブジェクトを設定する際は、[+] をクリックしてコマンドを有効にする必要がある場合があります。ロギングを無効にする場合は、[-] をクリックしてコマンドを無効にします。

- **eigrp log-neighbor-changes** EIGRP ネイバーとの隣接関係に関する変更のロギングを有効にします。
- **eigrp log-neighbor-warnings 10** EIGRP ネイバーの警告メッセージのロギングを有効にします。この数値は、ネイバー警告メッセージの反復間隔（1 ー 65535 秒）です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

ステップ 12 **setup stub** コマンドを設定する場合は、スタブルーティングのための EIGRP プロセスの設定（488 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。

EIGRP がアドバタイズするネットワークの設定

network コマンドを使用してネットワークを特定します。これにより、EIGRP ルーティングに含まれるインターフェイスが特定されます。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。

始める前に

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

アドバタイズするネットワークを定義するネットワークオブジェクトを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（  ）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（  ）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 オブジェクト本文の上にある [無効を表示（Show Disabled）] をクリックして、その他のすべての設定行を追加します。

ステップ 6 ネットワークをすでに設定している場合は、**[...]**>**[複製（Duplicate）]**（**network** 行の横）をクリックし、新しい空のコマンドを作成します。

まだネットワークを定義していない場合は、空の **network** *network-object* 行の横にある [+] をクリックします。

ステップ 7 **network** コマンドで、変数をクリックし、この自律システムに含めるネットワークを定義するオブジェクトを選択します。

通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

直接接続されているネットワークと静的ネットワークが定義されたネットワークに含まれていれば、プロセスによってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

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、EIGRP パッシブ ルーティング インターフェイスの設定 （494 ページ）を参照してください。

ステップ 8 ルーティングする追加のネットワークがある場合は、**[...]**>**[複製（Duplicate）]**（**network** コマンドの左横）をクリックして新しいネットワークを追加します。ルーティングするすべてのネットワークを設定するまで、**network** 行の追加を継続します。

ステップ 9 [OK] をクリックします。

EIGRP パッシブ ルーティング 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 **network** コマンドを設定し、**passive-interface** コマンドを使用して、そのインターフェイスが EIGRP 更新を送受信しないようにします。

デフォルトでは、システムは **no passive-interface default** コマンドを有効にします。これにより、すべてのインターフェイスがアクティブに設定され、EIGRP 更新が送受信されます。

次の手順では、インターフェイスをパッシブに変更する方法について説明します。

始める前に

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

プロセスを作成する際、**network** コマンドを追加して、EIGRP を使用してルーティングする必要があるネットワークを示します。ルーティングする追加のネットワークを設定するには、EIGRP がアドバタイズするネットワークの設定 （493 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（  ）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（  ）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 オブジェクト本文の上にある [無効を表示（Show Disabled）] をクリックして、その他のすべての設定行を追加します。

ステップ 6 オブジェクトを編集している場合、**configure interface passive** コマンドとその子である **no passive-interface default** が有効になります。

新しいオブジェクトの場合は、[+] をクリックして **configure routing-interface** *parameters* コマンドを有効にします。

ステップ 7 インターフェイスをデフォルトでアクティブになるように設定し、インターフェイスを選択的にパッシブにするには、次の手順に従います。

a) **configure routing-interface** コマンドで、変数をクリックし、**passive** を選択します。

このアクションにより **no passive-interface default** コマンドが有効になります。これにより、EIGRP インターフェイスがデフォルトでアクティブになります。

b) **passive-interface** *interface* コマンドの横にある [+] をクリックし、変数をクリックして、パッシブにして EIGRP ルーティング更新に参加させないインターフェイスを選択します。

c) **[...] > [複製（Duplicate）]**（**passive-interface** *interface* コマンドの横）をクリックします（追加のパッシブインターフェイスを設定する必要がある場合）。パッシブにする必要があるすべてのインターフェイスで **passive-interface** コマンドが有効になるまで続行します。

ステップ 8 インターフェイスをデフォルトでパッシブになるように設定し、インターフェイスを選択的にアクティブにするには、次の手順に従います。

a) **configure routing-interface** コマンドで、変数をクリックし、**active** を選択します。

このアクションにより **passive-interface default** コマンドが有効になります。これにより、EIGRP インターフェイスがデフォルトでパッシブになります。

b) **no passive-interface** *interface* コマンドの横にある [+] をクリックし、変数をクリックして、EIGRP ルーティング更新にアクティブに参加させるインターフェイスを選択します。

c) **[...] > [複製（Duplicate）]**（**no passive-interface** *interface* コマンドの横）をクリックします（追加のアクティブインターフェイスを設定する必要がある場合）。アクティブにする必要があるすべてのインターフェイスで **no passive-interface** コマンドが有効になるまで続行します。

ステップ 9 インターフェイスをデフォルトの動作（パッシブまたはアクティブ）に戻すには、特定のインターフェイスをパッシブまたはアクティブにするコマンドの横にある [-] をクリックします。これにより、例外アクションが削除され、設定されたデフォルトのアクションに従ってインターフェイスが動作するようになります。

ステップ 10 [OK] をクリックします。

静的 EIGRP ネイバーの設定

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 ネイバーが非ブロードキャスト ネットワーク（VPN トンネルなど）を超えた場所にある場合は、そのネイバーを手動で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。

通常のブロードキャスト ネットワークのルータは隣接関係を形成できるため、それらのネットワーク上にあるスタティック ネイバーを定義する必要はありません。

始める前に

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

システムがネイバーに到達するために使用するインターフェイスを決定します。

ネイバーのロギング設定を指定することもできます（EIGRP の詳細設定の設定 （491 ページ）を参照）。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（  ）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（  ）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **neighbor** コマンドを有効にします。

ステップ 6 ネイバーアドレスを設定します。

neighbor *ip-address* **interface** *interface*

- [ip-address] をクリックし、ネイバールータの IP アドレスを入力します。
- [interface] をクリックして、システムがルータに到達するために使用するインターフェイスを選択します。

ステップ 7 必要に応じて、ネイバールータのスタティックルートを設定します。

ルータの IP アドレスが、選択したインターフェイスと同じネットワーク上にある場合、スタティックルートは必要ありません。たとえば、IP アドレスが 10.100.10.1/24 であるインターフェイスを選択し、ネイバーアドレスが 10.100.10.2/24 の場合、スタティックルートは必要ありません。

ステップ 8 **[...]** > **[重複（Duplicate）]**（**neighbor** コマンドの横）をクリックして、別のスタティックネイバーを定義できます。必要な数だけ定義します。

ステップ 9 [OK] をクリックします。

EIGRP のデフォルトルート候補配信の制御

EIGRP プロセスからのデフォルトルート候補の送受信を制御できます。デフォルトでは、ルートフィルタリングおよび再配布設定に応じて、すべてのルート候補がアドバタイズされるか受け入れられます。

デフォルトルートの送受信を直接オフにすることはできません。EIGRP からのデフォルトルートの配信を防止する場合は、any-ipv4 ネットワークを拒否する標準 ACL を使用して、これらのコマンドを設定します。

始める前に

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

各フィルタルールに必要なスマート CLI 標準アクセスリストオブジェクトを作成します。拒否アクセス制御エントリ（ACE）を使用してエントリに一致するルートを除外し、更新する必要があるルートの ACE を許可します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 オブジェクト本文の上にある [無効を表示（Show Disabled）] をクリックして、その他のすべての設定行を追加します。

ステップ 6 [+] をクリックして次のコマンドのいずれかまたは両方を有効にします。

- **default-information in** *acl*：デフォルトルート候補の受信を制御する場合。
- **default-information out** *acl*：デフォルトルート候補の送信を制御する場合。

ステップ 7 変数をクリックし、フィルタを適用する標準 ACL を選択します。

ステップ 8 [OK] をクリックします。

EIGRP のフィルタルールの設定

標準アクセス制御リストで定義されているネットワークプレフィックスに基づいて、着信ルーティング更新または発信ルーティング更新をフィルタ処理できます。このフィルタ処理により、EIGRP 自律システムへのルート配布や他のルーティングプロセスへのアウトバウンドの制御が向上します。

始める前に

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

各フィルタルールに必要なスマート CLI 標準アクセスリストオブジェクトを作成します。拒否アクセス制御エントリ（ACE）を使用してエントリに一致するルートを除外し、更新する必要があるルートの ACE を許可します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 [無効を表示（Show Disabled）] をクリックしてすべてのコマンドを表示し、[+] をクリックして **configure filter-rules** *direction* コマンドを有効にします。

ステップ 6 [direction] をクリックし、**in**（インバウンドアップデートをフィルタ処理する場合）または **out**（アウトバウンドアップデートをフィルタ処理する場合）を選択します。

このアクションにより、**distribute-list** コマンドがオブジェクトに追加されます。

ステップ 7 インバウンドフィルタの場合は、必要に応じて、アップデートをフィルタ処理するインターフェイスを指定できます。インターフェイスを指定しない場合、フィルタは任意のインターフェイスで受信されるすべてのアップデートに適用されます。[+] をクリックして次のいずれかのオプションを有効にします。

- **distribute-list** *acl-name* **in**

  標準 ACL オブジェクトを選択します。

- **distribute-list** *acl-name* **in interface** *interface*

  標準ACLオブジェクトと、着信更新をフィルタ処理するインターフェイスを選択します。

ステップ 8 アウトバウンドフィルタの場合は、必要に応じて、プロトコルを指定して、そのルーティングプロセスによって生成されたルートと、更新をフィルタ処理するインターフェイスにフィルタを制限できます。[+] をクリックして次のいずれかのオプションを有効にします。

- **distribute-list** *acl-name* **out**

  標準 ACL オブジェクトを選択します。

- **distribute-list** *acl-name* **out interface** *interface*

  標準ACLオブジェクトと、発信更新をフィルタ処理するインターフェイスを選択します。

- **distribute-list** *acl-name* **out** *protocol*

  標準 ACL オブジェクトと次のいずれかのルートタイプを選択します。

  - **connected**を使用して無効にすることができます。システムのインターフェイスに直接接続されているネットワークに対して確立されたルート用です。
  - **static**を使用して無効にすることができます。手動で作成したスタティックルート用です。
  - **rip**を使用して無効にすることができます。RIP によって生成されたルート用です。

- **distribute-list** *acl-name* **out** *protocol identifier*

  標準 ACL オブジェクトと次のいずれかのルートタイプを選択します。

  - **ospf** *process-id*：OSPF によって生成されたルート用です。[identifier] をクリックし、システムで定義されている OSPF プロセスのプロセス ID を入力します。
  - **bgp** *automonous-system*：BGP によって生成されたルート用です。[identifier] をクリックし、システムで定義されている BGP プロセスの自律システム番号を入力します。

ステップ 9 **[...] > [重複（Duplicate）]**（**configure filter-rules** コマンドの横）をクリックして、別のフィルタルールを定義します。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

EIGRP のルート再配布の設定

他のルーティングプロトコル、接続されたルート、およびスタティックルートからの EIGRP プロセスへのルートの再配布を制御できます。

始める前に

EIGRP への再配布を設定する前に、ルートを再配布するルーティングプロセスを設定し、変更を展開することがベストプラクティスです。

ルートマップを適用して、再配布されるルートを微調整する場合は、Smart CLI ルートマップオブジェクトを作成します。ルートマップに一致するルートが再配布され、一致しないルートはすべて再配布されません。

この手順は、EIGRP プロセスがすでに設定されていることを前提としています（コア EIGRP プロセスの設定 （486 ページ）を参照）。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータが有効になっている場合は、グローバル仮想ルータの表示アイコン（  ）をクリックします。

ステップ 3 [EIGRP] タブをクリックします。

ステップ 4 EIGRP オブジェクトの編集アイコン（  ）をクリックします。

オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 [無効を表示（Show Disabled）] をクリックして、すべてのコマンドを表示します。

ステップ 6 （オプション）[+] をクリックして、**default-metric** コマンドを有効にします。このコマンドは、**setup eigrp advanced** コマンドグループに含まれています。

default-metric コマンドは、ルートタイプに関して特定の **redistribute metric** コマンドを設定しない場合に、再配布されたルートに使用するメトリックを設定します。

default-metric *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

変数をクリックして、次のように設定します。すべてのメトリック変数を設定する必要があります。

- *bandwidth-metric*：変数をクリックし、このルートの接続の帯域幅を 1 ー 4294967295 キロバイト/秒の範囲で入力します。
- *delay-metric*：変数をクリックし、ルート上の接続の遅延（10 マイクロ秒単位）を 0 ー 4294967295 の範囲で入力します。
- *reliability-metric*：変数をクリックし、ルートの EIGRP 信頼性メトリックを 0 ー 255 の範囲で入力します。255 は 100% の信頼性を示します。このメトリックは無視されますが、依然として設定する必要があります。
- *effective-bandwidth*：変数をクリックし、ルートの EIGRP 有効帯域幅を 1 ー 255 の範囲で入力します。255 は 100% の負荷を示します。このメトリックは無視されますが、依然として設定する必要があります。
- *path-MTU*：変数をクリックして、パスの平均伝送単位（MTU）を 1 ー 65535 の範囲で入力します。このメトリックは無視されますが、依然として設定する必要があります。

ステップ 7 + をクリックして、**configure redistribution** コマンドを有効にします。

ステップ 8 [protocol] 変数をクリックし、ルートの再配布元となる送信元プロセスを選択します。**connected** および **static** のルート、あるいは **bgp**、**isis**、**ospf**、または **rip** によって生成されたルートを再配布できます。

ステップ 9 ルーティングプロセスを選択した場合は、[identifier] 変数をクリックして、必要な値を入力します。

- **bgp**を使用して無効にすることができます。自律システムの番号を入力します。
- **ospf**を使用して無効にすることができます。プロセス ID 番号を入力します。
- **connected**、**static**、**isis**、**rip**。**none** を入力します。別の値を入力しても、無視されます。

ステップ 10 （任意：IS のみ）**redistribute isis route-level** *route-level* コマンドで、変数をクリックし、IS-IS エリア（**level-1**）内でのみ学習したルートを再配布するか、IS-IS エリア（**level-2**）間、または両方（**level-1-2**）で再配布するかを選択します。

ステップ 11 （任意：すべてのプロトコル）ルートマップに基づいて再配布されるルートを微調整するには、[+] をクリックして **redistribute** *route-map* コマンドを有効にし、変数をクリックして、制限を定義するルートマップを選択します。

ルートマップを適用しない場合は、（再配布用に設定された他のコマンドに適合する）プロセスのすべてのルートが再配布されます。

ステップ 12 （任意：すべてのプロトコル）再配布されたルートのメトリックを微調整するには、[+] をクリックして次のコマンドを有効にし、オプションを設定します。

redistribute *protocol* **metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

変数をクリックし、上記の **default-metric** コマンドで説明されている値を設定します。すべてのメトリック変数を設定する必要があります。

ステップ 13 （任意：OSPF のみ）OSPF プロセスからルートを再配布する場合、次のコマンドはデフォルトで有効になっています。[-] をクリックして、不要なコマンドを無効化できます。

これらのコマンドで、OSPF ルートを他のルーティングドメインに再配布する条件を指定します。

- **redistribute ospf match external 1**を使用して無効にすることができます。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。
- **redistribute ospf match external 2**を使用して無効にすることができます。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。
- **redistribute ospf match internal**を使用して無効にすることができます。特定の自律システムの内部ルート。
- **redistribute ospf match nssa-external 1**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。
- **redistribute ospf match nssa-external 2**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。

ステップ 14 **[...] > [重複（Duplicate）]**（**configure redistribution** コマンドの横）をクリックして、別のプロトコルの再配布を設定できます。ネットワークに適したプロトコルごとの再配布を設定します。

ステップ 15 [OK] をクリックします。

EIGRP のモニタリング

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。

- **show eigrp events** ［{*start end*} | **type**］

  EIGRP イベント ログを表示します。

- **show eigrp interfaces** ［*if-name*］［**detail**］

  EIGRP ルーティングに参加するインターフェイスを表示します。

- **show eigrp neighbors** ［**detail** | **static**］［*if-name*］

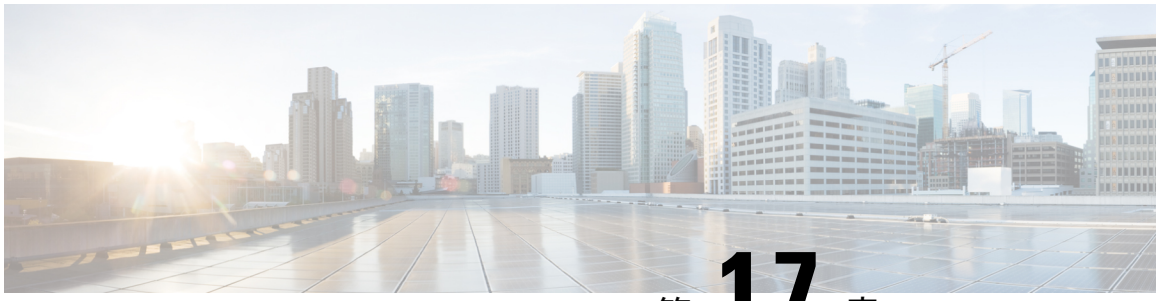
  EIGRP ネイバー テーブルを表示します。

- **show eigrp topology** ［*ip-addr* ［*mask*］ | **active** | **all-links** | **pending** | **summary** | **zero-successors**］

  EIGRP トポロジ テーブルを表示します。

- **show eigrp traffic**

  EIGRP トラフィックの統計情報を表示します。



第 17 章

ボーダーゲートウェイ プロトコル（BGP）

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。システムがサービス プロバイダー ネットワークへのゲートウェイである場合は、BGP の実装が必要になることがあります。1 つの自律システムに対して、デバイスに 1 つの BGP プロセスを設定できます。

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 プロバイダー（ISP）間で使用されるプロトコルです。

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 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。

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。

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 （508 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 の設定

ここでは、BGP の設定方法について説明します。

BGP のグローバル設定

仮想ルータを使用する場合、BGPを設定するとグローバル設定がすべての仮想ルータに適用されます。BGP プロセスを定義するために設定する追加の BGP 設定があります。仮想ルータを使用する場合は、仮想ルータごとに個別の BGP プロセスを作成できます。

始める前に

BGPグローバル設定オブジェクトを作成した後で、不要になった場合は削除できます。この手順に従ってオブジェクトを編集するだけですが、ダイアログボックスの下部にある [BGPグローバル設定オブジェクトの削除（Delete BGP Global Settings Object）] ボタンをクリックします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 メインのルーティングまたは仮想ルータのページで、[BGPグローバル設定（BGP Global Settings）] ボタンをクリックします。

仮想ルータを表示している場合は、仮想ルータのメインリストに戻る必要があります。

ステップ 3 BGP グローバル設定オブジェクトを設定していない場合は、[BGPグローバル設定オブジェクトの作成（Create BGP Global Settings Object）] をクリックします。

ステップ 4 （オプション）オブジェクト名の変更や、オブジェクトの説明の入力が可能です。デフォルトのオブジェクト名は BgpGeneralSettings です。

ステップ 5 少なくとも次の基本設定を行います。

- **router bgp** *as-number*。*as-number* をクリックして、BGP プロセスの自律システム（AS）番号を入力します。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。システムは、RFC 5396 で定義されている asplain および asdot 表記をサポートしています。

- **log-neighbor-changes** *state*。*state* をクリックして、enable または disable を選択します。enableにした場合（推奨）、BGPネイバーの変化（アップまたはダウン）とリセットがログに記録されます。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。
- **transport path-mtu-discovery** *state*。*state* をクリックして、enable または disable を選択します。enableにした場合（推奨）、システムは2つのIPホスト間のネットワークパスの最大伝送ユニット（MTU）サイズを確認し、最大MTUパスを利用します。これにより、IPフラグメンテーションが回避されます。
- **fast-external-fallover** *state*。*state* をクリックして、enable または disable を選択します。enable にした場合（推奨）、システムは BGP ピアリングセッションに対して、直接接続されている外部ピアとの高速外部フォールオーバーを使用します。リンクがダウンすると、セッションは即座にリセットされます。BGP高速外部フォールオーバーをディセーブルにした場合、BGPルーティングプロセスはデフォルトのホールドタイマーの期限（3回のキープアライブ）が切れるまで待ってからピアリングセッションをリセットします。
- **enforce-first-as** *state*。*state* をクリックして、enable または disable を選択します。enable にした場合（推奨）、システムは eBGP ピアから受信した、AS_PATH 属性内の最初のセグメントとしてそのピアの自律システム番号が示されていない着信アップデートを拒否します。このコマンドをイネーブルにすると、間違った設定のピアや権限のないピアが、別の自律システムからのルートであるかのようにルートをアドバタイズすることによってトラフィックを誤った宛先に送信する（ローカルルータをスプーフィングする）ことを回避できます。

ステップ 6 （オプション）オブジェクト本文の上にある [無効を表示（Show Disabled）] リンクをクリックして、その他のすべての設定行を追加します。

オプションの左側にある [+] をクリックすると、次のオプションを有効にすることができます。

- **bgp asnotation dot**を使用して無効にすることができます。デフォルトの表示を変更し、BGP 4 バイト自律システム番号の正規表現一致形式を、asplain（10 進数の値）から asdot（ドット付き表記）にします。システムでは自律システム番号のデフォルト表示形式として asplain が使用されますが、このコマンドをイネーブルにしていなくても、4バイト自律システム番号を asplain と asdot の両方の形式で設定できます。

  また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、このコマンドをイネーブルにしない場合は、4 バイト自律システム番号とマッチングする正規表現はすべて asplain 形式で記述する必要があります。
- **bgp scan time 60**を使用して無効にすることができます。数値をクリックし、ネクストホップを検証するための BGP ルータのスキャン間隔を入力します（5 ～ 60 秒）。デフォルトは 60 秒です。
- **configure nexthop trigger** *state*。*state* をクリックして、**enable** または **disable** を選択します。BGPネクストホップアドレストラッキングはイベントドリブンです。BGPプレフィックスは、ピアリングセッションの確立時に自動的にトラッキングされます。ネクストホップの変更は、ルーティング情報ベース（RIB）で更新されると BGP に迅速に報告されます。この最適化によって、RIBにインストールされているルートのネクストホップの変更

に対する応答時間が短縮されることで、全体的なBGPコンバージェンスが改善されます。BGP スキャナ サイクル間に最適パス計算が実行されると、変更内容だけが処理および追跡されます。ネクストホップ アドレス トラッキングをイネーブルにすると、次のコマンドが追加されます。新しいオブジェクトで全般オプションを設定しない場合、デフォルトではこの機能が有効になることに注意してください。

- **bgp nexthop trigger enable**を使用して無効にすることができます。BGP ネクストホップ アドレス トラッキングによって、BGP 応答時間を大幅に短縮できます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGPが不安定になることがあります。BGPへの影響の可能性を軽減するために、不安定なIGPピアリング セッションを積極的にダンプニングさせることを推奨します。
- **bgp nexthop trigger delay 5**を使用して無効にすることができます。数値をクリックして、BGPネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を設定します。すべてのルーティング テーブル ウォーク間の遅延間隔を調整して IGP の調整パラメータと一致させることで、BGP ネクストホップ アドレス トラッキングのパフォーマンスを向上させることができます。デフォルトの遅延間隔は5秒であり、高速で調整されるIGPの場合はこれが最適な値です。よりゆっくり収束する IGP の場合は、IGP コンバージェンス時間に応じて遅延間隔を 20 秒以上に変更できます。遅延は 0 ～ 100 秒の間で設定できます。

- **bgp aggregate-timer 30**を使用して無効にすることができます。数値をクリックして、BGPルートが集約される間隔を設定します（6 ～ 60 秒）。デフォルトは 30 秒です。
- **bgp router-id** *router-id*。*router-id* をクリックして、グローバルルータ ID として使用するIPv4アドレスを入力します。このIDは、ルータ IDを指定していない仮想ルータ内のすべての BGP プロセスに使用されます。このコマンドをイネーブルにしていない場合、ルータ ID は仮想ルータに割り当てられている物理インターフェイスの最上位の IP アドレスに設定されます。このコマンドを使用すると、ルータ ID が安定したまま維持されます。
- **bgp maxas-limit** *value*。*value* をクリックして、BGP アップデートメッセージ内の AS-path 属性に含まれる自律システム番号の最大数（1～254）を入力します。AS-path 属性は、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。システムは、指定された値を超える多数の自律システムを AS-path 内に持つルートを廃棄します。このコマンドは、AS パス セグメント内の自律システム番号の数に制限を設定するだけでなく、AS パス セグメントの数を 10 に制限します。このコマンドをイネーブルにしない場合、ルートは廃棄されません。

ステップ 7 （オプション）BGP の詳細オプションを設定します。

必要に応じて [無効を表示（Show Disabled）] リンクをクリックして、次のコマンドを表示します。設定を編集すると、**timers**および**bestpath**の両方のオプションセットが表示されます。これは、明示的に設定していない場合でも有効になっているデフォルトがいくつかあるためです。

configure bgp advanced *advanced-option*

advanced-option をクリックして、次のいずれかを選択します。左の列の [...] をクリックして [複製（Duplicate）] を選択すると、これらのオプションをすべて設定できます。

- **timers**を使用して無効にすることができます。BGP ネイバールータとの通信時に使用されるタイマーを設定します。

  timers bgp 60 180 0

  - 最初の値（デフォルトは 60）：キープアライブ間隔。数値をクリックして、システムがキープアライブメッセージを BGP ネイバーに送信する頻度を入力します（0 ～ 65535 秒）。20 以下を指定しないことをお勧めします。20 以下を指定すると、ルートが不必要にフラッピングする可能性があります。
  - 2 番目の値（デフォルトは 180）：ホールド時間。数値をクリックして、キープアライブメッセージを受信しなくなってから BGP ネイバーの dead を宣言するまでシステムが待機する時間を入力します（0 ～ 65535 秒）。
  - 3 番目の値（デフォルトは 0）：最小ホールド時間。数値をクリックして、BGP ネイバーで設定される最小許容ホールド時間を指定します。最小許容ホールド時間は、このシステムのホールド時間として指定した間隔以下にする必要があります。範囲は 0 ～ 65535 秒です。

- **bestpath**を使用して無効にすることができます。BGP ベストパス選択アルゴリズムで使用されるオプションを設定します。**bgp default local-preference** コマンドがデフォルトで設定されていますが、コマンドの [+] をクリックして他のコマンドを追加することもできます。
  - **bgp default local-preference 100**を使用して無効にすることができます。数値をクリックして、BGP AS 内の他のルータに対するこのシステムの優先順位を示す値を入力します（0 ～ 4294967295）。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。この属性は iBGP ピア間だけで交換され、ローカルポリシーを決定するために使用されます。
  - **bgp always-compare-med**を使用して無効にすることができます。異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）の比較を許可します。デフォルトでは、異なる自律システム内のネイバーからのパスに対して、MED を比較しません。
  - **bgp bestpath compare-routerid**を使用して無効にすることができます。2 つの異なるピア（ルータ ID を除くすべての属性が同じ）から 2 つの同一のルートが受信されたときに、最適パス選択のタイブレーカーとしてルータ ID を使用します。このコマンドがイネーブルになっている場合、その他の属性がすべてが等しければ、最も小さいルータ ID が最適パスとして選択されます。それ以外の場合は、最初に受信したルートが使用されます。
  - **bgp deterministic-med**を使用して無効にすることができます。隣接 AS からアドバタイズされた最適な MED パスを選択します。
  - **bgp bestpath med missing-as-worst**を使用して無効にすることができます。MED 属性が欠落しているパスを最も優先度の低いパスとして設定します。デフォルトでは、MED が欠落しているルートが最適ルートと見なされます。

- **graceful-restart**を使用して無効にすることができます。高可用性またはクラスタ構成のシステムのグレースフルリスタートを設定します。
  - **bgp graceful-restart**を使用して無効にすることができます。ノンストップ フォワーディングのグレースフルリスタートを有効にします。グレースフル リスタートを使用すると、システムは、再起動中にアドレス グループのフォワーディング ステートを維持する機能をアドバタイズできます。
  - **bgp graceful-restart restart-time 120**を使用して無効にすることができます。数値をクリックして、リスタートイベントが発生した後、グレースフルリスタート対応ネイバーが通常の動作に戻るまでシステムが待機する最大時間を入力します（1 ～ 3600 秒）。デフォルトは 120 秒です。
  - **bgp graceful-restart stalepath-time 360**を使用して無効にすることができます。数値をクリックして、リスタートしているピアの古いパスをシステムが保持する最大時間を入力します（1～3600秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。

ステップ 8 [OK] をクリックします。

BGP プロセスの設定

BGP グローバル設定を構成した後に、BGP プロセスを設定できます。仮想ルータを使用している場合は、仮想ルータごとに個別のプロセスを作成できます。システムまたは仮想ルータごとに、最大でも 1 つの BGP プロセスを設定できます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいプロセスを作成するには、[+] をクリックするか、[BGP オブジェクトの作成（Create BGP Object）]ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

プロセスが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 名前を入力し、オプションでオブジェクトの説明を入力します。

ステップ 6 プロセスの最小限の設定を行います。

- **router bgp** *as-number*。*as-number* をクリックして、グローバル設定で指定した BGP プロセスと同じ自律システム（AS）番号を入力します。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。システムは、RFC 5396 で定義されている asplain および asdot 表記をサポートしています。
- **configure address-family** *ip-protocol*。*Ip protocol* をクリックして、IPv4 または IPv6 を選択します。仮想ルータを使用している場合、IPv6 はグローバルルータにのみ設定できます。IPv4 は、すべての仮想ルータに設定できます。オプションを選択すると、**address-family ipv4 unicast** または **address-family ipv6 unicast** コマンドが追加され、さらに次のコマンドを設定する必要が生じます。
  - **configure address-family {ipv4 | ipv6}** *settings*。settings をクリックして、**general** または **advanced** を選択します。これらのオプションの下で少なくとも 1 つのコマンドを設定する必要がありますが、これだけでは意味のあるプロセスには不十分です。

ステップ 7 [無効を表示（Show Disabled）] をクリックして、ネットワークで正しく機能するようにプロセスをカスタマイズします。

ここまで説明したように、最小限のコマンドセットを設定すれば、オブジェクトを保存して後でプロセス設定をカスタマイズできます。以降のトピックでは、さまざまなオプションのセットについて説明します。少なくとも、ネットワーク設定を完了して、プロセスがルートを配布する先のネットワークを特定する必要があります。全般と詳細の両方の設定には、大部分の状況に適切となるコマンドのデフォルトがあります。

- BGP 一般設定 （515 ページ）
- BGP 詳細設定 （516 ページ）
- BGP がアドバタイズするネットワークの設定 （518 ページ）
- BGP ルートの挿入の設定 （520 ページ）
- BGP 集約アドレス設定 （521 ページ）
- IPv4 用の BGP フィルタ設定の指定 （523 ページ）
- BGP ネイバーの設定 （524 ページ）
- 他のルーティングプロトコルからの BGP ルート再配布の設定 （533 ページ）

ステップ 8 （オプション）プロセスのルータ ID を設定します。

BGP のグローバル設定で、BGP プロセスに使用するルータ ID を設定できます。必要に応じて、プロセスオブジェクトでも設定できます。プロセスオブジェクトで設定されたルータ ID は、グローバルルータ ID をオーバーライドします。これにより、特定の仮想ルータのグローバル値を簡単にオーバーライドすることができます。

次のコマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックし、その横にある [+] をクリックしてコマンドを有効にします。

- **bgp router-id** *router-id*。*router-id* をクリックして、このプロセスのルータ ID として使用する IPv4 アドレスを入力します。このコマンドをイネーブルにしていない場合、ルータ ID はグローバルルータ ID、または仮想ルータに割り当てられている物理インターフェイスの最上位の IP アドレスに設定されます。このコマンドを使用すると、ルータ ID が安定したまま維持されます。

ステップ 9 [OK] をクリックします。

BGP 一般設定

全般設定では、アドミニストレーティブ ディスタンス、タイマー、ネクストホップ アドレス トラッキング（IPv4 のみ）が定義されます。これらのオプションには、ほとんどのネットワークに適したデフォルト設定があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

ステップ 5 **configure address-family ipv4** または **ipv6** 行を見つけます。**general** オプションがすでに選択されている場合は、次の手順に進みます。それでも、次の対応を試してください。

- *settings* 変数がまだ表示されている場合は、 それをクリックして **general** を選択します。
- 高度なオプションをすでに設定している場合は、コマンドの左側にある [...] ボタンをクリックして、[複製（Duplicate）] を選択します。次に、*settings* をクリックして **general** を選択します。

ステップ 6 次のコマンドを設定します。

- **distance bgp 20 200 200**を使用して無効にすることができます。BGP のアドミニストレーティブ ディスタンスを設定します（1 ～ 255）。これらの数値は、システムが最適なルートを選択したときに他のルーティングプロセスに割り当てられる管理値との相対的な値です。通常は、値が大きいほど、信頼性の格付けが下がります。他のプロトコルが外部BGP（eBGP）によって実際に学習されたルートよりも良いルートをノードに提供できることがわかっている場合、または一部の内部ルートが BGP によって優先されるべきである場合、このコマンドを使用します。アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。数値は、次を意味します。

- 最初の値（デフォルトは 20）：外部ディスタンス。数値をクリックして、外部 BGP ルートのアドミニストレーティブディスタンスを入力します。外部自律システムから学習されたルートは、外部ルートです。
- 2 番目の値（デフォルトは 200）：内部ディスタンス。数値をクリックして、内部 BGP ルートのアドミニストレーティブディスタンスを入力します。ローカル自律システムのピアから学習されたルートは、内部ルートです。内部 BGP 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ことは危険と見なされており、推奨されません。不適切な設定により、ルーティングテーブルの不整合性やルーティングの中断が発生する可能性があります。
- 3 番目の値（デフォルトは 200）：ローカルディスタンス。数値をクリックして、ローカル BGP ルートのアドミニストレーティブディスタンスを入力します。ローカルルートは、BGP ルーティングプロセスで **network** コマンドによりリストされるネットワーク（つまりプロセスがアドバタイズしているネットワーク）、または別のプロセスから BGP に再配布されているネットワーク向けのものです。

ステップ 7 [OK] をクリックします。

BGP 詳細設定

詳細設定を使用して、特別な状況下でのみ必要となる各種オプションを設定します。これらのオプションのほとんどは、デフォルトでは無効になっています。

始める前に

table-map コマンドを設定する場合は、初めに **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページに移動して、コマンドで必要となるスマート CLI ルートマップオブジェクトを作成する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

ステップ 5 **configure address-family ipv4** または **ipv6** 行を見つけます。**advanced** オプションがすでに選択されている場合は、次の手順に進みます。それでも、次の対応を試してください。

- *settings* 変数がまだ表示されている場合は、それをクリックして **advanced** を選択します。

- すでに全般オプションを設定している場合は、コマンドの左側にある [...] ボタンをクリックして [複製（Duplicate）] を選択します。次に、*settings* をクリックして **advanced** を選択します。

ステップ 6 次のコマンドを設定します。最初にオブジェクトを作成するときに、最初のコマンド以外のすべてのコマンド表示するには [無効を表示（Show Disabled）] をクリックする必要があります。

コマンドを有効にするには、コマンドの [+] をクリックします。

- **bgp redistribute-internal**を使用して無効にすることができます。EIGRP や OSPF などの内部ゲートウェイプロトコル（IGP）への iBGP の再配布を設定します。iBGP を IGP に再配布する際は、慎重に行ってください。再配布されるプレフィックスの数を制限するために IP prefix-list ステートメントおよび route-map ステートメントを使用します。フィルタリングされていない BGP ルーティング テーブルを IGP に再配布すると、通常の IGP ネットワーク動作に影響を及ぼす可能性があります。このコマンドはデフォルトで有効になっているため、オフにするには [-] ボタンをクリックする必要があります。
- **bgp suppress-inactive**を使用して無効にすることができます。RIB（非アクティブなルート）にインストールされていないルートがピアにアドバタイズされることを防止します。デフォルトの設定では、BGP は非アクティブなルートをアドバタイズします。BGP は、RIB にインストールされていないルートに RIB 失敗フラグを付けることに注意してください。このフラグは、**show bgp** コマンドの出力にも、Rib-Failure (17) のように表示されます。このフラグは、ルートまたは RIB に関するエラーまたは問題を示すものではありません。
- **auto-summary**を使用して無効にすることができます。（IPv4 のみ）サブネットルートをネットワークレベルのルートに自動的に集約します。ルート集約により、ルーティングテーブルにおけるルーティング情報の量が少なくなります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズを無効にします。自動サマライズを無効にすると、サブネットがアドバタイズされます。
- **synchronization**を使用して無効にすることができます。BGP と、OSPF などの内部ゲートウェイプロトコル（IGP）システムの間の同期を有効にします。通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。この機能により、自律システム内のルータおよびアクセス サーバーは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。自律システム内の他のルータが BGP を実行していない場合、このコマンドを使用します。
- **table-map** *route-map options*。（IPv4 のみ）BGP ルーティングテーブル内で更新されたルートのメトリック、タグ値、またはトラフィックインデックスを設定するルートマップを適用するか、ルートが RIB にダウンロードされるかどうかを制御します。*route map* をクリックして、ルートマップを定義するスマート CLI オブジェクトを選択します。ルートマップでは、IP アクセスリスト、自律システムパス、コミュニティ、プレフィックスリスト、およびネクストホップに対して match 句を使用できます。

  options をクリックして、空白または **filter** のいずれかを選択することで、ルートマップの使用方法を決定できます。

- **filter** を選択しない場合、ルートが RIB にインストールされる前に、ルートマップを使用してルートの特定のプロパティが設定されます。ルートは、ルートマップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。
- **filter** を選択すると、ルートマップは BGP ルートが RIB にダウンロードされるかどうかも制御します。ルートマップで許可されているルートのみがダウンロードされます。拒否されたルートはダウンロードされません。

- **default-information originate**を使用して無効にすることができます。デフォルトのルート（ネットワーク 0.0.0.0）をアドバタイズするように BGP を設定します。**default-information originate** コマンドの設定は、**network** コマンドの設定に似ています。ただし、**default-information originate** コマンドではルート 0.0.0.0 を明示的に再配布する必要があり、これもこのオブジェクトで設定する必要があります。**network** コマンドでは、ルート 0.0.0.0 が OSPF などの内部ゲートウェイプロトコル（IGP）のルーティング テーブルに存在することのみが必要です。このため、デフォルトルートを配布する場合に**network** コマンドが優先されます。
- **maximum paths 1**を使用して無効にすることができます。ルーティングテーブルにインストールできる並列 BGP ルートの最大数を制御します（1 ～ 8）。このコマンドは、BGP ピアリングセッションに等コストまたは非等コスト マルチパス ロード シェアリングを設定するために使用されます。ルートを BGP ルーティング テーブル内のマルチパスとして導入する場合、ルートはすでにある他のルートと同じネクストホップを持つことはできません。BGP ルーティング プロセスは、BGP マルチパス ロード シェアリングが設定されている場合、BGP ピアに最適パスをアドバタイズします。等コスト ルートの場合、最下位のルータ ID を持つネイバーからのパスは、ベストパスとしてアドバタイズされます。

  BGP 等コスト マルチパス ロード シェアリングを設定するには、すべてのパス属性を同じにする必要があります。パスの属性には、重み値、ローカルプリファレンス、自律システムパス（長さだけでなく、属性全体）、オリジンコード、MED、および Interior Gateway Protocol（IGP）のディスタンスが含まれます。
- **maximum paths ibgp 1**を使用して無効にすることができます。ルーティングテーブルにインストールできる内部 BGP ルートの最大数を制御します（1 ～ 8）。マルチパス iBGP の考慮事項は、上記の **maximum paths** コマンドで説明されているものと同じです。

ステップ 7 [OK] をクリックします。

BGP がアドバタイズするネットワークの設定

BGP ルーティングプロセスによってアドバタイズ可能なネットワークを定義する必要があります。

始める前に

アドバタイズするネットワークを定義するネットワークオブジェクトを作成します。BGP 用に設定するアドレスファミリに応じて、IPv4 または IPv6 ネットワーク、またはその両方を定義できます。

ネットワークオブジェクトで大規模なネットワークスペースが指定されている場合は、アドバタイズしたくない大きなスペース内のサブネットを除外するために、ネットワークオブジェクトに対して適用するルートマップを作成することもできます。ルートマップの仕様に一致するルートだけがアドバタイズされます。Smart CLI を使用して、ルートマップオブジェクトを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

network コマンドは、**configure address family ipv4** または **ipv6** コマンドの下のコマンドセット内にあります。アドバタイズするネットワークを設定するには、アドレスファミリを設定する必要があります。

各アドレスグループ内の**network** コマンドは、設定するアドレスファミリに一致するアドレスを指定する必要があります。

ステップ 5 [無効を表示（Show Disabled）] をクリックしてすべてのコマンドを表示し、[+] をクリックして **network** または **network route-map** コマンドを有効にします。

- *network-object*：変数をクリックして、アドバタイズするネットワークを定義するネットワークオブジェクト（IPv4 ネットワークアドレスとマスク、または IPv6 ネットワークアドレスとプレフィックス）を選択します。
- **route-map** *map-tag*：変数をクリックし、ネットワークオブジェクトに適用するルートマップを選択して、範囲内のどのアドレスをアドバタイズするかをフィルタリングします。
- （任意、IPv6 のみ）*prefix-name*：変数をクリックし、プレフィックスをアドバタイズする DHCPv6 プレフィックスの名前を入力します。このオプションを設定すると、ネットワークオブジェクトはプレフィックスのサブネットとして機能します。このオプションを使用するには、DHCPv6 プレフィックス委任クライアントをイネーブルにする必要があります。これを行うには、FlexcCnfig を使用して、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client pd** コマンドをインターフェイスに追加する必要があります。

ステップ 6 **[...] > [重複（Duplicate）]**（**network** または **network route-map** コマンドの横）をクリックして、アドバタイズする追加のネットワークを設定します。

ステップ 7 [OK] をクリックします。

BGP ルートの挿入の設定

BGP ルーティングテーブルに固有性の強いルートを注入するよう条件付きルート注入を設定することができます。条件付きルート注入により、一致するものがなくても、より具体的なプレフィックスを BGP ルーティング テーブルにすることができます。注入されたプレフィックスには、有効な親ルートが存在する必要があります。集約ルート（既存プレフィックス）と同じかそれより具体的なプレフィックスのみを注入できます。

始める前に

プレフィックスを定義するために必要なルートマップを作成する必要があります。これらのルートマップは、手順で説明されている要件を満たしている必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

route injection コマンドは、**configure address family ipv4** または **ipv6** コマンドの下のコマンドセット内にあります。アドバタイズするネットワークを設定するには、アドレスファミリを設定する必要があります。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **bgp inject-map** コマンドを有効にします。

ステップ 6 コマンドのプロパティを設定します。

- **inject-map** *inject-map*：変数をクリックし、作成されてルーティングテーブルにインストールされるプレフィックスを定義するルートマップを選択します。注入されたプレフィックスは、ローカル BGP RIB に格納されます。有効な親ルートが存在する必要があります。集約ルート（既存プレフィックス）と同じかそれより具体的なプレフィックスのみを注入できます。ルートマップでは、プレフィックスリストを使用して、注入するルートを指定する必要があります。
- **exist-map** *exist-map*：変数をクリックし、BGP スピーカーが追跡するプレフィックスを定義するルートマップを選択します。このルートマップでは、プレフィックスリストを使用して、集約プレフィックスとルートソースを指定する必要があります。ルートソースは、サブネットではなく、ルータ（10.2.1.1/32 など）になります。

- *options*：必要に応じて、変数をクリックし、**copy-attributes** を選択します。このオプションにより、集約ルートと同じ属性を継承するように、注入されたプレフィックスが設定されます。このキーワードを選択しない場合、注入されたプレフィックスは、ローカルで生成されたルートのデフォルト属性を使用します。

ステップ 7 追加のルート注入ルールを設定するには、**[...]** > **[重複（Duplicate）]**（**bgp inject-map** コマンドの横）をクリックします。

ステップ 8 [OK] をクリックします。

BGP 集約アドレス設定

BGP ネイバーはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約は、複数の異なるルートの属性を合成し、1 つのルートだけがアドバタイズされるようにするプロセスです。集約プレフィックスは、クラスレス ドメイン間ルーティング（CIDR）の原則を使用して、複数の隣接するネットワークを、ルーティング テーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。結果として、アドバタイズの必要なルートは少なくなります。

キーワードを指定せずに集約ルートを設定すると、指定された範囲内にあるより具体的なBGPルートが使用できる場合、BGPルーティングテーブルに集約エントリが作成されます（集約に一致する長いプレフィックスは、ルーティング情報ベース（RIB）に存在する必要があります）。集約ルートは自律システムからのルートとしてアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、アトミック集約属性が設定されますアトミック集約属性は、**as-set** キーワードを指定しない限り設定されます。

次の手順では、特定のルートを 1 つのルートに集約する設定方法について説明します。

始める前に

ルートマップを適用して、集約されるルート、または集約ルートに設定されている属性を微調整するには、Smart CLI ルートマップオブジェクトを作成します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

aggregation コマンドは、**configure address family ipv4** または **ipv6** コマンドの下のコマンドセット内にあります。集約を設定するには、アドレスファミリを設定する必要があります。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **configure aggregate-address** コマンドを有効にします。

ステップ 6 *map-type* 変数をクリックし、この特定の集約ルートに適用するルートマップのタイプを選択します。

このオプションでは、オブジェクトに追加される **aggregate-address** コマンドに含めるパラメータを決めます。最大 3 つの独立したルートマップを適用して、集約からのルートを抑制し、ルートをアドバタイズし、集約ルートに適用する属性を定義できます。

- ルートマップを適用する必要がない場合は、**no-map** を選択します。
- 3 つのオプションすべてにルートマップを適用する場合は、**all** を選択します。
- すべてではなく、1 つまたは 2 つのマップを適用する場合は、適切なキーワードの組み合わせを選択します。**suppress-map**、**advertise-map**、**attribute-map**、**suppress-advertise**、**suppress-attribute**、**advertise-attribute**。

ステップ 7 集約するルートのプロパティを設定します。

次に、プロパティの完全なリストを示します。表示される内容は、選択するマップタイプによって異なります。

- *network-object*：変数をクリックし、集約するアドレス空間を定義するネットワークオブジェクトを選択します。オブジェクトでは、設定しているアドレスタイプに一致する IPv4 または IPv6 アドレッシングを使用する必要があります。たとえば、すべての 10.0.0.0/8 サブネットのルートを集約できます。
- **suppress-map** *suppress-route-map*：変数をクリックし、ルートマップを選択して、指定されたルートのアドバタイズメントを抑制します。ルートマップの match 句を使用して、集約のより具体的な一部のルートを選択的に抑制し、他のルートは抑制しないようにできます。ルートマップは、アクセスリストと自律システムパスに基づいてルートを照合できます。
- **advertise-map** *advertise-route-map*：変数をクリックし、集約ルートの異なるコンポーネント（AS_SET やコミュニティなど）を構築するために使用される特定のルートを選択するルートマップを選択します。これは、集約のコンポーネントが別々の自律システムにあり、AS_SET で集約を作成して同じ自律システムの一部にアドバタイズする場合に役立ちます。AS_SET から特定の自律システム番号を省略し、集約が受信ルータの BGP ループ検出メカニズムによってドロップされるのを防ぐことを忘れてはなりません。ルートマップは、アクセスリストと自律システムパスに基づいてルートを照合できます。
- **attribute-map** *attribute-route-map*：変数をクリックし、集約ルートの属性を変更するルートマップを選択します。これは、AS_SET を構成するルートの 1 つが community no-export 属性（集約ルートがエクスポートされるのを防ぐ）などの属性で設定されている場合に役立ちます。
- *options*：変数をクリックし、次のオプションのいずれか、またはすべてを選択するか、いずれも選択しません。

- **as-set**を使用して無効にすることができます。集約ルートの自律システム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。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更新する必要があるため、多くのパスを集約する際にはこのキーワードを使用しないでください。
- **summary-only**を使用して無効にすることができます。すべてのネイバーへの、より具体的なルートのアドバタイズメントを抑制します。

ステップ 8 **[...] > [重複（Duplicate）]**（**configure aggregate-address** コマンドの横）をクリックして、集約する追加ルートを設定します。

ステップ 9 [OK] をクリックします。

IPv4 用の BGP フィルタ設定の指定

システムが他のルーティングプロトコルから学習する、または他のルーティングプロトコルにアドバタイズする、ルーティング情報を制限するフィルタルールを作成できます。

ここで説明する設定は、すべてのローカルプロセスに適用され、すべての BGP ネイバーへのアップデートのフィルタ処理に使用されます。ネイバー設定では、ネイバーごとに異なるフィルタルールを設定できます。

始める前に

各フィルタルールに必要なスマートCLI標準アクセスリストオブジェクトを作成します。拒否アクセス制御エントリ（ACE）を使用してエントリに一致するルートを除外し、更新する必要があるルートの ACE を許可します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

filtering コマンドは、**configure address family ipv4** コマンドの下のコマンドセット内にあります。フィルタ処理を設定するには、アドレスファミリを設定する必要があります。これらのルールは IPv6 には使用できません。

ステップ 5 [無効を表示（Show Disabled）] をクリックしてすべてのコマンドを表示し、[+] をクリックして **configure filter-rules** *direction* コマンドを有効にします。

ステップ 6 [direction] をクリックし、**in**（インバウンドアップデートをフィルタ処理する場合）または **out**（アウトバウンドアップデートをフィルタ処理する場合）を選択します。

ステップ 7 インバウンドフィルタの場合は、必要に応じて、アップデートをフィルタ処理するインターフェイスを指定できます。インターフェイスを指定しない場合、フィルタは任意のインターフェイスで受信されるすべてのアップデートに適用されます。

a) [+] をクリックして **distribute-list** *acl-name* **in interface** *interface* コマンドを有効にします。

b) [interface] 変数をクリックし、インターフェイスを選択します。

ステップ 8 アウトバウンドフィルタの場合は、必要に応じて、プロトコルを指定して、そのルーティングプロセスにアドバタイズされたルートにフィルタを制限できます。

distribute-list out コマンドには 2 つの形式があります。一方には [protocol] 変数の後に [identifier] 識別子があり、もう一方には [identifier] 識別子がありません。次のプロトコルを選択できますが、追加の識別子情報を提供する必要があるかどうかに基づいて、これらのコマンドのバージョン間でプロトコルが分けられます。

- **connected**を使用して無効にすることができます。システムのインターフェイスに直接接続されているネットワークに対して確立されたルート用です。
- **static**を使用して無効にすることができます。手動で作成したスタティックルート用です。
- **rip**を使用して無効にすることができます。RIP にアドバタイズされたルート用です。
- **bgp** *automonous-system*：BGP にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている BGP プロセスの自律システム番号を入力します。
- **eigrp** *automonous-system*：EIGRP にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている EIGRP プロセスの自律システム番号を入力します。
- **ospf** *process-id*：OSPF にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている OSPF プロセスのプロセス ID を入力します。

ステップ 9 **[...] > [重複（Duplicate）]**（**configure filter-rules** コマンドの横）をクリックして、別のフィルタルールを定義します。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

BGP ネイバーの設定

BGP がルーティングアップデートを交換するネイバーを定義する必要があります。

始める前に

いくつかのオプションコマンドには、ルートマップ、プレフィックスリストなどのために Smart CLI オブジェクトが必要です。設定が必要なオプションを調べて、オブジェクトが必要かどうかを判断してください。Smart CLI オブジェクトは、関連する BGP コマンドを設定する前に作成する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

neighbor コマンドは、**configure address family ipv4** または **ipv6** コマンドの下のコマンドセット内にあります。ネイバーは、アドレスファミリごとに個別に設定する必要があります。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **configure neighbor** コマンドを有効にします。

ステップ 6 neighbor コマンドで基本ネイバーパラメータを設定します。

- **neighbor** *neighbor-address*：変数をクリックし、設定しているアドレスグループに応じて、BGP ネイバールータの IPv4 アドレスまたは IPv6 アドレスを入力します。
- **remote-as** *as-number*：変数をクリックし、BGP ネイバールータの自律システム番号を入力します。
- *config-options*：変数をクリックし、**properties** を選択します。デフォルトで設定されているプロパティだけで、ネイバーがアクティブになります。この手順で説明されているように、他のオプションを調整できます。

ステップ 7 （オプション）ネイバーの全般設定を指定します。

a) [+] をクリックして **configure neighbor** *neighbor-address* **remote-as** *settings* コマンドを有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。

b) [settings] をクリックし、**general** を選択します。

c) **configure neighbor description** コマンドで、変数をクリックし、最大 80 文字のネイバーの説明（場所や目的など）を入力するか、説明が必要ない場合は [-] をクリックしてコマンドを無効にします。説明にスペースや疑問符を含めることはできません。

d) （IPv4 のみ）**configure neighbor shutdown** コマンドは、最初は有効になっています。このコマンドにより、このBGPネイバーとの通信が無効になり、アクティブなセッションが終了して、関連するルーティング情報がすべて削除されます。このネイバーとアクティブに通信するには、[-] をクリックしてこのコマンドを無効にします。

e) **configure neighbor fall-over bfd** コマンドで、[option] をクリックして、**single-hop** または **multi-hop**（BFD 構成に基づいて）を選択するか、[-] をクリックしてコマンドを無効にします。

このコマンドにより、Bidirectional Forwarding Detection（BFD）からフォワーディングパス検出エラーメッセージを受信するためにBGPが登録されます。シングルホップを選択するかマルチホップを選択するかは、このネイバーへの接続に使用されるインターフェイスに

対して作成して適用したBFDテンプレートのタイプによって異なります。ここでの選択がBFDテンプレートと一致していることを確認してください。BFDテンプレートを作成と適用にはFlexConfigを使用する必要があります。

ステップ 8 （オプション）ネイバーの詳細設定を指定します。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **remote-as** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。

b) [settings] をクリックし、**advanced** を選択します。

c) **neighbor password** コマンドで、[secret] 変数をクリックし、ネイバーの認証時に使用するパスワードを含む秘密鍵オブジェクトを選択するか、メッセージダイジェスト 5（MD5）認証を使用しない場合は [-] をクリックしてコマンドを無効にします。BGP オブジェクトの編集時に鍵オブジェクトを作成できます。

秘密鍵オブジェクトには、大文字と小文字が区別される最大 25 文字のパスワードを含める必要があります。この文字列には、英数字とスペースおよび特殊文字の ` ~ ! @ # $ % ^ & * () - _ = + | \ } ] { [ " ` : ; / > < . , ? を使用できます。ただし、数字-スペース-任意の文字の形式ではパスワードを指定できません。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。

ネイバーが同じパスワードを使用するように設定されていることを確認します。

d) **configure neighbor hops** コマンドで、[options] 変数をクリックして次のいずれかを選択するか、ピアが複数ホップ離れていない（つまり、このシステムに直接接続されていない）場合は [-] をクリックしてコマンドを無効にします。これらのオプションはルーティングループや振動ルートを発生させる可能性があるため、注意して使用してください。直接接続されたピアのみを設定することをお勧めします。

- **ebgp-multihop**を使用して無効にすることができます。直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。このオプションを選択すると、次のコマンドが追加されます。
  - **neighbor ebgp-multihop 255**を使用して無効にすることができます。[255] をクリックし、1 ～ 255 のホップ数で存続可能時間の値を入力します。
  - **neighbor disable-connected-check**を使用して無効にすることができます。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の eBGP ピアリングセッションを確立するには、[+] をクリックしてこのコマンドを有効にして、接続検証を無効にします。このコマンドを使用しない場合、ピアが同じネットワークセグメントに直接接続されていないと、ピアリングセッションは確立されません。
- **ttl-security-hop**を使用して無効にすることができます。BGP ピアリングセッションを保護し、2つの外部BGP（eBGP）ピアを区切るホップの最大数を設定します。このオプションを選択すると、次のコマンドが追加されます。

neighbor ttl-security hops *hop-count*：変数をクリックし、ピアを区切るホップの最大数を 1 ～ 254 の範囲で入力します。

neighbor ttl-security コマンドは、CPU 利用率に基づく攻撃から BGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケット ヘッダーの送信元と宛先の IP アドレスを偽造した大量の IP パケットでネットワークをあふれさせてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。

この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。

この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するように hop-count の値を正確に設定する必要があります。また、この機能をマルチホップ ピアリング セッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。ネットワーク内のすべてのルータでこの機能が設定されていることを確認してください。

e) **neighbor version** コマンドで、[version-number] 変数をクリックし、「4」と入力してソフトウェアに BGP バージョン 4 を強制的に使用させるか、[-] をクリックしてコマンドを無効にします。ソフトウェアはデフォルトではバージョン 4 を使用し、必要に応じて動的にバージョン 2 にネゴシエートします。このコマンドで「4」を設定すると、バージョンネゴシエーションが防止されます。

f) **neighbor transport connection-mode** コマンドで、[options] 変数をクリックして TCP 接続が **active** または **passive** のいずれであるかを選択するか、[-] をクリックしてコマンドを無効にして、モードをデフォルトのままにします。

g) **neighbor transport path-mtu-discovery** コマンドで、[options] 変数をクリックし、**blank** を選択してパス MTU ディスカバリを有効にするか、**disable** を選択してパス MTU ディスカバリを無効にします。パス MTU ディスカバリはデフォルトで実行されるため、空白を選択することは、[-] をクリックしてコマンドを無効にすることと同じです。パス MTU ディスカバリにより、BGP セッションは、より大きな MTU リンクを利用することが可能になります。

ステップ 9 （オプション）ネイバーの移行設定を指定します。

移行設定では、**neighbor local-as** コマンドを設定します。**neighbor local-as** コマンドを使用して、eBGP ネイバーから受信するルートの自律システム番号を追加および削除することで、AS_PATH 属性がカスタマイズされます。このコマンドの設定により、自律システム番号を移行するために、外部ピアに対して別の自律システムのメンバとしてルータを表示できます。この機能を使用すると、既存のピアリング関係を維持したまま、ネットワーク オペレータが通常のサービス時間内に顧客を新しいコンフィギュレーションに移行できるため、BGP ネットワークの自律システム番号を変更するプロセスが簡単になります。

この移行は、正しい eBGP ピアリングセッションについてのみ実行できます。2 つのピアがコンフェデレーションの別々のサブ自律システムにある場合は機能しません。

注意 BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。このコマンドは自律システムの移行のためにのみ設定し、移行が完了したら設定を解除してください。この手順は、経験豊富なネットワーク オペレータだけが行うべきものです。不適切な設定によりルーティングループが発生する可能性があります。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **remote-as** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。

b) [settings] をクリックし、**migration** を選択します。これにより、次のコマンドが追加されます。

configure *neighbor-address* **local-as** *local-as-number options*

c) [local-as-number] 変数をクリックし、ローカル自律システム（AS）番号を入力して、AS_PATH 属性の先頭に 1 ～ 4294967295（asplain 表記）または 1.0 ～ 65535.65535（asdot 表記）を追加します。ローカルBGPルーティングプロセスからの自律システム番号またはリモートピアのネットワークからの自律システム番号を指定することはできません。

d) [options] 変数をクリックし、次のいずれかを選択します。このリスト内の項目（**none** 以外）を選択すると、リスト内のその上のすべてのオプションも選択されることに注意してください。これは予期されることです。オプションは完全に独立しているわけではありません。

- **none**を使用して無効にすることができます。次のオプションは設定しないでください。
- **no-prepend**を使用して無効にすることができます。eBGPネイバーから受信されたルートにローカル自律システム番号を追加しないでください。
- **replace-as**を使用して無効にすることができます。実際の自律システム番号を eBGP アップデートのローカル自律システム番号で置き換えます。ローカルBGPルーティング プロセスからの自律システム番号は、追加されません。
- **dual-as**を使用して無効にすることができます。実際の自律システム番号（ローカルBGPルーティングプロセスからの）を使用するか、ローカル自律システム番号を使用してピアリングセッションを確立するように eBGP ネイバーを設定します。

ステップ 10 （オプション。IPv4 のみ）ネイバーのハイアベイラビリティ（HA）設定を指定します。

HAモード設定では、個々のBGPネイバーのグレースフルリスタート機能を有効または無効にする **neighbor ha-mode graceful-restart** コマンドが設定されます。グレースフル リスタート機能が BGP ピアでイネーブルになっている場合は、disable キーワードを使用してディセーブルにできます。

グレースフル リスタート機能は、セッションの確立時にOPENメッセージのノンストップ フォワーディング（NSF）対応ピアと NSF 認識ピアの間でネゴシエートされます。BGP セッショ

ンが確立された後にグレースフルリスタート機能を有効にする場合は、ソフトリセットまたはハードリセットによってセッションを再起動する必要があります。

HAモード設定では、個々のネイバーのグレースフルリスタートを設定します。代わりに、BGPグローバル設定を使用して、すべてのネイバーのグレースフルリスタートを有効にできます。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **remote-as** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。
b) [settings] をクリックし、**ha-mode** を選択します。
c) グレースフルリスタートを無効にする場合は、**neighbor ha-mode graceful-restart** コマンドの [options] をクリックし、**disable** を選択します。以前の無効化アクションを取り消すには、空白を選択します。

ステップ 11 （オプション）ネイバーのアクティベーション オプションを設定します。

新しいネイバーを設定すると、デフォルトでアクティブになります。ネイバーを最初に無効にする場合、または他のアクティベーション設定を指定する場合は、アクティベーション設定を有効にする必要があります。

a) **configure neighbor** *neighbor-address* **activate** *activate-options* コマンドを有効にするには、[+] をクリックします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。
b) [activate-options] をクリックし、**properties** を選択します。
c) **neighbor** *neighbor-address* **activate** コマンドが有効な状態で追加されます。コマンドを無効にして、ネイバーを最初に無効として設定するには、[-] をクリックしてください。ネイバーと通信する準備ができたら、このオブジェクトを編集してネイバーを有効にする必要があります。

ステップ 12 （オプション）ネイバーのアクティベーション設定でフィルタ処理を設定します。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **activate** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。
b) [settings] をクリックし、**filtering** を選択します。
c) 次の neighbor コマンドの任意の組み合わせを使用して、このネイバーから受信されるプレフィックスまたはこのネイバーに送信されるプレフィックスを制御するようにフィルタ処理を設定します。使用しないものを無効にするには、[-] をクリックします。これらのコマンドはすべて、着信方向と発信方向の両方でフィルタ処理を許可します。双方向を設定する場合は、コマンドに対して **[...]** > **[複製（Duplicate）]** をクリックしてください。

   同じ方向のネイバーに **neighbor distribute-list** コマンドと **neighbor prefix-list** コマンドの両方を適用しないでください。これら 2 つのコマンドは相互に排他的であり、インバウンドまたはアウトバウンドの各方向に適用できるのは、いずれかだけです。

- **distribute-list** *acl options*：（IPv4 のみ）選択した標準アクセスリスト（ACL）に基づいてプレフィックスをフィルタ処理します。次に、[options] をクリックし、フィルタを **in** 方向で適用するか **out** 方向で適用するかを選択します。
- **route-map** *route-map options*。選択したルートマップに基づいてプレフィックスをフィルタ処理します。次に、[options] をクリックし、フィルタを **in** 方向で適用するか **out** 方向で適用するかを選択します。ルートマップ内で、アクセスリスト、AS パス、プレフィックス、および配布リストに基づいてフィルタ処理を設定できます。
- **prefix-list** *prefix-list options*：選択した IPv4 または IPv6 プレフィックスリストに基づいてプレフィックスをフィルタ処理します。次に、[options] をクリックし、フィルタを **in** 方向で適用するか **out** 方向で適用するかを選択します。
- **filter-list** *as-path options*：選択した AS パスフィルタオブジェクトに基づいてプレフィックスをフィルタ処理します。次に、[options] をクリックし、フィルタを **in** 方向で適用するか **out** 方向で適用するかを選択します。

d) **configure prefix-limit neighbor** *neighbor-address limit-options* コマンドで、[limit-options] をクリックして次のいずれかを選択するか、[-] をクリックしてコマンドを無効にします。いずれかのオプションを選択すると、何らかの形式の **neighbor maximum-prefix** コマンドが、設定する必要がある追加のオプションとともに追加されます。このコマンドを使用して、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。

- **none**を使用して無効にすることができます。追加パラメータのない基本形式のコマンドを設定します。変数をクリックし、次の値を設定します。
  - max-prefix-limit：このネイバーから許可されるプレフィックスの最大数（1 ～ 2147483647）。他のいずれかのオプションを選択する場合も、この変数を設定する必要があります。
  - **75**（しきい値）：ルータが警告メッセージの生成を開始する最大値に対するパーセンテージ（1 ～ 100）。デフォルトは 75 % です。
- **restart**を使用して無効にすることができます。制限に達するとネイバーとのピアリングセッションを停止します。[restart-interval] 変数をクリックし、システムがセッションを再開する前に待機する時間を 1 ～ 65535 分の範囲で設定します。
- **warning-only**を使用して無効にすることができます。制限に達してもセッションを停止しません。代わりに、単に警告の Syslog メッセージを発行して、セッションを続行します。

ステップ 13 （オプション）ネイバーのアクティベーション設定でルートを設定します。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **activate** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。

b) [settings] をクリックし、**routes** を選択します。

c) **neighbor advertisement-interval** コマンドで、[value] 変数をクリックし、このネイバーへのルートアップデート送信の最小ルート アドバタイズメント インターバルを 0 ～ 600 秒の範囲で入力します。または、[-] をクリックすることでコマンドを無効にして、インターバルを、デフォルトの 0（仮想ルータでの iBGP および eBGP セッションの場合）または 30（仮想ルータ以外での eBGP セッションの場合）のままにします。値を 0 にすると、頻度を考慮せず、ルーティングテーブルが変更されるたびにアップデートが送信されます。

d) **neighbor advertise-map** コマンドで、次のオプションを設定して、選択したルートをネイバーに条件付きでアドバタイズするか、[-] をクリックすることでコマンドを無効にして、すべてのルートアップデートをネイバーに無条件で送信します。

条件付きでアドバタイズされるルート（プレフィックス）は、アドバタイズマップと存在マップまたは非存在マップの 2 つのルート マップで定義されます。

存在マップまたは不在マップと関連付けられているルートマップは、BGP スピーカーが追跡するプレフィックスを指定します。

アドバタイズ マップと関連付けられているルート マップは、条件が満たされたときに、指定されたネイバーにアドバタイズされるプレフィックスを指定します。

存在マップを設定する場合、プレフィックスがアドバタイズマップと存在マップの両方に存在するときに条件が満たされます。

不在マップを設定する場合、プレフィックスがアドバタイズマップには存在するが、不在マップには存在しないときに条件が満たされます。

条件が満たされない場合、ルートは取り消され、条件付きアドバタイズメントは行われません。条件付きアドバタイズメントを行うには、ダイナミックにアドバタイズされるルート、またはアドバタイズされないルートがすべて BGP ルーティング テーブルに存在する必要があります。

- *advertise-route-map*：この変数をクリックし、存在マップまたは不在マップの条件が満たされた場合にアドバタイズされるルートを定義するルートマップを選択します。
- *options condition-route-map*：[options] をクリックし、次のいずれかを選択します。
  - **exist-map**を使用して無効にすることができます。変数をクリックし、存在ルートマップを選択します。
  - **non-exist-map**を使用して無効にすることができます。変数をクリックし、不在ルートマップを選択します。

e) **neighbor** *neighbor-address* **remove-private-as** コマンドが有効な状態で追加されます。コマンドを無効にするには [-] をクリックします。このコマンドにより、プライベート自律システム番号が eBGP アウトバウンドルーティング アップデートから削除されます。プライベート AS の値の範囲は 64512 ～ 65535 です。

f) **configure neighbor default-originate** コマンドで、[options] をクリックして次のいずれかを選択するか、[-] をクリックしてコマンドを無効にします。

- **none**を使用して無効にすることができます。システムがデフォルトルートをネイバーに無条件で送信することを可能にします。

- **route-map**を使用して無効にすることができます。システムがデフォルトルートをネイバーに条件付きで送信するようにします。match IP address 句を含むルートマップとともに使用することで、IP アクセスリストと完全に一致するルートがある場合にデフォルトルートが挿入されるようにすることができます。ルートマップで標準アクセスリストまたは拡張アクセスリストを使用してデフォルトルートを定義することができます。オブジェクトに追加された **neighbor default-originate** コマンドの [route-map] 変数をクリックし、ルートマップを選択する必要があります。

ステップ 14 （オプション）ネイバーのアクティベーション設定でタイマーを設定します。

ネイバーのタイマーを設定すると、この設定が、グローバル BGP 設定ですべての BGP ネイバーに対して設定されているタイマーよりも優先されます。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **activate** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。
b) [settings] をクリックし、**timers** を選択します。
c) **neighbors timers** コマンドで、次の変数を設定します。

- *keepalive-interval*：システムがこのネイバーにキープアライブメッセージを送信する頻度（0 ～ 65535 秒）。このコマンドを設定しない場合、デフォルトは 60 秒です。
- *hold-time*：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、このネイバーがデッドであるとシステムが宣言するまでの時間（0 ～ 65535 秒）。このコマンドを設定しない場合、デフォルトは 180 秒です。
- **0**（最小ホールド時間）：このネイバーに設定できる最小許容ホールド時間（0～65535 秒）。この値は、このシステムに設定されているホールド時間以下である必要があります。ネイバーのホールド時間がこの値よりも小さい場合、システムはネイバーとの BGP セッションを確立しません。

ステップ 15 （オプション）高度なネイバーアクティベーション設定を指定します。

a) すでに設定されている場合は、**[...]** > **[複製（Duplicate）]** を **configure neighbor** *neighbor-address* **activate** *settings* コマンドに対してクリックするか、まだ使用されていない場合は [+] をクリックして有効にします。コマンドが表示されない場合は、[無効を表示（Show Disabled）] をクリックします。
b) [settings] をクリックし、**advanced** を選択します。
c) 次の **neighbor** コマンドのどれを有効のままにするのかを決定します。[-] をクリックして不要なオプションを無効にします。

- **send-community**を使用して無効にすることができます。ネイバーにコミュニティ属性を送信します。
- **weight** *value*。このネイバーから学習したルートに初期重み（0～65535）を割り当てるには、この変数をクリックします。このコマンドを設定しない場合、別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカルルータから送信されたルートのデ

フォルトの重みは32768です。ただし、ルートマップを使用して設定されたルートの重みは、このコマンドを使用して設定された重みよりも優先されます。

- **next-hop-self**を使用して無効にすることができます。ルータをBGP対応ネイバーのネクストホップとして設定します。このコマンドは、BGP ネイバーから同じ IP サブネット上の他の一部のネイバーに直接アクセスできない非メッシュ型のネットワーク（フレーム リレーや X.25 など）で便利です。

ステップ 16 **[...]** > **[重複（Duplicate）]**（**configure neighbor** コマンドの横）をクリックして、別のネイバーを定義します。必要な数だけ定義します。

ステップ 17 [OK] をクリックします。

他のルーティングプロトコルからの BGP ルート再配布の設定

他のルーティングプロトコル、接続されたルート、およびスタティックルートからの BGP プロセスへのルートの再配布を制御できます。

始める前に

BGPへの再配布を設定する前に、ルートを再配布するルーティングプロセスを設定し、変更を展開することがベストプラクティスです。

ルートマップを適用して、再配布されるルートを微調整する場合は、Smart CLI ルートマップオブジェクトを作成します。ルートマップに一致するルートが再配布され、一致しないルートはすべて再配布されません。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、BGP を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [BGP] タブをクリックします。

ステップ 4 BGP プロセスオブジェクトを追加または編集します。

redistribution コマンドは、**configure address family ipv4** または **ipv6** コマンドの下のコマンドセット内にあります。再配布を設定するには、アドレスファミリを設定する必要があります。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **configure ipv4/ipv6 redistribution** コマンドを有効にします。

ステップ 6 [protocol] 変数をクリックし、ルートの再配布元となる送信元プロセスを選択します。**connected** および **static** のルート、あるいは **eigrp**（IPv4 のみ）、**isis**、**ospf**、**rip**（IPv4 のみ）によって生成されたルートを再配布できます。

ステップ 7 ルーティングプロセスを選択した場合は、[identifier] 変数をクリックして、必要な値を入力します。

- **eigrp**を使用して無効にすることができます。自律システムの番号を入力します。
- **ospf**を使用して無効にすることができます。プロセス ID 番号を入力します。
- **connected**、**static**、**isis**、**rip**。**none** を入力します。別の値を入力しても、無視されます。

ステップ 8 （任意：IS のみ）**redistribute isis level-2** コマンドで、**level-2** をクリックして、IS-IS エリア（**level-1**）内でのみ学習したルートを再配布するか、IS-IS エリア（**level-2**）間、または両方（**level-1-2**）で再配布するかを選択します。

ステップ 9 （任意：すべてのプロトコル）再配布されたルートのメトリックを微調整するには、[+] をクリックして次のコマンドを有効にし、オプションを設定します。

redistribute *protocol* **metric** *metric-value*

変数をクリックし、配布されているルートのメトリック値（0～4294967295）を入力します。

ステップ 10 （任意：すべてのプロトコル）ルートマップに基づいて再配布されるルートを微調整するには、[+] をクリックして **redistribute route-map** コマンドを有効にし、変数をクリックして、制限を定義するルートマップを選択します。

ルートマップを適用しない場合は、（再配布用に設定された他のコマンドに適合する）プロセスのすべてのルートが再配布されます。

ステップ 11 （任意：OSPF のみ）OSPF プロセスからルートを再配布する場合、次のコマンドはデフォルトで有効になっています。[-] をクリックして、不要なコマンドを無効化できます。

これらのコマンドで、OSPF ルートを他のルーティングドメインに再配布する条件を指定します。

- **redistribute ospf match external 1**を使用して無効にすることができます。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。
- **redistribute ospf match external 2**を使用して無効にすることができます。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。
- **redistribute ospf match internal**を使用して無効にすることができます。特定の自律システムの内部ルート。
- **redistribute ospf match nssa-external 1**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。
- **redistribute ospf match nssa-external 2**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。

ステップ 12 **[...] > [重複（Duplicate）]**（**configure redistribution** コマンドの横）をクリックして、別のプロトコルの再配布を設定できます。ネットワークに適したプロトコルごとの再配布を設定します。

ステップ 13 [OK] をクリックします。

BGP のモニタリング

BGP をモニターし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。また、[ルーティング（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

追加オプションのリストを取得するには、**show bgp ?** を使用します。たとえば、自律システム番号（および仮想ルータ）を指定して、表示する情報を制限することができます。また、探している情報だけを対象とするその他のオプションも指定できます。次のリストは概要のみです。

- **show bgp**

  BGP ルーティング テーブル内のエントリを表示します。

- **show bgp cidr-only**

  ナチュラル ネットワーク マスク以外を使用するルート（つまり、クラスレス ドメイン間ルーティング（CIDR））を表示します。

- **show bgp community**

  指定された BGP コミュニティに属するルートを示します。

- **show bgp community-list**

  BGP コミュニティ リストによって許可されたルートを表示します。

- **show bgp filter-list** *access-list-number*

  指定されたフィルタ リストと一致するルートを表示します。

- **show bgp injected-paths**

  BGP ルーティング テーブルに注入されたすべてのパスを表示します。

- **show bgp ipv4 unicast**

  ユニキャスト セッションの IPv4 BGP ルーティング テーブルのエントリを表示します。

- **show bgp ipv6 unicast**

  IPv6 BGP ルーティング テーブルのエントリを表示します。

- **show bgp neighbors**

  ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。

- **show bgp paths**

  データベース内のすべての BGP パスを表示します。

- **show bgp prefix-list**

  プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。

- **show bgp regexp** *regexp*

  自律システム パスの正規表現と一致するルートを表示します。

- **show bgp rib-failure**

  ルーティング情報ベース（RIB）テーブルにインストールできなかったBGPルートを表示します。

- **show bgp summary**

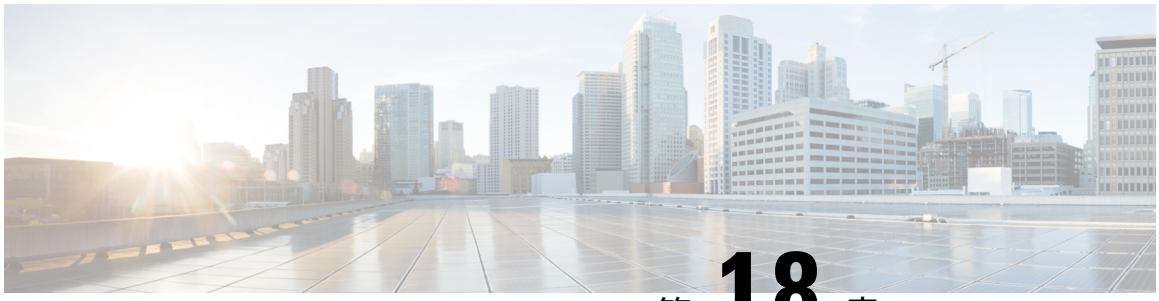
  すべての BGP 接続のステータスを表示します。

- **show bgp update-group**

  BGP アップデート グループに関する情報を表示します。

第 V 部

セキュリティ ポリシー



第 18 章

SSL 復号

HTTPS など一部のプロトコルは、セキュア ソケット レイヤ（SSL）またはその後継バージョンである Transport Layer Security（TLS）を使用して、セキュアな転送のためにトラフィックを暗号化します。システムでは暗号化された接続を検査できないため、アクセス判断のために上位層のトラフィック特性を考慮したアクセスルールを適用する場合は、暗号化された接続を復号する必要があります。

SSL 復号について

通常、接続は、許可されるかブロックされるかを決定するアクセス コントロール ポリシーを経由します。ただし、SSL復号ポリシーを有効にする場合、暗号化された接続は最初にSSL復号ポリシー経由で送信され、復号化するかブロックする必要があるかが判断されます。ブロックされていない接続は、復号化されているかどうかにかかわらず、許可/ブロックの最終的な決定のためアクセス コントロール ポリシーを経由します。

（注） アイデンティティ ポリシーでアクティブな認証ルールを実装するためには、SSL復号ポリシーを有効にする必要があります。SSL復号を有効にしてアイデンティティ ポリシーを有効にするが、SSL 復号は実装しない場合、デフォルトのアクションに [復号しない（Do Not Decrypt）] を選択し、追加のSSL復号ルールは作成しないでください。アイデンティティ ポリシーでは、必要なルールを自動的に生成します。

ここでは、暗号化トラフィック フロー管理と復号化についてさらに詳しく説明します。

SSL 復号を実装する理由

HTTPS 接続などの暗号化されたトラフィックは検査することができません。

銀行や他の金融機関への接続など、多くの接続は合法的に暗号化されます。多くの Web サイトでは、プライバシーや機密性の高いデータを保護するために暗号化を使用します。たとえば、Device Manager への接続は暗号化されます。

ただし、暗号化された接続の中ではユーザが望ましくないトラフィックを隠すこともできます。

SSL復号を実装することによって、接続を復号して脅威またはその他の望ましくないトラフィックが含まれていないかを確認するために検査し、再度暗号化してから接続の続行を許可できます。（復号されたトラフィックは、アクセス制御ポリシーを通過し、暗号化された特性ではなく、復号された接続の検査特性に基づいたルールに一致します。）これは、機密情報を保護するために、アクセス制御ポリシーを適用する必要性とユーザの必要性との間でバランスをとります。

ネットワークを利用させたくない種類の暗号化されたトラフィックをブロックする SSL 復号ルールを構成することもできます。

トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

暗号化されたトラフィックに適用できるアクション

SSL復号ルールを設定する場合は、次のトピックで説明しているアクションを適用できます。これらのアクションは、明示的なルールと一致しないすべてのトラフィックに適用されるデフォルトのアクションにも使用できます。

（注） SSL 復号ポリシーを経由するすべてのトラフィックは、アクセス コントロール ポリシーを経由する必要があります。SSL復号ポリシーにドロップするトラフィックを除き、許可またはドロップの最終的な決定はアクセス コントロール ポリシーに委ねられます。

再署名の復号

トラフィックを復号し再署名する場合、システムは中間者として機能します。

たとえば、ユーザがブラウザで https://www.cisco.com と入力します。トラフィックが 脅威に対する防御デバイスに達すると、デバイスはルールで指定されたCA証明書を使用するユーザーとネゴシエーションを行い、ユーザーと 脅威に対する防御 デバイス間に SSL トンネルを構築します。同時に、デバイスはhttps://www.cisco.com に接続し、サーバーと 脅威に対する防御 デバイスの間に SSL トンネルを作成します。

このため、ユーザには、www.cisco.com からの証明書ではなく、SSL 復号ルールで設定された CA 証明書が表示されます。ユーザは、接続を完了するために証明書を信頼する必要がありま

す。脅威に対する防御デバイスは、ユーザーと宛先サーバーの間のトラフィックで両方向に復号/再暗号化を実行します。

（注） サーバー証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザーに出されます。これを防止するには、クライアントの信用できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

再署名の復号アクションでルールを設定する場合、設定されているルールの条件に加え、参照される内部 CA 証明書の署名アルゴリズムの種類に基づいてルールがトラフィックと一致します。SSL 復号ポリシーに 1 つの再署名証明書を選択できるため、これによって再署名ルールのトラフィック一致を制限できます。

たとえば、楕円曲線（EC）アルゴリズムで暗号化された発信トラフィックは、再署名証明書が EC ベースの CA 証明書の場合にのみ、再署名の復号ルールと一致します。同様に、RSA アルゴリズムで暗号化されたトラフィックは、グローバル再署名証明書が RSA の場合にのみ、再署名の復号ルールと一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されたその他すべてのルール条件が一致していても、このルールとは一致しません。

既知のキーの復号

宛先サーバを所有している場合、既知のキーで復号化を実装できます。この場合、ユーザーが https://www.cisco.com への接続を開くと、証明書を提示しているのが 脅威に対する防御 デバイスであっても、www.cisco.com の実際の証明書がユーザーに表示されます。

ドメインおよび証明書の所有者は、所属組織でなければなりません。cisco.com を例として取り上げると、エンドユーザにシスコの証明書が表示されるのは、組織が実際にドメイン cisco.com の所有者であり（つまり、所属企業が Cisco Systems であること）、パブリック CA によって署名された cisco.com 証明書の所有権を持っている場合のみです。復号できるのは、所属組織が所有するサイトの既存のキーを使用する場合のみです。

既知のキーを使用して復号する主な目的は、HTTPS サーバへのトラフィックを復号して、社内サーバを外部の攻撃から保護することです。外部 HTTPS サイトへのクライアント側のトラフィックを検査する場合は、サーバを所有していないので、再署名の復号を使用する必要があります。

（注） 既知のキーの復号を使用するには、サーバーの証明書およびキーを内部アイデンティティ証明書としてアップロードし、SSL復号ポリシー設定で既知のキーの証明書一覧に追加する必要があります。その後は、宛先アドレスとしてサーバのアドレスを使用して既知のキーの復号化のルールを作成できます。SSL復号ポリシーに証明書を追加する方法については、既知のキーと復号の再署名の証明書の設定 （559 ページ）を参照してください。

復号禁止

特定の種類のトラフィックで復号をバイパスする場合、トラフィックの処理は行われません。暗号化されたトラフィックはアクセス コントロール ポリシーに渡され、一致するアクセス制御ルールに基づいて許可またはドロップされます。

ブロック

単にSSL復号ルールと一致する暗号化されたトラフィックをブロックできます。SSL復号ポリシーのブロックでは、アクセス コントロール ポリシーに接続が達することを防ぎます。

HTTPS 接続をブロックすると、ユーザにはシステムのデフォルトのブロック応答ページが表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルト ページが表示されます。エラー メッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

自動的に生成された SSL 復号ルール

SSL復号ポリシーを有効にしてもしなくても、システムはアクティブな認証を実装する各アイデンティティ ポリシー ルールに対して再署名の復号ルールを自動的に生成します。これは、HTTPS 接続でアクティブな認証を有効にするために必要です。

SSL復号ポリシーを有効にすると、アイデンティティ ポリシーのアクティブな認証ルールの見出しの下にこれらのルールが表示されます。これらのルールは、SSL復号ポリシーの上部にグループ化されます。ルールは読み取り専用です。アイデンティティ ポリシーを変更することによってのみ変更できます。

復号できないトラフィックの処理

接続が復号できなくなる特性は複数あります。接続に次の特性のいずれかがある場合、接続で一致するルールがあっても接続にはデフォルトのアクションが適用されます。（[復号しない（Do Not Decrypt）] ではなく）デフォルト アクションとしてブロックを選択する場合、正当

なトラフィックの過剰なドロップなどの問題があることがあります。デフォルトの動作は変更できます（高度なトラフィックおよび復号できないトラフィックの設定の指定（560 ページ）を参照）。

- 圧縮されたセッション：データ圧縮が接続に適用されています。
- SSLv2 セッション：サポートされている最下位の SSL バージョンは SSLv3 です。
- 不明な暗号スイート：システムで接続の暗号スイートが認識されません。
- サポート外の暗号スイート：システムで、検出された暗号スイートに基づく復号化がサポートされません。
- キャッシュされないセッション：SSL セッションにおいてセッションの再利用が可能になっていて、クライアントとサーバがセッション ID でセッションを再確立したときに、システムがそのセッション ID をキャッシュに入れなかったことを意味します。
- ハンドシェイク エラー：SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。
- 復号エラー：復号処理中にエラーが発生しました。
- パッシブ インターフェイス トラフィック：パッシブ インターフェイス（パッシブ セキュリティ ゾーン）のすべてのトラフィックが復号不能です。

SSL 復号のためのライセンス要件

SSL 復号ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するには、**URL** ライセンスが必要です。ライセンスの設定については、オプション ライセンスの有効化または無効化 （109 ページ）を参照してください。

SSL 復号のガイドライン

SSL 復号ポリシーを設定してモニターする場合は、次の点に注意してください。

- SSL復号ポリシーは、次のようなアクセス制御ルールがトラフィックを信頼またはブロックするように設定されている場合に、それらのルールに一致する接続に関してバイパスされます。
  - セキュリティゾーン、ネットワーク、地理位置情報、およびポートだけをトラフィック照合基準として使用する。
  - 検査を必要とする他のルール（アプリケーションまたは URL に基づいて接続を照合するルールなど）に先立つか、侵入またはファイル検査を適用するルールを許可する。

- URL カテゴリのマッチングを使用するときは、サイトのログイン ページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は「Web ベースの電子メール」カテゴリにあり、ログイン ページは「インターネット ポータル」カテゴリにあります。これらのサイトへの接続を復号するには、両方のカテゴリをルールに含める必要があります。
- 脆弱性データベース（VDB）の更新によってアプリケーションが削除（廃止）される場合は、削除されたアプリケーションを使用するすべての SSL 暗号解読ルールまたはアプリケーションフィルタに変更を加える必要があります。これらのルールを修正するまで、変更は展開できません。さらに、システムソフトウェアの更新は、問題を修正するまでインストールできません。[アプリケーションフィルタ（Application Filters）] オブジェクト ページ、またはルールの [アプリケーション（Application）] タブでは、これらのアプリケーション名の後に「（廃止）（Deprecated）」と表示されます。
- アクティブ認証ルールを使用している場合は、SSL 復号ポリシーを無効にすることができません。SSL 復号ポリシーを無効にするには、アイデンティティ ポリシーを無効にするか、またはアクティブ認証を使用するアイデンティティ ルールを削除する必要があります。

SSL 復号ポリシーの実装および管理方法

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーン テキスト トラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL 復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

他のセキュリティ ポリシーの場合とは異なり、SSL 復号ポリシーは、監視して積極的に保守する必要があります。これは、証明書の期限が切れたり、宛先サーバで変更されたりするためです。さらに、クライアント ソフトウェアの変更により特定の接続を復号する能力が変わる場合もあります。これは、再署名の復号アクションを中間者攻撃と区別できないためです。

次の手順では、SSL 復号ポリシーの実装と保守のエンドツーエンド プロセスを説明します。

手順

ステップ 1 再署名の復号ルールを実装する場合は、必要な内部 CA 証明書を作成します。

内部認証局（CA）証明書を使用する必要があります。次の選択肢があります。ユーザは証明書を信頼する必要があるため、すでに信頼されると設定されているクライアント ブラウザに証明書をアップロードするか、またはアップロードする証明書がブラウザの信頼ストアに追加されるようにします。

- デバイス自体によって署名される自己署名内部 CA 証明書を作成します。自己署名内部および内部 CA 証明書の生成 （186 ページ）を参照してください。
- 外部の信頼できる CA または組織内部の CA によって署名される内部 CA 証明書およびキーをアップロードします。内部および内部 CA 証明書のアップロード （184 ページ）を参照してください。

ステップ 2 既知のキーの復号ルールを実装する場合は、各内部サーバーから証明書とキーを収集します。

サーバーから証明書とキーを取得する必要があるため、既知のキーの復号は自分で制御しているサーバーでのみ使用できます。これらの証明書とキーを内部証明書（内部 CA 証明書ではない）としてアップロードします。「内部および内部CA証明書のアップロード（184ページ）」を参照してください。

ステップ 3 SSL 復号ポリシーの有効化 （548 ページ）。

ポリシーを有効にする際に、いくつかの基本的な設定も構成します。

ステップ 4 SSL 復号のデフォルト アクションの設定 （549 ページ）。

不確かな場合は、デフォルト アクションとして [復号しない（Do not decrypt）] を選択します。この場合でも、アクセス コントロール ポリシーは、デフォルトの SSL 復号ルールに一致するトラフィックを適切であればドロップできます。

ステップ 5 SSL 復号ルールの設定 （550 ページ）。

復号するトラフィック、および適用する復号のタイプを識別します。

ステップ 6 既知のキーでの復号を設定する場合は、これらの証明書を含めるようにSSL復号ポリシー設定を編集します。既知のキーと復号の再署名の証明書の設定（559ページ）を参照してください。

ステップ 7 必要に応じて、再署名の復号ルールに使用する CA 証明書をダウンロードして、クライアント ワークステーションのブラウザにアップロードします。

証明書のダウンロードおよびクライアントへの配布については、再署名の復号ルールの CA 証明書のダウンロード （561 ページ）を参照してください。

ステップ 8 定期的に、再署名証明書および既知のキーの証明書を更新します。

- 再署名証明書：期限切れになる前にこの証明書を更新します。Device Manager を使用して証明書を生成する場合は、5 年間有効です。証明書の有効期間を確認するには、**[オブジェクト（Objects）]** > **[証明書（Certificates）]** を選択し、リスト内で証明書を見つけて [アクション（Actions）] 列の [情報（information）] アイコン（  ）をクリックします。情報ダイアログ ボックスに、有効期間およびその他の特性が表示されます。このページから代替証明書をアップロードすることもできます。
- 既知のキーの証明書：既知のキーによる復号ルールの場合、宛先サーバーの現在の証明書とキーがアップロードされていることを確認する必要があります。サポートされるサーバで証明書およびキーが変更されるたびに、新しい証明書およびキーを（内部証明書として）アップロードし、新しい証明書を使用するようにSSL復号設定を更新する必要があります。

ステップ 9 外部サーバで不足している信頼できる CA 証明書をアップロードします。

システムには、サードパーティによって発行された、広範な信頼できるCAルート証明書および信頼できるCA中間証明書が含まれています。これらは、再署名の復号ルールについて脅威に対する防御 と宛先サーバーの間で接続をネゴシエートするときに必要です。

信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。**[オブジェクト（Objects）]** > **[証明書（Certificates）]** ページで証明書をアップロードします。信頼できる CA 証明書のアップロード （188 ページ） を参照してください。

SSL 復号ポリシーの設定

URL フィルタリング、侵入、マルウェア コントロール、および詳細なパケット検査を必要とするその他のサービスを適用できるように、SSL 復号ポリシーを使用して暗号化されたトラフィックをプレーン テキスト トラフィックにできます。ポリシーがトラフィックを許可する場合、そのトラフィックはデバイスから出る前に再暗号化されます。

SSL復号ポリシーは、暗号化されたトラフィックにのみ適用されます。暗号化されていない接続は SSL 復号ルールに対して評価されません。

（注） VPN トンネルは SSL 復号ポリシーが評価される前に復号されるので、トンネル自体にはポリシーは適用されません。ただし、トンネル内で暗号化された接続はSSL復号ポリシーによる評価の対象となります。

以下の手順で、SSL復号ポリシーを設定する方法を説明します。SSL復号を作成および管理するエンドツーエンドプロセスの説明については、SSL復号ポリシーの実装および管理方法（544 ページ）を参照してください。

始める前に

SSL 復号ルール テーブルには、2 つのセクションが含まれています。

- [アイデンティティポリシーアクティブ認証ルール（Identity Policy Active Authentication Rules）]：アイデンティティ ポリシーを有効にしてアクティブ認証を使用するルールを作成すると、システムがこれらのポリシーの動作に必要なSSL復号ルールを自動的に作成します。これらのルールは、常に自分で作成したSSL復号ルールの前に評価されます。アイデンティティ ポリシーに変更することによって、間接的にのみこれらのルール変更できます。
- [SSLネイティブルール（SSL Native Rules）]：これらは自分で構成したルールです。このセクションにのみルールを追加できます。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

ポリシーをまだ有効化していない場合は、[SSL復号の有効化（Enable SSL Decryption）] をクリックし、「SSL 復号ポリシーの有効化 （548 ページ）」の説明に従ってポリシーを設定します。

ステップ 2 ポリシーのデフォルト アクションを設定します。

最も安全な選択肢は、[復号しない（Do Not Decrypt）] です。詳細については、SSL 復号のデフォルト アクションの設定 （549 ページ）を参照してください。

ステップ 3 SSL 復号ポリシーを管理します。

SSL復号を設定した後、このページにすべてのルールが順番に一覧表示されます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- ポリシーを無効にするには、[SSL復号ポリシー（SSL Decryption Policy）] トグルをクリックします。[SSL複合を有効化（Enable SSL Decryption）] をクリックすると再度有効にできます。
- ポリシーで使用する証明書のリストを含むポリシー設定を編集するには、[SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックします。SSL 復号設定の指定 （559 ページ）を参照してください。また、クライアントに配布できるように、再署名の復号ルールで使用する証明書をダウンロードできます。次のトピックを参照してください。
  - 既知のキーと復号の再署名の証明書の設定 （559 ページ）
  - 再署名の復号ルールの CA 証明書のダウンロード （561 ページ）
- ルールを設定するには、次の手順を実行します。
  - 新しいルールを作成するには、[+] ボタンをクリックします。SSL 復号ルールの設定（550 ページ）を参照してください。
  - 既存のルールを編集する場合は、（[操作（Actions）] 列の）対象のルールの編集アイコン（✎）をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
  - 不要になったルールを削除する場合は、（[操作（Actions）] 列の）対象のルールの [削除（delete）] アイコン（🗑）をクリックします。
- ルールを移動するには、編集して [順序（Order）] ドロップダウン リストから新しい場所を選択します。
- URL カテゴリの削除または変更などが原因で特定のルールに問題が発生した場合、これらのルールのみを表示するには、検索ボックスの横にある [See Problem Rules] リンクをクリッ

クしてテーブルをフィルタ処理します。これらのルールを編集および修正（または削除）して、必要とするサービスが提供されるようにします。

SSL 復号ポリシーの有効化

SSL 復号ルールを設定する前に、ポリシーを有効にして、いくつかの基本的な設定を構成する必要があります。以下の手順で、ポリシーを直接有効にする方法を説明します。アイデンティティ ポリシーを有効にするときにこのポリシーを有効にすることもできます。アイデンティティ ポリシーでは、SSL 復号ポリシーを有効にする必要があります。

始める前に

SSL復号ポリシーを持たないリリースからアップグレードし、アクティブな認証ルールを使用してアイデンティティ ポリシーを設定した場合、SSL復号ポリシーはすでに有効になっています。必ず使用する再署名の復号証明書を選択し、必要に応じて事前定義されたルールを有効にします。

手順

ステップ 1 **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [SSL復号の有効化（Enable SSL Decryption）] をクリックしてポリシー設定を構成します。

- このポリシーを初めて有効にする場合は、[SSL復号設定（SSL Decryption Configuration）] ダイアログ ボックスが開きます。次の手順に進みます。
- 以前にこのポリシーを設定した後で無効にした場合は、前の設定とルールを使用してポリシーが再度有効になります。[SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックし、既知のキーと復号の再署名の証明書の設定（559 ページ）で説明されているように設定できます。

ステップ 3 [再署名証明書の復号（Decrypt Re-Sign Certificate）] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成（Create Internal CA）] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（⬇）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロード（561 ページ）も参照してください。

ステップ 4 （オプション）[信頼できるCA証明書（Trusted CA Certificates）] の下にある [+] をクリックし、ポリシーで信頼する証明書または証明書グループを選択します。

デフォルトグループの Cisco-Trusted-Authorities には、システム定義の信頼できる CA 証明書がすべて含まれています。追加の証明書をアップロードした場合は、ここでそれらを追加するか、それらを独自のグループに収集して、ここでグループを選択できます。
Cisco-Trusted-Authorities グループを置き換えるか、単に独自のグループを追加できます。ユーザーは、証明書の署名機関がこのリストに含まれていないサイトの証明書を受け入れるように求められます。証明書が信頼されていないという理由だけで、サイトへのアクセスがブロックされることはありません。

リストを空のままにするか、空の証明書グループのみを選択すると、SSL復号ポリシーはすべての証明書を信頼します。

ステップ 5 初期 SSL 復号ルールを選択します。

システムには以下の事前定義ルールが含まれており、役立つ場合があります。

- [Sensitive_Data]：このルールでは、金融サービスまたは健康と医療の URL カテゴリ（銀行、医療機関、ヘルスケア サービスなど）内の Web サイトに一致するトラフィックは復号しません。このルールを実装するには、URL ライセンスを有効にする必要があります。

ステップ 6 [有効（Enable）] をクリックします。

SSL 復号のデフォルト アクションの設定

暗号化された接続が特定のSSL復号ルールに一致しない場合、SSL復号ポリシーのデフォルトアクションに基づいて処理されます。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [デフォルトアクション（Default Action）] フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [復号しない（Do Not Decrypt）]：暗号化された接続を許可します。次にアクセス制御ポリシーは、暗号化された接続を評価し、アクセス制御ルールに基づいてドロップまたは許可します。
- [ブロック（Block）]：接続をすぐに切断します。接続はアクセス制御ポリシーに渡されません。

ステップ 4 （オプション）デフォルト アクションのロギングを設定します。

デフォルトアクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベントビューアに記載されるようにするには、トラフィックのロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時（At End of Connection）]：接続の終了時にイベントを生成します。

- [接続イベントの送信先（Send Connection Events To）]：外部の syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバオブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバーの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバーへのロギングを無効にするには、サーバー リストから [任意（Any）] を選択します）。

  デバイスのイベント ストレージは限られているため、外部 syslog サーバーへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

- [ロギングなし（No Logging）]：イベントを生成しません。

ステップ 5 [保存（Save）] をクリックします。

SSL 復号ルールの設定

SSL 復号ルールを使用して、暗号化された接続を処理する方法を決定します。SSL 復号ポリシーに設定されたルールは、上から下への順に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

[SSLネイティブルール（SSL Native Rules）] セクションでのみルールを作成し、編集できます。

（注） SSL 復号ポリシーが接続を評価する前に、VPN 接続（サイト間とリモート アクセスの両方）のトラフィックが復号されます。したがって、SSL 復号ルールが VPN 接続に適用されることはなく、これらのルールを作成するときに VPN 接続を考慮する必要はありません。ただし、VPN トンネル内で暗号化された接続を使用する場合は評価されます。たとえば、RA VPN トンネル自体は（すでに復号されているので）評価されなくても、RA VPN 接続経由の内部サーバへの HTTPS 接続は、SSL 復号ルールによって評価されます。

始める前に

既知のキーの復号ルールを作成する場合は、宛先サーバーのための証明書とキーを（内部証明書として）アップロードし、証明書を使用するために SSL 復号ポリシーの設定も編集します。既知のキーのルールは通常、ルールの宛先ネットワークの条件で宛先サーバーを指定します。詳細については、既知のキーと復号の再署名の証明書の設定（559 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

（アクティブ認証アイデンティティ ルール用に自動的に生成されたもの以外に）任意の SSL 復号ルールを構成していない場合、[事前定義済みルールを追加（Add Pre-Defined Rules）] を

クリックして、事前定義済みのルールを追加できます。ルールを選択するように要求されます。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（  ）をクリックします。

ステップ 3 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

[SSLネイティブルール（SSL Native Rules）] セクションにのみルールを挿入できます。アイデンティティ ポリシーアクティブ認証ルールはアイデンティティ ポリシーから自動的に生成され、読み取り専用です。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+ . _ -

ステップ 5 一致するトラフィックに適用するアクションを選択します。

各オプションの詳細については、次を参照してください。

- 再署名の復号 （540 ページ）
- 既知のキーの復号 （541 ページ）
- 復号禁止 （542 ページ）
- ブロック （542 ページ）

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/送信先（Source/Destination）]：トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的ロケーション）、トラフィックで使用されている TCP ポート。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。SSL 復号ルールの送信元/送信先基準 （553 ページ）を参照してください。
- [アプリケーション（Application）]：アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトは

任意の暗号化されたアプリケーションです。SSL復号ルールのアプリケーション基準（554ページ）を参照してください。

- [URL]：Web 要求の URL カテゴリ。デフォルトでは URL カテゴリおよびレピュテーションはマッチングの目的では考慮されません。「SSL復号ルールのURL基準（555ページ）」を参照してください。
- [ユーザー（Users）]：アイデンティティ ソース、ユーザーまたはユーザー グループ。アイデンティティ ポリシーは、ユーザーとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。SSL 復号ルールのユーザー基準（556 ページ）を参照してください。
- [拡張（Advanced）]：SSL/TLS バージョンや証明書のステータスなどの接続に使用する証明書に由来する特性。SSL 復号ルールの詳細条件（558 ページ）を参照してください。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件を SSL 復号ルールに追加する際は、以下のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、URL カテゴリに基づいて復号するために単一のルールを使用できます。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはアプリケーション フィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。
- URL カテゴリのマッチングには、URL フィルタリング機能のライセンスが必要です。

ステップ 7 （オプション）ルールのロギングを設定します。

ルールと一致するトラフィックをダッシュボード データまたはイベント ビューアに含めるには、ロギングを有効にする必要があります。次のオプションから選択します。

- [接続終了時（At End of Connection）]：接続の終了時にイベントを生成します。
  - [接続イベントの送信先（Send Connection Events To）]：外部の syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバーの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバへのロギングを無効化するには、サーバのリストから [任意（Any）] を選択します）。

    デバイスのイベント ストレージは限られているため、外部 syslog サーバーへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

- [ロギングなし（No Logging）]：イベントを生成しません。

ステップ 8 [OK] をクリックします。

SSL 復号ルールの送信元/送信先基準

SSL 復号ルールの [送信元/送信先（Source/Destination）] 基準で、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的ロケーション）、トラフィックで使用されている TCP ポートを定義します。デフォルトでは、すべてのゾーン、アドレス、地理的ロケーション、TCP ポートが対象になります。TCP は、SSL 復号ルールに一致する唯一のプロトコルです。

条件を変更するには、その条件内の [+] ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、外部ホストから内部ホストへのすべてのトラフィックが復号されたことを確認したい場合、[送信元ゾーン（Source Zones）] で外部ゾーンを選択し、[送信先ゾーン（Destination Zones）] で内部ゾーンを選択します。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。

- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。

（注） 既知のキーの復号ルールの場合、証明書とアップロードしたキーを使用する送信先サーバーの IP アドレスを持つオブジェクトを選択します。

- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。SSL 復号ルールに対してのみ TCP プロトコルとポートを指定できます。

- TCP ポートからのトラフィックを一致させるには、[送信元ポート（Source Ports）] を設定します。
- TCP ポートへのトラフィックを一致させるには、[送信先ポート/プロトコル（Destination Ports/Protocols）] を設定します。
- 特定の TCP ポートから特定の TCP ポートへ発信されるトラフィックを一致させるには、両方のポートを設定します。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

SSL 復号ルールのアプリケーション基準

SSL 復号ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタ処理が定義されます。デフォルトは、SSL プロトコル タグを持つアプリケーションです。暗号化されていないアプリケーションは SSL 復号ルールと一致できません。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高くビジネスとの関連性が低いすべてのアプリケーションを復号またはブロックする SSL 復号ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションが復号またはブロックされます。

また、シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーション ディテクタを更新し追加します。これにより、リスクの高いアプリケーションのルールが新しいアプリケーションに自動的に適用される可能性があり、手動でルールを更新する必要がなくなります。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーション フィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタ リストを変更するには、条件内の [+] ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーション フィルタ オブジェクトを選択してから、ポップアップ表示されるダイアログボックスで [OK] をクリックします。いずれかのタブで [詳細フィルタ（Advanced Filte）] をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存（Save As Filter）] リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーション フィルタ オブジェクトとして保存します。

アプリケーション基準と、高度なフィルタを設定してアプリケーションを選択する方法の詳細については、アプリケーション フィルタ オブジェクトの設定（169 ページ）を参照してください。

SSL 復号ルールでアプリケーション基準を使用する場合は、次のヒントを考慮してください。

- このシステムでは、StartTLS を使用して暗号化される非暗号化アプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、TLS ClientHello メッセージ内の Server Name Indication、またはサーバー証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。
- システムは、サーバ証明書の交換後にのみアプリケーションを識別できます。SSL ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。この動作により、ハンドシェイクが完了し、アプリケーションを識別できるようになります。システムによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。
- 選択したアプリケーションが VDB の更新によって削除された場合は、アプリケーション名の後に「Deprecated（廃止）」が表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

SSL 復号ルールの URL 基準

SSL 復号ルールの URL の基準は、Web 要求の URL が属するカテゴリを定義します。また、復号、ブロック、または復号せずに許可するサイトの相対的なレピュテーションも指定できます。デフォルトでは、URL カテゴリに基づき接続と一致しません。

たとえば、すべての暗号化されたギャンブルサイトをブロックしたり、信頼できないソーシャル ネットワーキング サイトを復号したりできます。該当するカテゴリとレピュテーションのURLをユーザが参照しようとすると、セッションがブロックされるか、または復号されます。URL カテゴリの照合の詳細については、カテゴリ別とレピュテーション別の URL のフィルタリング （598 ページ）を参照してください。

[カテゴリ（Categories）] タブ

[+] をクリックし、目的のカテゴリを選択して、[OK] をクリックします。ポリシーからカテゴリやオブジェクトを削除するには、該当する [x] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべての URL にルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意（Any）] チェックボックスを選択解除し、[レピュテーション（Reputation）] スライダを使用してレピュテーション レベルを選択します。レピュテーション スライダの左側に復号なしで許可されるサイトが示され、右側に復号またはブロックされるサイトが示されます。レピュテーションがどのように使用されるかは、ルール アクションによって異なります。

- ルールで接続が復号またはブロックされる場合は、レピュテーション レベルを選択すると、そのレベルよりもシビラティ（重大度）が高いすべてのレピュテーションも選択されます。たとえば、**問題のあるサイト**（レベル2）を復号またはブロックするルールを設定する場合、**信頼できない**（レベル 1）サイトも自動的に復号またはブロックされます。
- ルールで復号なし（復号しない）で接続が許可される場合は、レピュテーション レベルを選択すると、そのレベルよりもシビラティ（重大度）が低いすべてのレピュテーションも選択されます。たとえば、**お気に入りのサイト**（レベル4）を復号しないルールを設定する場合、**信頼できる**（レベル 5）サイトも自動的に復号化されません。

レピュテーションが不明な URL をレピュテーション一致に含めるには、[レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] オプションを選択します。通常、新しいサイトは評価されていません。また、その他の理由でサイトのレピュテーションが不明である（または判断できない）場合もあります。

URL のカテゴリの確認

特定の URL のカテゴリとレピュテーションを確認できます。[確認するURL（URL to Check）] ボックスに URL を入力し、[移動（Go）] をクリックします。結果を表示するには、外部の Web サイトに移動します。分類に同意しない場合は、[URLカテゴリの異議を送信する（Submit a URL Category Dispute）] リンクをクリックしてお知らせください。

SSL 復号ルールのユーザー基準

SSL 復号ルールのユーザ基準は、IP 接続のユーザまたはユーザ グループを定義します。ルールにユーザまたはユーザ グループの基準を含めるように、アイデンティティ ポリシーと関連ディレクトリ サーバを設定する必要があります。

アイデンティティ ポリシーは、特定の接続に関してユーザー アイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストの IP アドレスに識別された

ユーザーが関連付けられます。したがって、送信元 IP アドレスがユーザーにマッピングされているトラフィックは、そのユーザーからのものとみなされます。IP パケット自体にはユーザー アイデンティティ情報は含まれていないため、この IP アドレスとユーザー間のマッピングが使用可能な中での最良近似となります。

1 つのルールに最大 50 のユーザーまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザーを選択するより有意義です。たとえば、外部ネットワークからエンジニアリンググループへのトラフィックを復号するルールを作成し、そのグループからの発信トラフィックを復号しない別のルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバーのエンジニアリング グループに追加するだけです。

そのソース内のすべてのユーザーに適用するアイデンティティ ソースを選択することもできます。したがって、複数の Active Directory ドメインをサポートしている場合は、ドメインに基づいて差分復号を提供できます。

ユーザー リストを変更するには、条件内の [+] ボタンをクリックし、次の手法のいずれかを使用して、目的のユーザーまたはユーザー グループを選択します。ポリシーからユーザーまたはグループを削除するには、対応する [x] をクリックします。

- [アイデンティティ ソース（Identity Sources）]：AD レルムやローカル ユーザー データベースなど、選択したソースから取得したすべてのユーザーにルールを適用するアイデンティティ ソースを選択します。必要なレルムがまだ存在しない場合、[新規アイデンティティ レルムの作成（Create New Identity Realm）] をクリックして作成します。
- [グループ（Groups）]：目的のユーザー グループを選択します。グループは、ディレクトリ サーバーにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセス ルールを作成し、それをアクセス コントロール ポリシー内で親グループのルールの上に配置する必要があります。
- [ユーザー（Users）]：個々のユーザーを選択します。ユーザー名には、Realm\username などのアイデンティティ ソースがプレフィックスとして付けられます。

  Special-Identities-Realm の下にはいくつかの組み込みユーザーがあります。

  - [認証失敗（Failed Authentication）]：ユーザーは認証を求められましたが、最大許容試行回数内に有効なユーザー名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザーのネットワークへのアクセスは妨げられませんが、これらのユーザーのネットワーク アクセスを制限するためのアクセス ルールを記述できます。
  - [ゲスト（Guest）]：ゲスト ユーザーは、これらのユーザーをゲストと呼ぶようにアイデンティティ ルールが設定されている点を除き、認証失敗ユーザーと同様です。ゲスト ユーザーは認証を求められましたが、最大試行回数内に認証されることができませんでした。
  - [認証不要（No Authentication Required）]：ユーザーの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザーは認証を求められませんでした。

- [不明（Unknown）]：IP アドレスのユーザーマッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

SSL 復号ルールの詳細条件

詳細のトラフィックの一致条件は、接続に使用する証明書に由来する特徴に関連します。次のオプションのいずれかまたはすべてを設定できます。

証明書のプロパティ

トラフィックは、選択したプロパティのいずれかに一致する場合、ルールの証明書プロパティのオプションに一致します。次の設定を行えます。

証明書のステータス

証明書が [有効（Valid）] か [無効（Invalid）] か。証明書のステータスを気にしない場合は、[任意（Any）]（デフォルト）を選択します。

証明書は、次の条件のすべてが満たされている場合に有効とみなされ、それ以外の場合は無効とみなされます。

- ポリシーが証明書を発行した CA を信用できる。
- 証明書の署名を証明書の内容に対して正しく検証できる。
- 発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。
- ポリシーの信頼できる CA のいずれも証明書を失効させていません。
- 現在の日付が証明書の [有効期間の開始（Valid From）] と [有効期間の終了（Valid To）] の期間内にある。

自己署名

サーバ証明書に同じサブジェクトおよび発行元識別名が含まれているかどうか。次のいずれかを選択します。

- [自己署名（Self-Signing）]：サーバー証明書は自己署名されています。
- [CA 署名（CA-Signing）]：サーバー証明書は認証局によって署名されています。つまり、発行元とサブジェクトは同じではありません。
- [任意（Any）]：証明書が自己署名されているかどうかを一致条件として考慮しません。

サポートされるバージョン

一致する SSL/TLS バージョン。ルールは、選択したいずれかのバージョンを使用するトラフィックにのみ適用されます。デフォルトは全バージョンです。**SSL 3.0**、**TLS 1.0**、**TLS 1.1**、**TLS 1.2**、**TLS 1.3** から選択してください。

たとえば、TLSv1.2/3 の接続のみを許可する場合は、それよりも低いバージョンにブロックルールを作成できます。

TLS 1.3 接続に一致させるには Snort 3 を使用している必要があります。

記載されていない SSL v2.0 などのバージョンを使用するトラフィックは、SSL 復号ポリシーのデフォルトのアクションによって処理されます。

SSL 復号設定の指定

トラフィックを復号するルールがある場合は、証明書設定を指定する必要があります。設定を変更して、暗号化されたトラフィックに復号を適用する方法を変更することもできます。以降のトピックでは、オプションについて説明します。

既知のキーと復号の再署名の証明書の設定

再署名によってまたは既知のキーを使用して復号を実装する場合は、SSL 復号ルールが使用できる証明書を特定する必要があります。すべての証明書が有効で、期限が切れていないことを確認します。

特に既知のキーを復号する場合は、復号する接続の各宛先サーバーの現在の証明書とキーがシステムにあることを確認する必要があります。既知のキーの復号ルールでは、復号の宛先サーバーからの実際の証明書とキーを使用します。したがって、常に 脅威に対する防御 デバイスに最新の証明書とキーがあることを確認する必要があります。そうでない場合、復号に失敗します。

既知のキーのルールで宛先サーバーの証明書またはキーを変更するたびに新しい内部証明書とキーをアップロードします。それらを内部証明書（内部 CA 証明書ではありません）としてアップロードします。次の手順の間に証明書をアップロードするか、**[オブジェクト（Objects）]**> **[証明書（Certificates）]** ページに進み、そこにアップロードします。

手順

ステップ 1 **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックします。

必要に応じて、[基本（Basic）] タブを選択します。

ステップ 3 [再署名証明書の復号（Decrypt Re-Sign Certificate）] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成（Create Internal CA）] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（⬇）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブ

ラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロード（561 ページ）も参照してください。

ステップ 4 既知のキーを使用して復号するルールごとに、宛先サーバの内部証明書とキーをアップロードします。

a) [既知のキーの証明書の復号（Decrypt Known-Key Certificates）] で [+] をクリックします。
b) 内部 ID の証明書を選択するか、[新しい内部証明書の作成（Create New Internal Certificate）] をクリックし、ここでそれをアップロードします。
c) [OK] をクリックします。

ステップ 5 （オプション）[信頼できるCA証明書（Trusted CA Certificates）] の下にある [+] をクリックし、ポリシーで信頼する証明書または証明書グループを選択します。

デフォルトグループの Cisco-Trusted-Authorities には、システム定義の信頼できる CA 証明書がすべて含まれています。この設定の変更が必要になる可能性のある主なケースは次のとおりです。

- デフォルトグループにない信頼できる CA 証明書を使用する場合。作成後、SSL 復号ポリシー設定でデフォルトグループと新しいグループの両方を選択します。これは、追加の信頼できる CA 証明書をアップロード済みの場合に実行できます。
- デフォルトグループにあるものよりも限定された信頼できる CA 証明書のリストを使用する場合。作成後、信頼できる証明書の完全なリスト（差分だけでなく）を持つグループを作成し、SSL 復号ポリシー設定で唯一のグループとして選択します。

ユーザーは、証明書の署名機関がこのリストに含まれていないサイトの証明書を受け入れるように求められます。証明書が信頼されていないという理由だけで、サイトへのアクセスがブロックされることはありません。

リストを空のままにするか、空の証明書グループのみを選択すると、SSL復号ポリシーはすべての証明書を信頼します。

ステップ 6 [保存（Save）] をクリックします。

高度なトラフィックおよび復号できないトラフィックの設定の指定

デフォルトの動作を使用しない場合は、高度な復号の設定と復号できないトラフィックの設定を指定できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [SSL復号設定（SSL Decryption Settings）] ボタン（⚙）をクリックします。

ステップ 3 [詳細（Advanced）] タブで、**TLS 1.3 復号**を有効にするかどうかを選択します。

TLS 1.3 復号を有効にする場合は、TLS 1.3 に適用する必要がある各ルールの [詳細（Advanced）] タブでも [TLS 1.3] オプションを選択する必要があります。TLS 1.3 を復号するには、Snort 3 を実行している必要があります。

ステップ 4 [復号化不可のアクション（Undecryptable Actions）] タブで、復号を実装するルールに一致するものの復号できない接続をシステムが処理する方法を変更します。

デフォルトでは、これらの接続にはデフォルトアクションと同じアクションが適用されます。例外は復号エラーの発生であり、それについてはブロックするかリセットによりブロックすることのみを選択できます。

これらのカテゴリの説明については、復号できないトラフィックの処理（542 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。

再署名の復号ルールの CA 証明書のダウンロード

トラフィックを復号する場合、ユーザは、TLS/SSL を使用するアプリケーションで信頼できるルート認証局として定義された暗号化プロセスで使用される、内部 CA 証明書を持っている必要があります。通常、証明書を生成した場合や、証明書をインポートした場合であっても、これらのアプリケーションで証明書がすでに信頼されているものとして定義されることはありません。大部分の Web ブラウザはデフォルトで、ユーザが HTTPS 要求を送信すると、Web サイトのセキュリティ証明書に問題があることを知らせる警告メッセージがクライアント アプリケーションから表示されます。通常、このエラー メッセージでは、Web サイトのセキュリティ証明書が信頼された認証局から発行されたものではないこと、または Web サイトが不明な認証局で証明されたものであることが示されますが、警告によって処理中に中間者攻撃の可能性があることが示唆される場合もあります。クライアントアプリケーションによっては、この警告メッセージがユーザに示されず、ユーザは承認されない証明書を受け入れることができません。

以下のいくつかの方法で、ユーザに必要な証明書を提供できます。

ルート証明書を受け入れるようにユーザに通知する

組織内のユーザに、企業の新しいポリシーについて通知し、組織が提供したルート証明書を、信頼できる認証局として受け入れるように指示できます。ユーザは証明書を受け入れ、信頼されたルート認証局のストレージエリアにそれを保存して、次にサイトにアクセスしたときにプロンプトが再度表示されないようにする必要があります。

（注） ユーザは、代替証明書を作成した CA 証明書を受け入れて、信頼する必要があります。そうではなく、単に代替サーバ証明書を信頼した場合は、異なる HTTPS サイトを訪問するたびに、警告が表示される状況が続きます。

クライアントデバイスにルート証明書を追加する

ネットワーク上のすべてのクライアントデバイスに、信頼できるルート認証局としてルート証明書を追加できます。そうすれば、クライアントアプリケーションは自動的にルート証明書を持つトランザクションを受け入れるようになります。

証明書を電子メールで送信するか、共有サイトに置くことで、ユーザが証明書を入手できるようにします。または、会社のワークステーションイメージに証明書を組み込み、アプリケーションの更新機能を使用して、ユーザに証明書を自動的に配布することもできます。

次に、内部 CA 証明書をダウンロードして、Windows クライアントにインストールする方法を説明します。

手順

ステップ 1 Device Manager から証明書をダウンロードします。

a) **[ポリシー（Policies）]** > **[SSL復号（SSL Decryption）]** の順に選択します。

b) [SSL復号設定（SSL Decryption Settings）] ボタン（  ）をクリックします。

c) [Download] ボタン（  ）をクリックします。

d) ダウンロード場所を選択して、必要に応じてファイル名を変更し（拡張子はそのまま）、[保存（Save）] をクリックします。

これで、[SSL復号設定（SSL Decryption Settings）] ダイアログ ボックスからキャンセルできます。

ステップ 2 クライアント システムの Web ブラウザにある信頼されたルート認証局のストレージ エリアに証明書をインストールするか、クライアント自体が証明書をインストールできるようにします。

プロセスは、オペレーティングシステムとブラウザの種類によって異なります。たとえば、Windows 上で実行されている Internet Explorer および Chrome の場合は次のプロセスを使用できます。（Firefox の場合は、**[ツール（Tools）]**>**[オプション（Options）]**>**[詳細（Advanced）]** ページでインストールします。）

a) [スタート（Start）] メニューから、**[コントロールパネル（Control Panel）]**>**[インターネットオプション（Internet Options）]** を選択します。

b) [Content] タブを選択します。

c) [証明書（Certificates）] ボタンをクリックして、[証明書（Certificates）] ダイアログ ボックスを開きます。

d) [信頼されたルート証明機関（Trusted Root Certification Authorities）] タブを選択します。

e) [インポート（Import）] をクリックし、ウィザードに従ってダウンロードされたファイル（<uuid>_internalCA.crt）を見つけて選択し、信頼できるルート認証局のストアに追加します。

f) [終了（Finish）] をクリックします。

メッセージは、インポートが成功したことを示しているはずです。ユーザがよく知られたサードパーティの認証局から証明書を取得するのではなく自己署名証明書を生成した場合は、途中で Windows が証明書を検証できなかったことを警告するダイアログ ボックスが表示される場合があります。

[証明書（Certificates）] ダイアログ ボックスと [インターネットオプション（Internet Options）] ダイアログ ボックスを閉じることができます。

例：ネットワークからの古いSSL/TLSバージョンのブロック

一部の組織では、政府の規制または会社のポリシーにより、古いバージョンのSSLまたはTLSの使用を禁止する必要があります。SSL復号ポリシーを使用して、禁止するSSL/TLSバージョンを使用するトラフィックをブロックできます。禁止されたトラフィックをすぐに捕捉できるようにするには、このルールをSSL復号ポリシーの先頭に配置することを検討してください。

次の例では、すべての SSL 3.0 および TLS 1.0 接続をブロックします。

始める前に

この手順では、SSL復号ポリシーがすでに有効になっていると仮定します（SSL 復号ポリシーの有効化 （548 ページ） を参照）。

手順

ステップ 1 **[ポリシー（Policies）] > [SSL復号（SSL Decryption）]** の順に選択します。

ステップ 2 [+] ボタンをクリックして、新しいルールを作成します。

ステップ 3 [順序（Order）] で、[1] を選択してルールをポリシーの先頭に配置するか、またはネットワークに最も適した数を選択します。

デフォルトでは、ルールはポリシーの最後に追加されます。

ステップ 4 [タイトル（Title）] に、ルールの名前（たとえば、Block_SSL3.0_and_TLS1.0）を入力します。

ステップ 5 [アクション（Action）] で、[ブロック（Block）] を選択します。これにより、ルールに一致するすべてのトラフィックが即座にドロップされます。

ステップ 6 [送信元/宛先（Source/Destination）]、[アプリケーション（Applications）]、[URL（URLs）]、[ユーザ（Users）] の各タブについては、すべてのオプションをデフォルト値のままにします。

ステップ 7 [詳細（Advanced）] タブをクリックし、[サポートされているバージョン（Supported Versions）] の下の [SSL 3.0] と [TLS 1.0] を選択したままにします。ただし、[TLS 1.1]、[TLS 1.2]、および [TLS 1.3] はオフにします。

ステップ 8 （任意）ブロックされた接続をダッシュボードやイベントに反映させるには、[ロギング（Logging）] タブをクリックし、[接続終了（At End of Connection）] を選択します。外部 syslog サーバーを使用している場合は、それを選択することもできます。

ステップ 9 [OK] をクリック

これでポリシーを展開できます。展開すると、システムを通過する SSL 3.0 または TLS 1.0 接続はドロップされます。

（注） SSL 2.0 接続は、ポリシーのデフォルトアクションによって処理されます。これらもドロップされるようにするには、デフォルトアクションを [ブロック（Block）] に変更します。

次のタスク

このルールを実装する場合、次の推奨事項があります。

- どのタイプの復号ルールでも、すべての SSL/TLS オプションが選択されている [詳細設定（Advanced）] タブはデフォルト設定のままにします。すべてのバージョンに適用することで、ハンドシェイクプロセスが簡素化されます。ただし、最初のブロックルールでは、SSL 3.0 および TLS 1.0 接続が引き続き妨げられます。
- 通常は、ポリシーのデフォルトアクションとして [復号しない（Do Not Decrypt）] を使用することをお勧めします。しかし、SSL 2.0 接続は常にデフォルトアクションによって処理されるため、代わりに [ブロック（Block）] を使用することもできます。ただし、すべての復号可能なトラフィックのデフォルトアクションとして [復号しない（Do Not Decrypt）] を適用する場合は、ポリシーの最後に [復号しない（Do Not Decrypt）] ルールを作成し、トラフィック一致基準のすべてのデフォルト値を受け入れます。このルールならば、テーブル内の以前のルールに一致しない、すべてのサポート対象の TLS 接続に一致し、それらの TLS バージョンにおけるデフォルトとして機能します。

SSL 復号のモニタリングとトラブルシューティング

ここでは、SSL 復号ポリシーのモニタリングおよびトラブルシューティング方法について説明します。

SSL 復号のモニタリング

ダッシュボードに復号についての情報を表示でき、ログ収集を有効化したルール（またはデフォルトのアクション）に一致するトラフィックのイベントを表示できます。

SSL 復号のダッシュボード

全体的な復号の統計情報を評価するには、**[モニタリング（Monitoring）] > [SSL復号（SSL Decryption）]** ダッシュボードを表示します。ダッシュボードには次の情報が表示されます。

- 暗号化されたトラフィックとプレーン テキスト トラフィックの割合。
- SSL ルールに従って、暗号化されたトラフィックがどの程度復号されたか。

イベン

ダッシュボードに加えて、イベント ビューア（**[モニタリング（Monitoring）]** > **[イベント（Events）]**）には、暗号化されたトラフィックの SSL 情報が含まれています。イベントの評価についていくつかのヒントを次に示します。

- 一致するトラフィックをブロックするSSLルール（またはデフォルトのアクション）と一致したためにドロップされた接続の場合、[アクション（Action）]は「ブロック」、[理由（Reason）] は「SSL ブロック」であることが必要です。
- [実際のSSLアクション（SSL Actual Action）] フィールドは、システムが接続に適用した実際のアクションを示します。これは、一致するルールに定義されたアクションを示す [予期されたSSLアクション（SSL Expected Action）] とは異なります。たとえば、接続が復号を適用するルールと一致しても、いくつかの理由で復号できないことがあります。

復号再署名がブラウザでは機能するがアプリでは機能しないWebサイトの処理（SSL または認証局ピニング）

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL（または認証局）ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、元のサーバー証明書のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが脅威に対する防御デバイスから再署名された証明書を受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Webサイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Webブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で https://www.facebook.com を指定すると接続に成功します。

SSL ピニングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

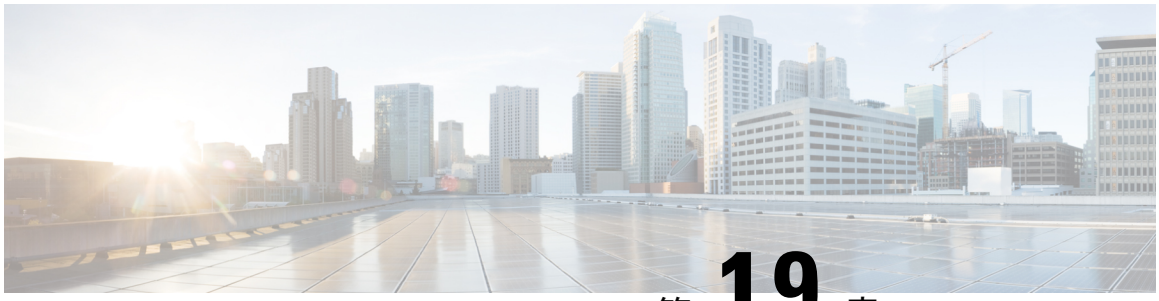
- アプリケーションのユーザをサポートします。この場合は、サイトへのトラフィックを復号できません。[SSL復号（SSL Decryption）] ルールの [アプリケーション（Application）] タブで、サイトのアプリケーションの [復号しない（Do Not Decrypt）] ルールを作成し、そのルールが、接続に適用される [再署名の復号（Decrypt Re-sign）] ルールの前に適用されることを確認します。
- ユーザにブラウザだけを使用させます。サイトへのトラフィックを復号する必要がある場合は、ネットワーク経由での接続にサイトのアプリケーションを使用できないため、ブラウザのみを使用しなければならないことをユーザーに通知する必要があります。

詳細

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実にSSL ピニングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピニングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション（Facebook など）は、サーバから SH、CERT、SHD メッセージを受け取るとすぐにSSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「Unknown CA (48)」アラートです。アラート メッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
  - SSL フロー フラグには ALERT_SEEN が含まれます。
  - SSL フロー フラグには APP_DATA_C2S または APP_DATA_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE です。
- グループ 2 のアプリケーション（Dropbox など）はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
  - SSL フロー フラグには ALERT_SEEN、APP_DATA_C2S または APP_DATA_S2C は含まれません。
  - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED です。



第 19 章

アイデンティティ ポリシー

アイデンティティポリシーを使用して、接続からユーザーアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザー グループに基づくアクセス コントロールを設定できます。

アイデンティティ ポリシーの概要

接続に関連付けられているユーザーを検出するためにアイデンティティ ポリシーを使用できます。ユーザーを識別することで、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザー ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザーに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。

たとえば、侵入イベントのターゲットとされたホストを誰が所有し、誰が内部攻撃やポート スキャンを開始したかを確認できます。また、高帯域幅のユーザーや、望ましくない Web サイトまたはアプリケーションにアクセスしているユーザーを確認することもできます。

ユーザーの検出は、分析用のデータを収集するだけではありません。ユーザ アイデンティティに基づいてリソースへのアクセスを選択的に許可またはブロックできるようユーザ名やユーザ グループ名に基づくアクセス ルールを作成することもできます。

ユーザ アイデンティティは、次の方法で取得できます。

- パッシブ認証：すべてのタイプの接続で、ユーザ名とパスワードを求められることなく、その他の認証サービスからユーザ アイデンティティを取得します。

- アクティブ認証：HTTP 接続でのみ、ユーザ名とパスワードの入力が求められ、送信元 IP アドレスのユーザ アイデンティティを取得するために指定のアイデンティティ ソースに対する認証が行われます。

ここでは、ユーザー アイデンティティについて詳しく説明します。

パッシブ認証によるユーザー アイデンティティの確立

パッシブ認証では、ユーザーにユーザー名とパスワードを求めることなくユーザー ID を収集します。システムは、指定したアイデンティティ ソースからマッピングを取得します。

ユーザと IP アドレスのマッピングは次のソースから受動的に取得できます。

- リモート アクセス VPN ログイン。パッシブ アイデンティティについては次のユーザ タイプがサポートされています。
  - 外部認証サーバで定義されたユーザ アカウント。
  - Device Manager で定義されたローカルユーザーアカウント。
- Cisco Identity Services Engine（ISE）、Cisco Identity Services Engine Passive Identity Connector（ISE PIC）。

特定のユーザーが複数のソースによって識別される場合は、RA VPN ID が優先されます。

アクティブ認証によるユーザー ID の確立

認証は、ユーザのアイデンティティを確認する動作です。

アクティブ認証を使用すると、HTTP トラフィック フローがユーザー ID のマッピングがないシステムの IP アドレスから送られてきたときに、ネットワークに設定されたディレクトリを使用して、トラフィック フローを開始したユーザーを認証するかどうかを決定できます。ユーザーが正常に認証された場合、IP アドレスは認証されたユーザーの識別情報を保持していると見なされます。

認証が失敗しても、ユーザーのネットワーク アクセスは妨げられません。アクセス ルールは最終的に、これらのユーザーにどのアクセスを提供するか決定します。

不明なユーザーの対処

アイデンティティ ポリシーのディレクトリ サーバーを設定すると、システムはディレクトリ サーバーからユーザーおよびグループ メンバーシップ情報をダウンロードします。この情報は、24 時間ごとに夜中に更新されるか、またはディレクトリ設定を編集して保存するたびに（変更がなくても）更新されます。

アクティブな認証アイデンティティ ルールによって求められた認証に成功したにも関わらず、ユーザー名がダウンロードしたユーザー ID 情報の中に存在しない場合、不明なユーザーとし

てマークされます。ID 関連のダッシュボードにそのユーザーの ID は表示されず、ユーザー一致グループ ルールにも検出されません。

ただし、不明なユーザーに対するアクセス コントロール ルールが適用されます。たとえば、不明なユーザーの接続をブロックすると、これらのユーザーは、たとえ認証に成功（ディレクトリ サーバーがユーザーとパスワードが有効であると認識したことを意味する）してもブロックされます。

そのため、ユーザーの追加や削除、グループ メンバーシップの変更などをディレクトリ サーバーに加えた場合、システムがディレクトリから更新情報をダウンロードするまで、これらの変更はポリシーの適用に反映されません。

真夜中の日次更新まで待てず、すぐに更新を適用させる必要がある場合は、ディレクトリのレルム情報を編集します（**[オブジェクト（Objects）]** > **[アイデンティティ ソース（Identity Sources）]** に移動し、レルムを編集する）。[保存（Save）] をクリックして、変更を展開します。システムはただちに更新情報をダウンロードします。

（注） 新規に追加したユーザー、または削除したユーザーの情報がシステムに反映されているかどうかを確認するには、**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択して、[ルールの追加(+)（Add Rule (+)）] ボタンをクリックします。[ユーザー（Users）] タブに表示されたユーザーのリストを確認してください。新規ユーザーを検出できないか、または削除されたユーザーが検出される場合、システムには古い情報があります。

アイデンティティ ポリシーを実装する方法

ユーザ アイデンティティの取得を有効にし、IP アドレスに関連付けられているユーザを認識させるには、いくつかの項目を設定する必要があります。正しく設定されている場合、監視ダッシュボードおよびイベントでユーザ名を確認できます。ユーザ アイデンティティは、アクセス制御ルールや SSL 復号化ルールでもトラフィック一致基準として使用できます。

次の手順では、アイデンティティ ポリシーを機能させるために設定する必要がある内容の概要を示します。

手順

ステップ 1 AD アイデンティティ レルムを設定します。

（ユーザ認証を要求して）ユーザ アイデンティティをアクティブに収集するか、またはパッシブに収集して、ユーザ アイデンティティ情報を含む Active Directory（AD）サーバを設定する必要があります。AD アイデンティティ レルムの設定 （195 ページ）を参照してください。

パッシブ ID を設定すると、複数の AD レルムの ID からシステムがプルできる AD レルム シーケンスを作成できます。この機能は、ネットワーク内に複数の AD ドメインがある場合に役立ちます。

ステップ 2 パッシブ認証アイデンティティ ルールを使用する場合は、パッシブ アイデンティティ ソースを設定します。

デバイスに実装しているサービスおよびネットワークで使用可能なサービスに基づき、次のいずれかを設定できます。

- リモートアクセス VPN：デバイスへのリモートアクセス VPN 接続をサポートする場合は、AD サーバーまたは（Device Manager に定義されている）ローカルユーザーに基づいて、ユーザーログイン時にアイデンティティを提供できます。RA VPN の設定方法については、リモート アクセス VPN の設定 （838 ページ）を参照してください。
- Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE PIC）：これらの製品を使用する場合は、デバイスを pxGrid サブスクライバとして設定し、ISE からユーザ アイデンティティを取得できます。「Identity Services Engine の設定 （206 ページ）」を参照してください。

ステップ 3 **[ポリシー（Policies）]>[アイデンティティ（Identity）]** を選択し、アイデンティティ ポリシーを有効にします。「アイデンティティ ポリシーの設定 （571 ページ）」を参照してください。

ステップ 4 アイデンティティ ポリシー設定の構成 （572 ページ）。

システムに設定しているソースに基づいて、パッシブ アイデンティティ ソースが自動的に選択されます。アクティブ認証を設定する場合は、キャプティブ ポータルおよび（SSL 復号ポリシーをまだ有効にしていない場合の）SSL 再署名復号用の証明書を設定する必要があります。

ステップ 5 アイデンティティ ポリシーのデフォルト アクションの設定 （575 ページ）。

パッシブ認証だけを使用する場合は、パッシブ認証に対するデフォルト アクションを設定でき、特定のルールを作成する必要はありません。

ステップ 6 アイデンティティ ルールの設定 （575 ページ）。

関連するネットワークからパッシブまたはアクティブ ユーザー アイデンティティを収集するルールを作成します。

アクティブ認証のベストプラクティス

アイデンティティ ルールにユーザのアクティブ認証が必要な場合、ユーザは接続されているインターフェイスのキャプティブ ポータル ポートにリダイレクトされ、その後、認証を要求されます。

このリダイレクションはインターフェイス IP アドレスに対するものなので、ID ポリシー証明書は正確には一致せず、ユーザーは信頼できない証明書エラーを受け取ります。続行してデバイスに対して認証されるには、ユーザーは証明書を受け入れる必要があります。この動作は中間者攻撃に似ているため、ユーザーは信頼できない証明書を受け入れることに消極的です。

この問題を回避するために、デバイス上の 1 インターフェイスの完全修飾ドメイン名（FQDN）を使用するようにアクティブ認証を設定できます。適切に設定された証明書を使用すると、

ユーザーは信頼できない証明書エラーを受け取ることがなくなり、認証がよりシームレスになり、安全性が向上します。

始める前に

アクティブ認証はHTTPトラフィックに対してのみ行われ、ユーザーのワークステーションや他のクライアントデバイスに対する最新のユーザーマッピングがデバイスにない場合は常に、エンドユーザーの作業が中断されます。代わりにパッシブ認証を実装することで、中断を回避できます。

手順

ステップ 1 DNSサーバーで、アクティブ認証を収集するために使用するインターフェイスのインターフェイス IP アドレスの完全修飾ドメイン名（FQDN）を定義します。

これはキャプティブポータルとも呼ばれ、ルーテッドインターフェイスである必要があります。

ステップ 2 認証局（CA）を使用して、この FQDN の証明書を取得します。

ftd1.captive-port.example.com など、特定の FQDN の証明書を作成できます。（任意）以下を実行できます。

- *.captive-port.example.com など、さまざまなデバイス上のキャプティブ ポータル インターフェイスに適用できるワイルドカード証明書を取得します。ワイルドカードの範囲を広くして、*.eng.example.com や *.example.com などの幅広いエンドポイントに適用できます。
- 証明書に複数のサブジェクト代替名（SAN）を含めます。

ステップ 3 **[オブジェクト（Objects）]** > **[証明書（Certificates）]** を選択し、証明書をアップロードします。

ステップ 4 **[オブジェクト（Objects）]** > **[ネットワーク（Network）]** を選択し、DNS 名の FQDN ネットワークオブジェクトを作成します。

ステップ 5 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** ページで、証明書と FQDN オブジェクトを使用して ID ポリシー設定を更新します。

ステップ 6 アクティブ認証を使用する ID ポリシーのルールを作成します。

アイデンティティ ポリシーの設定

アイデンティティポリシーを使用して、接続からユーザーアイデンティティ情報を収集できます。その後で、ダッシュボードにユーザーアイデンティティに基づく使用状況を表示し、ユーザーまたはユーザー グループに基づくアクセス コントロールを設定できます。

次に、アイデンティティ ポリシーでユーザー アイデンティティを取得するために必要な要素を設定する方法の概要を示します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** を選択します。

アイデンティティ ポリシーをまだ定義していない場合には、[アイデンティティポリシーを有効にする（Enable Identity Policy）] をクリックして、アイデンティティ ポリシー設定の構成（572 ページ）の説明のとおりに設定します。

ステップ 2 アイデンティティ ポリシーを管理します。

アイデンティティ設定を行うと、このページにすべてのルールが順番にリストアップされます。上から下に向かってルールがトラフィックと照合され、最初に適合したルールによって、適用されるアクションが決定されます。このページで次の操作を実行できます。

- アイデンティティ ポリシーを有効または無効にするには、[アイデンティティポリシー（Identity Policy）] トグルをクリックします。
- アイデンティティポリシー設定を変更するには、[アイデンティティポリシー設定（Identity Policy Configuration）] ボタン（  ）をクリックします。
- [デフォルトアクション（Default Action）] を変更するには、アクションをクリックして、希望のアクションを選択します。アイデンティティ ポリシーのデフォルト アクションの設定 （575 ページ）を参照してください。
- ルールを移動するには、編集して [順序（Order）] ドロップダウン リストから新しい場所を選択します。
- ルールを設定するには、次の手順を実行します。
  - 新しいルールを作成するには、[+] ボタンをクリックします。
  - 既存のルールを編集する場合は、（[操作（Actions）]列の）対象のルールの編集アイコン（  ）をクリックします。テーブルでプロパティをクリックして、選択的にルールのプロパティを編集することもできます。
  - 不要になったルールを削除する場合は、（[操作（Actions）] 列の）対象のルールの [削除（delete）] アイコン（  ）をクリックします。

アイデンティティ ルールの作成と変更の詳細については、アイデンティティ ルールの設定（575 ページ）を参照してください。

アイデンティティ ポリシー設定の構成

アイデンティティ ポリシーを機能させるには、ユーザ アイデンティティ情報を提供する送信元を設定する必要があります。必要な設定は、設定するルールのタイプ（パッシブ、アクティブ、または両方）によって異なります。

別のセクションで、設定ダイアログボックスにこれらの設定が表示されます。ダイアログボックスにアクセスする方法に応じて、両方のセクションが表示されるか、または片方のセクションだけが表示されます。構成済みの必要な設定を使用せずに認証タイプのルールを作成しようとすると、自動的にダイアログボックスが表示されます。

次の手順で、すべてのダイアログボックスについて説明します。

始める前に

ディレクトリ サーバー、Threat Defense デバイス、およびクライアント間で、時刻設定が一致していることを確認します。これらのデバイス間で時刻にずれがあると、ユーザ認証が成功しない場合があります。「一致」とは、別のタイムゾーンを使用できますが、たとえば、10 AM PST = 1 PM EST など、それらのゾーンに対して相対的に同じになっている必要があることを意味しています。

手順

ステップ 1 **[ポリシー（Policies）] > [アイデンティティ（Identity）]** を選択します。

ステップ 2 [アイデンティティポリシー設定（Identity Policy Configuration）] ボタン（  ）をクリックします。

ステップ 3 [パッシブ認証（Passive Authentication）] オプションを設定します。

ダイアログボックスに、設定済みのパッシブ認証ソースが表示されます。

必要に応じて、このダイアログボックスで ISE を設定できます。ISE オブジェクトを設定していない場合は、[ISEの統合（Integrate ISE）] リンクをクリックしてすぐに作成できます。オブジェクトが存在する場合は、状態（[有効（Enabled）] または [無効（Disabled）]）とともに表示されます。

パッシブ認証ルールを作成するには、少なくとも 1 つの有効なパッシブ アイデンティティ ソースを設定している必要があります。

ステップ 4 [アクティブ認証（Active Authentication）] オプションを設定します。

アイデンティティルールによりユーザーのアクティブ認証が要求されると、そのユーザーはキャプティブポータルポートにリダイレクトされ、認証を求められます。これらの設定を設定する前に、アクティブ認証のベストプラクティス （570 ページ）を読んでください。

- [サーバ証明書（Server Certificate）]：アクティブ認証時にユーザに提示する内部証明書を選択します。必要な証明書をまだ作成していない場合は、ドロップダウンリストの一番下にある [新しい内部証明書の作成（Create New Internal Certificate）] をクリックします。

  ブラウザが信頼している証明書をアップロードしない場合、ユーザは証明書を許可する必要があります。

- [ホスト名にリダイレクト（Redirect to Host Name）]（Snort 3.0 のみ）：アクティブな認証要求のキャプティブポータルとして使用するインターフェイスの完全修飾ホスト名を定義するネットワークオブジェクトを選択します。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。

FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。

アイデンティティルールによりユーザーのアクティブ認証が要求されているが、リダイレクト FQDN を指定していない場合、ユーザーは、接続されているインターフェイス上のキャプティブポータルポートにリダイレクトされます。

- [ポート（Port）]：キャプティブ ポータル ポート。デフォルトは、885（TCP）です。別のポートを設定する場合は、1025 ～ 65535 の範囲にする必要があります。

（注） [ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザーがキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してリダイレクトされます。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用する場合は、アクティブ認証が必要なすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバーを更新する必要もあります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。

ステップ 5 （アクティブ認証のみ）。[再署名証明書の復号（Decrypt Re-Sign Certificate）] で、再署名証明書での復号を実装するルールに使用するために内部 CA 証明書を選択します。

事前定義済みの NGFW-Default-InternalCA 証明書か、作成またはアップロードしたものを使用できます。証明書がまだ存在しない場合は、[内部CAを作成（Create Internal CA）] をクリックして作成します。

クライアントのブラウザに証明書をまだインストールしていない場合は、ダウンロードボタン（）をクリックしてコピーを入手します。証明書をインストールする方法については、各ブラウザのマニュアルを参照してください。再署名の復号ルールの CA 証明書のダウンロード（561 ページ）も参照してください。

（注） SSL 復号ポリシーをまだ構成していない場合にのみ SSL 復号の設定が求められます。ID ポリシーを有効にした後、これらの設定を変更するには、SSL 復号ポリシー設定を編集します。

ステップ 6 [保存（Save）] をクリックします。

アイデンティティ ポリシーのデフォルト アクションの設定

アイデンティティ ポリシーにはデフォルト アクションがあり、これは個別のアイデンティティ ルールに一致しない接続に実行されます。

実際には、ルールがないことがポリシーの有効な設定になります。すべてのトラフィックの送信元でパッシブ認証を使用する予定の場合は、単純にパッシブ認証をデフォルト アクションとして設定します。

手順

ステップ 1 **[ポリシー（Policies）] > [アイデンティティ（Identity）]** を選択します。

ステップ 2 [デフォルトアクション（Default Action）] をクリックして、次のいずれかを選択します。

- [パッシブ認証（任意のアイデンティティソース）（Passive Auth (Any Identity Source)）]：ユーザ アイデンティティは、任意のアイデンティティ ルールに一致しない接続に対して設定されたすべてのパッシブ アイデンティティ ソースを使用して特定されます。パッシブ アイデンティティ ソースを設定しない場合は、パッシブ認証をデフォルトとして使用すると [認証なし（No Auth）] を使用することと同じになります。
- [認証なし（認証不要）（No Auth (No Authentication Required)]：ユーザー アイデンティティは、任意のアイデンティティ ルールに一致しない接続について特定されません。

アイデンティティ ルールの設定

アイデンティティ ルールは、一致するトラフィックに対してユーザ識別情報を収集する必要があるかどうかを定義します。一致するトラフィックのユーザ識別情報を取得しない場合は、「認証なし」を設定します。

ルール設定に関係なく、アクティブ認証はHTTPトラフィックに対してのみ実行されることに注意してください。したがって、HTTP以外のトラフィックをアクティブ認証から除外するルールを作成する必要はありません。すべてのHTTPトラフィックに対してユーザ識別情報を取得する場合は、アクティブ認証ルールをすべての送信元および宛先に適用するだけで済みます。

（注） また、認証に失敗してもネットワーク アクセスには影響しません。アイデンティティ ポリシーは、ユーザ識別情報のみを収集します。認証に失敗したユーザがネットワークにアクセスできないようにするには、アクセス ルールを使用する必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アイデンティティ（Identity）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（  ）をクリックします。

ステップ 3 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。

ステップ 5 [Action] を選択し、必要に応じて [AD Identity Source] を選択します。

パッシブおよびアクティブ認証ルールのユーザ アカウントが含まれる AD アイデンティティ レルムを選択する必要があります。必要なレルムがまだ存在しない場合、[新規アイデンティティ レルムの作成（Create New Identity Realm）] をクリックして作成します。パッシブ認証では、単一の AD レルムオブジェクトではなく、AD レルムシーケンスを選択できます。

- [パッシブ認証（Passive Auth）]：パッシブ認証を使用して、ユーザ アイデンティティを判断します。設定されたすべてのアイデンティティ ソースが表示されます。ルールでは、設定されたすべてのソースが自動的に使用されます。
- [アクティブ認証（Active Auth）]：アクティブ認証を使用して、ユーザ アイデンティティを判断します。アクティブ認証はHTTP トラフィックのみに適用されます。他のタイプのトラフィックが、アクティブ認証を要求または許可するアイデンティティ ポリシーに適合した場合、アクティブ認証は試行されません。
- [認証なし（No Auth）]：ユーザ識別情報を取得しません。このトラフィックに、アイデンティティベースのアクセス ルールは適用されません。これらのユーザは、[認証不要（No Authentication Required）] とマークが付けられます。

ステップ 6 （アクティブ認証のみ）ディレクトリ サーバでサポートする認証方法（[タイプ（Type）]）を選択します。

- [HTTP基本（HTTP Basic）]：暗号化されていないHTTP 基本認証（BA）接続を使用して、ユーザを認証します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。これがデフォルトです。
- [NTLM]：NT LAN マネージャ（NTLM）接続を使用して、ユーザを認証します。この選択は AD レルムを選択するときにのみ使用できます。Windows ドメインのログインを使ってトランスペアレント認証が行われるよう、IE と Firefox ブラウザを設定することはできますが、ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします（トランスペアレント ユーザ認証の有効化（579 ページ）を参照してください）。

- [HTTPネゴシエート（HTTP Negotiate）]：ユーザ エージェント（トラフィック フローを開始するためにユーザが使用しているアプリケーション）方式とActive Directoryサーバ方式の間でデバイスがネゴシエーションできるようになります。ネゴシエーションの結果は、NTLM、ベーシックの順に、共通にサポートされ、使用されている最も強力な方式になります。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- [HTTP応答ページ（HTTP Response Page）]：システムが提供するWebページを使用して、ユーザに認証を求めるプロンプトを表示します。これは、HTTP 基本認証の 1 つの形式です。

（注） [ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定しない場合、HTTP 基本、HTTP 応答ページ、および NTLM 認証方式では、インターフェイスの IP アドレスを使用してユーザーがキャプティブポータルにリダイレクトされます。ただし、HTTP ネゴシエートでは、ユーザは完全修飾 DNS 名 *firewall-hostname.AD-domain-name* を使用してリダイレクトされます。[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を指定せずに HTTP ネゴシエートを使用する場合は、アクティブ認証が必要なすべての内部インターフェイスの IP アドレスにこの名前をマッピングするように DNS サーバーを更新する必要もあります。そうしないと、リダイレクトは実行できず、ユーザを認証できません。認証方式に関係なく一貫した動作を確保するために、[ホスト名にリダイレクト（Redirect to Host Name）] FQDN を常に指定することを推奨します。

ステップ 7 （アクティブ認証のみ）アクティブ認証に失敗したユーザをゲストユーザとしてラベル付けするかどうかを決めるには、**[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オン/オフ（On/Off）]** を選択します。

ユーザは、正常に認証する3つの機会が得られます。失敗した場合、このオプションの選択により、ユーザがどのようにマーク付けされるかが決まります。これらの値に基づき、アクセスルールを書き込みできます。

- **[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オン（On）]**：ユーザは [ゲスト（Guest）] としてマークされます。
- **[ゲストとしてフォールバック（Fall Back as Guest）]** > **[オフ（Off）]**：ユーザは [失敗した認証（Failed Authentication）] としてマークされます。

ステップ 8 [送信元/宛先（Source/Destination）] タブで、トラフィック一致基準を定義します。

アクティブ認証は、HTTP トラフィックに対してのみ試されることに注意してください。したがって、HTTP 以外のトラフィックに対して 「認証なし」のルールを設定は不要で、HTTP 以外のトラフィックに対してアクティブ認証ルールを作成するポイントもありません。ただし、パッシブ認証は任意のタイプのトラフィックに有効です。

アイデンティティ ルールの送信元/宛先基準は、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレス、または IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートを定義します。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次のトラフィック一致基準を設定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1つの基準を定義する 、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、内部ネットワークから発信されるすべてのトラフィックからユーザ識別情報を収集する場合、内部ゾーンを [送信元ゾーン（Source Zones）] として選択し、宛先ゾーンを空のままにします。

（注） 1 つのルールにパッシブ セキュリティ ゾーンとルーテッド セキュリティ ゾーンを混在させることはできません。さらに、パッシブセキュリティゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）] : 制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。

- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

  （注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、これにポートを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

ステップ 9 [OK] をクリックします。

トランスペアレント ユーザ認証の有効化

アクティブ認証を有効にするためにアイデンティティ ポリシーを設定する場合、ユーザ ID を取得するために次の認証方式を使用できます。

HTTP Basic

HTTP 基本認証では、ユーザは常に自分のディレクトリ ユーザ名とパスワードを認証するように要求されます。パスワードはクリアテキストで送信されます。そのため、基本認証はセキュアな認証形式とは見なされません。

基本認証は、デフォルトの認証メカニズムです。

HTTP 応答ページ

これは、HTTP 基本認証の一種であり、ユーザのログイン ブラウザ ページに表示されます。

NTLM、HTTP ネゴシエート（Active Directory のための統合 Windows 認証）

統合 Windows 認証は、実際にはユーザがドメインにログインしてワークステーションを使用するために利用されます。ブラウザは、アクティブ認証中の脅威に対する防御キャプティブ ポータルを含め、サーバへのアクセス時にこのドメイン ログインの使用を試みます。パスワードは送信されません。認証が成功すると、ユーザは何らかの認証チャレンジが実行されたことを意識せずに、トランスペアレント認証が行われます。

ブラウザがドメイン ログイン クレデンシャルを使用して認証要求を満たせない場合、ユーザは、ユーザ名とパスワードの入力を要求されますが、これは基本認証と同じユーザ エクスペリエンスです。したがって、統合 Windows 認証を設定した場合、同じドメイン内のネットワークまたはサーバにアクセスするときに、ユーザがクレデンシャルを入力する必要性を減らすことができます。

なお、HTTP ネゴシエートは、アクティブ ディレクトリ サーバとユーザ エージェントの両方がサポートする、最も強力な方式を選択することに注意してください。ネゴシエーションが認証方式としてHTTP基本認証を選択した場合、トランスペアレント認証は行われません。強度の順序は、NTLM、次に基本認証です。トランスペアレント認証を可能にするには、ネゴシエーションが NTLM を選択する必要があります。

トランスペアレント認証を有効にするには、統合 Windows 認証をサポートするようにクライアント ブラウザを設定する必要があります。以下に、統合 Windows 認証をサポートする、広く使用されている一部のブラウザに関して、一般的な要件と基本設定について説明します。ソフトウェア リリースごとに技術が変更される場合があるため、詳細情報についてはブラウザ（または他のユーザ エージェント）のヘルプを参照してください。

ヒント Chrome および Safari など、すべてのブラウザが統合 Windows 認証をサポートするとは限りません（このガイドのリリース時に使用可能だったバージョンに基づきます）。ユーザはユーザ名とパスワードの入力を要求されます。使用しているバージョンでサポートが使用可能かどうかを確認するには、ブラウザのマニュアルを参照してください。

トランスペアレント認証の要件

トランスペアレント認証を実装するには、ブラウザまたはユーザーエージェントを設定する必要があります。これは、個別に実行することも、そのための設定を作成し、ソフトウェア配布ツールを使用してその設定をクライアント ワークステーションにプッシュすることもできます。この作業をユーザーが自分で実行する場合は、ネットワークで機能する具体的な設定パラメータを提供する必要があります。

ブラウザまたはユーザ エージェントに関係なく、次の一般的な設定を実装する必要があります。

- 脅威に対する防御リダイレクトホスト名、またはユーザーがネットワークへの接続に使用するインターフェイスを [信頼済みサイト（Trusted Sites）] リストに追加します。リダイレクトホスト名を使用しない場合、IPアドレスか、使用可能な場合は完全修飾ドメイン名（inside.example.comなど）を使用できます。また、ワイルドカードまたはアドレスの一部

を使用して、汎用化された信頼済みサイトを作成できます。たとえば、一般的には *.example.com または単に example.com を使用してすべて内部サイトを網羅し、ネットワーク内のすべてのサイトを信頼できます（自身のドメイン名を使用）。インターフェイスの特定アドレスを追加する場合は、信頼済みサイトに複数のアドレスを追加して、ネットワークへのすべてのユーザーアクセスポイントに対処することが必要な場合があります。

- 統合 Windows 認証は、プロキシ サーバ経由で機能しません。したがって、プロキシを使用しないか、脅威に対する防御リダイレクトホスト名を追加するか、またはプロキシを経由しないアドレスにインターフェイスを追加する必要があります。プロキシを使用する必要がある場合、ユーザーは NTLM を使用する場合でも認証を要求されます。

ヒント　トランスペアレント認証の設定は必須ではありませんが、エンドユーザにとって便利です。トランスペアレント認証を設定しなかった場合、ユーザーはすべての認証方式に対するログインチャレンジを提示されます。

トランスペアレント認証用の Internet Explorer の設定

NTLM トランスペアレント認証を有効にするよう Internet Explorer を設定するには、次の手順を実行します。

手順

ステップ 1　[ツール（Tools）] > [インターネットオプション（Internet Options）] を選択します。

ステップ 2　[セキュリティ（Security）] タブを選択し、[ローカルイントラネット（Local Intranet）] ゾーンを選択した後、次の手順を実行します。

a) [サイト（Sites）] ボタンをクリックして、信頼できるサイトのリストを開きます。

b) 少なくとも次のオプションの 1 つが選択されていることを確認します。

- [イントラネットネットワークを自動的に検出する（Automatically detect intranet network）] このオプションを選択すると、他のすべてのオプションが無効になります。
- [プロキシをバイパスするすべてのサイトを含める（Include all sites that bypass the proxy）]

c) [詳細（Advanced）] をクリックして [ローカルイントラネットサイト（Local Intranet Sites）] ダイアログボックスを開き、次に信頼する URL を [サイトの追加（Add Site）] ボックスに貼り付けて [追加（Add）] をクリックします。

複数の URL が存在する場合は、このステップを繰り返します。ワイルドカードを使用して、**http://*.example.com** のように URL の一部を指定するか、または単に ***.example.com** と指定します。

このダイアログボックスを閉じて、[インターネットオプション（Internet Options）] ダイアログボックスに戻ります。

d) [ローカルイントラネット（Local Intranet）] が選択されたままの状態で、[カスタムレベル（Custom Level）] をクリックして [セキュリティ設定（Security Settings）] ダイアログボックスを開きます。**[ユーザー認証（User Authentication）]** > **[ログオン（Logon）]** 設定を探して、[自動ログオンをイントラネットゾーンのみで有効にする（Automatic logon only in Intranet zone）] を選択します。[OK] をクリック

ステップ 3 [インターネットオプション（Internet Options）] ダイアログボックスで [接続（Connections）] タブをクリックし、次に [LAN 設定（LAN Settings）] をクリックします。

[LANでプロキシ サーバーを使用する（Use a proxy server for your LAN）] が選択されている場合、脅威に対する防御インターフェイスがプロキシをバイパスすることを確認する必要があります。必要に応じて、次のいずれかを実行します。

- [ローカルアドレスにはプロキシサーバを使用しない（Bypass proxy server for local addresses）] を選択します。
- [詳細（Advanced）] をクリックして、アドレスを [次で始まるアドレスにはプロキシサーバーを使用しない（Do not use proxy server for addresses beginning with）] ボックスに入力します。たとえば、**`*.example.com`** のようにワイルドカードを使用できます。

トランスペアレント認証用の Firefox の設定

NTLM トランスペアレント認証を有効にするよう Firefox を設定するには、次の手順を実行します。

手順

ステップ 1 [about:config] を開きます。フィルタ バーを使用して、修正する必要のある設定を検索します。

ステップ 2 NTLM をサポートするには、次の設定を修正します（network.automatic でフィルタリング）。

- [network.automatic-ntlm-auth.trusted-uris] ：設定をダブルクリックし、URL を入力して [OK] をクリックします。カンマで区切って複数の URL を入力できます。プロトコルを含めるかどうかは任意です。次に例を示します。

```
http://host.example.com, http://hostname, myhost.example.com
```

URL の一部を使用することもできます。Firefox は、ランダムに部分文字列と照合するのではなく、文字列の末尾と照合します。したがって、ドメイン名のみ指定することにより、内部ネットワーク全体を包含することができます。次に例を示します。

```
example.com
```

- [network.automatic-ntlm-auth.allow-proxies] ：値が、デフォルトの [true] であることを確認します。値が [false] になっている場合は、ダブルクリックして変更します。

ステップ 3 HTTP プロキシ設定を確認します。これは、**[ツール（Tools）]**>**[オプション（Options）]** を選択し、次に [オプション（Options）] ダイアログボックスで [ネットワーク（Network）] タブをクリックすると見つかります。[接続（Connection）] グループで、[設定（Settings）] ボタンをクリックします。

- [プロキシなし（No Proxy）] が選択されている場合は、何も設定する必要がありません。
- [システムのプロキシ設定を使用（Use System Proxy Settings）] が選択されている場合、[about:config] 内の [network.proxy.no_proxies_on] プロパティを修正して、[network.automatic-ntlm-auth.trusted-uris] に含めた信頼済み URI を追加する必要があります。
- [手動プロキシ設定（Manual Proxy Configuration）] が選択されている場合、これらの信頼済み URI を包含するように [プロキシなし（No Proxy For）] リストを更新します。
- 他のオプションの 1 つが選択されている場合、これらの設定で使用するプロパティから同一の信頼済み URI が除外されていることを確認します。

アイデンティティ ポリシーのモニタリング

認証を必要とするアイデンティティ ポリシーが正常に動作している場合は、**[モニタリング（Monitoring）]**>**[ユーザー（Users）]** ダッシュボードやユーザー情報を含むその他のダッシュボードにユーザー情報が表示されます。

さらに、**[モニタリング（Monitoring）]**>**[イベント（Events）]** に表示されるイベントにもユーザー情報が含まれています。

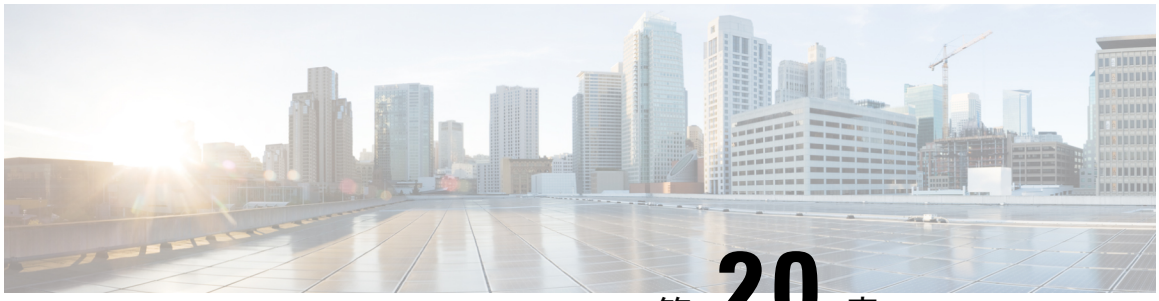
ユーザー情報が表示されない場合は、ディレクトリ サーバーが正常に機能していることを確認します。接続を確認するには、ディレクトリ サーバーの設定ダイアログ ボックスの [テスト（Test）] ボタンを使用します。

ディレクトリ サーバが機能し、使用可能である場合、アクティブ認証を必要とするアイデンティティルールのトラフィック一致条件が、ユーザを照合するように書かれていることを確認します。たとえば、送信元ゾーンに、ユーザー トラフィックがデバイスに入力するために経由するインターフェイスが含まれていることを確認します。アクティブ認証アイデンティティルールはHTTP トラフィックのみを照合するため、ユーザはデバイスを通じてそのタイプのトラフィックを送信している必要があります。

パッシブ認証の場合、そのソースを使用しているときは、ISE オブジェクトの [テスト（Test）] ボタンを使用します。リモート アクセス VPN を使用している場合は、サービスが正常に機能していることと、ユーザが VPN 接続を確立できることを確認します。問題の特定と解決の詳細については、これらの機能に関するトラブルシューティングのトピックを参照してください。

アイデンティティ ポリシーの例

使用例の章には、アイデンティティ ポリシーの実装例が含まれています。ネットワーク トラフィックを調べる方法 （55 ページ）を参照してください。



第 20 章

セキュリティ インテリジェンス

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。ここでは、セキュリティ インテリジェンスの実装方法について説明します。

セキュリティ インテリジェンスについて

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。システムは、この望ましくないトラフィックをアクセス制御ポリシーで評価する前にドロップすることにより、使用されるシステムリソースの量を減らします。

次のものに基づいてトラフィックをブロックできます。

- Cisco Talos Intelligence Group（Talos） フィード：Talos定期的に更新されるセキュリティ インテリジェンス フィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムはフィードの更新を定期的にダウンロードするため、設定を再導入する必要なく新しい脅威インテリジェンスを利用できます。

（注） Talos フィードはデフォルトで 1 時間ごとに更新されます。**[デバイス（Device）]** > **[更新（Updates）]** ページからは、更新頻度を変更するだけでなく、オンデマンドでフィードを更新することもできます。

- ネットワークおよびURL オブジェクト：ブロック対象の IP アドレスまたは URL が既知の場合は、それらのオブジェクトを作成し、それらをブロックリストまたは例外リストに追加することができます。FQDN または範囲指定によりネットワークオブジェクトを使用できないことに注意してください。

IP アドレス（ネットワーク）と URL で別のリストを作成します。

（注） HTTP/HTTPS リクエストの宛先が、ホスト名ではなく IP アドレスを使用する URL の場合は、ネットワークアドレスリストにある IP アドレスのレピュテーションが検索されます。ネットワークおよび URL リストで IP アドレスを重複させる必要はありません。

ブロックリストの例外の作成

ブロックリストごとに、関連する例外リスト（ブロック禁止リストとも呼ばれる）を作成できます。例外リストの唯一の目的は、ブロックリストに表示される IP アドレスまたは URL を除外することです。つまり、使用する必要があり、安全であることがわかっているアドレスや URL が、ブロックリストに設定されているフィードにある場合、ブロックリストから完全にカテゴリを削除せずに、そのネットワーク/URL を除外できます。

除外されたトラフィックは、以後アクセス コントロール ポリシーによって評価されます。接続が許可またはドロップされたかどうかの最終決定は、接続に一致するアクセス制御ルールに基づきます。また、アクセスルールは接続に侵入やマルウェア検査を適用するかどうかも判断します。

セキュリティ インテリジェンス フィード カテゴリ

次の表では、Cisco Talos Intelligence Group（Talos） フィードで使用可能なカテゴリについて説明します。これらのカテゴリは、ネットワークブロッキングと URL ブロッキングの両方で使用できます。

これらのカテゴリは時間とともに変化する可能性があるため、新しくダウンロードしたフィードのカテゴリが変更される場合があります。セキュリティインテリジェンスを設定する際は、カテゴリ名の横にある情報アイコンをクリックして説明を表示できます。

表 *10 : Cisco Talos Intelligence Group（Talos） フィードカテゴリ*

セキュリティインテリジェンス カテゴリ	説明
Attackers	悪意のある発信アクティビティが知られているアクティブスキャナやホスト
Banking_fraud	電子バンキングに関連する詐欺行為を行うサイト
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス

セキュリティインテリジェンス カテゴリ	説明
Bots	バイナリ マルウェア ドロッパを有するサイト
CnC	botnets 用のホスト C & C サーバーを有するサイト
Cryptomining	プールと財布へのリモートアクセスを提供するホスト (cryptocurrency のマイニングのため)
Dga	C & C サーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
High_risk	セキュリティグラフからの OpenDNS 予測セキュリティアルゴリズムと一致するドメインとホスト名
Ioc	侵害の兆候（IOC）に関与していることが観察されているホスト
Link_sharing	権限のないファイルを共有する web サイト
Malicious	他のより詳細な脅威カテゴリに必ずしも適合しているわけではない、悪意のある動作を示しているサイト
マルウェア	マルウェアバイナリまたはエクスプロイト キットを有するサイト
Newly_seen	最近登録されたドメイン、またはテレメトリでまだ認識されていないドメイン **注目** 現在、このカテゴリにはアクティブなフィードがなく、将来の使用のために予約されています。
Open_proxy	匿名の web ブラウジングが可能な公開プロキシ
Open_relay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシング ページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL
Spam	スパムを送信することが知られているメール ホスト
Spyware	スパイウェアおよびアドウェアのアクティビティを含む、提供する、またはサポートすることが知られているサイト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル

セキュリティインテリジェンス カテゴリ	説明
Tor_exit_node	Torアノニマイザーネットワークの出口ノードサービスを提供することが知られているホスト

セキュリティインテリジェンスのためのライセンス要件

セキュリティ インテリジェンスを使用するには、**IPS** ライセンスを有効にする必要があります。オプション ライセンスの有効化または無効化 （109 ページ） を参照してください。

セキュリティ インテリジェンスの設定

セキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティ インテリジェンスを使用するには、IPS ライセンスを有効にする必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[セキュリティインテリジェンス（Security Intelligence）]** の順に選択します。

ステップ 2 ポリシーが有効になっていない場合は、[セキュリティインテリジェンスの有効化（Enable Security Intelligence）] ボタンをクリックします。

[セキュリティインテリジェンス（Security Intelligence）] をクリックして [オフ（Off）] にすることで、いつでもポリシーを無効にできます。設定は維持されるため、ポリシーを再度有効にするときに再設定する必要はありません。

ステップ 3 セキュリティ インテリジェンスを設定します。

ネットワーク（IP アドレス）と URL には別々のブロックリストがあります。

a) [ネットワーク（Network）] または [URL] タブをクリックして、設定するリストを表示します。

b) ブロック/ドロップリストで、[+] をクリックして、接続をすぐにドロップするオブジェクトまたはフィードを選択します。

オブジェクトセレクタは、種類によってオブジェクトおよびフィードを別々のタブに整理します。希望するオブジェクトがまだ存在しない場合、リストの下部にある [新しいオブジェクトの作成（Create New Object）] リンクをクリックして作成します。Cisco Talos Intelligence Group（Talos） フィードの説明については、フィードの横にある [i] ボタンをク

リックします。セキュリティインテリジェンス フィードカテゴリ （586ページ）も参照してください。

（注） セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。これには、any-ipv4 と any-ipv6 のネットワーク オブジェクトが含まれます。ネットワークのブロックのためにこれらのオブジェクトを選択しないでください。

c) 非ブロックリストで、[+] をクリックし、ブロックリストの例外をすべて選択します。

このリストを設定する唯一の理由は、ブロックリストにある IP アドレスまたは URL を例外にすることです。適用除外された接続は、その後アクセス制御ポリシーによって評価され、いずれにしても破棄される可能性があります。

d) 他のブロックリストを設定するには上記の手順を繰り返します。

ステップ 4 （オプション）[ログ設定の編集（Edit Logging Settings）] ボタン（⚙）をクリックしてロギングを設定します。

ロギングを有効にした場合は、ブロックリストのエントリに一致するものが記録されます。ロギングを有効にして、除外された接続がアクセス制御ルールに一致した場合、ログ メッセージは取得しますが例外エントリに一致するものは記録されません。

次を設定します。

- [接続イベントロギング（Connection Events Logging）]：クリックしてロギングを有効または無効に切り替えます。
- [Syslog]：外部の syslog サーバーにイベントのコピーを送信するには、このオプションを選択して、syslog サーバーを定義するサーバー オブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しいSyslogサーバーの追加（Add Syslog Server）] をクリックして作成します。

  デバイスのイベント ストレージは限られているため、外部 syslog サーバーへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

セキュリティ インテリジェンスのモニタリング

セキュリティ インテリジェンス ポリシーのログ記録を有効にすると、システムは、ブロックリストの項目に一致する接続ごとにセキュリティ インテリジェンス イベントを生成します。これらの接続に一致する接続イベントがあります。

ドロップされた接続の統計情報は、[モニタリング（Monitoring）] ページの、使用可能なさまざまなダッシュボードに表示されます。

[モニタリング（Monitoring）] > **[アクセスおよびSIルール（Access and SI Rules）]** ダッシュボードに、トラフィックと一致する、上位のアクセス ルールとセキュリティ インテリジェンスに相当するルールが表示されます。

さらに、**[モニタリング（Monitoring）]** > **[イベント（Events）]**、次に [セキュリティインテリジェンス（Security Intelligence）] を選択して、セキュリティ インテリジェンス イベントと、関連する接続イベントを [接続（Connection）] タブに表示できます。

- イベントの [SIカテゴリID（SI Category ID）] フィールドは、ネットワークまたは URL オブジェクトあるいはフィードなど、ブロックリストに一致するオブジェクトを示します。
- 接続イベントの [理由（Reason）] フィールドは、イベントに表示されたアクションが適用された理由について説明します。たとえば、ブロックアクションは、IP ブロックまたは URL ブロックなどの理由と組み合わされて、接続がセキュリティ インテリジェンスによってドロップされたことを示します。

セキュリティ インテリジェンスの例

使用例の章には、セキュリティ インテリジェンス ポリシーの実装例が含まれています。脅威をブロックする方法 （64 ページ）を参照してください。

第 21 章

アクセス コントロール

ここでは、アクセス コントロール ルールについて説明します。これらのルールにより、デバイスを通過するトラフィックが制御されるとともに、侵入インスペクションなどの高度なサービスがトラフィックに適用されます。

アクセス制御のベストプラクティス

アクセス制御ポリシーは、内部ネットワークを保護し、ユーザーが望ましくない外部ネットワークリソース（不適切なWebサイトなど）にアクセスすることを防止するための主要なツールです。そのため、このポリシーに特に注意を払い、必要な保護と接続のレベルを得るためにポリシーを微調整することをお勧めします。

次の手順は、アクセス制御ポリシーを使用する場合に実行する必要がある基本的なことの概要を示しています。これは概要であり、各タスクを実行するための完全な手順は示していません。

アクセス制御ポリシーにアクセスするには、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

手順

ステップ 1 ポリシーのデフォルト アクションを設定します。

デフォルトアクションでは、ポリシー内の特定のルールに一致しない接続が処理されます。デフォルトでは、このアクションは [ブロック（Block）] であるため、ルールに含まれていない

ものはすべてブロックされます。そのため、必要なトラフィックを許可するアクセス制御ルールを作成するだけで済みます。これは、アクセス制御ポリシーを設定する従来の方法です。

反対に、デフォルトでトラフィックを許可して既知の望ましくないトラフィックをドロップするルールを作成することができます。この場合、許可するすべてのものに関するルールを用意する必要がなくなります。これにより、新しいサービスの使用が容易になりますが、気付かないうちに新しい望ましくないトラフィックが通過するリスクが生じます。

ステップ 2 [アクセスポリシーの設定（Access Policy Settings）]（⚙）ボタンをクリックし、[TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] オプションを有効にします。

このオプションにより、TLS 1.3 接続の最初のアプリケーション検出と URL カテゴリおよびレピュテーションの識別が改善されます。このオプションを有効にしないと、TLS 1.3 トラフィックが意図したルールと一致しない可能性があります。また、このオプションを有効にすることにより、復号ルールの有効性が向上する可能性もあります。

ステップ 3 できるだけ少ないアクセス制御ルールを作成します。

従来のファイアウォールでは、IP アドレスとポートのさまざまな組み合わせに対して何万ものルールが作成される場合があります。次世代ファイアウォールでは、高度な検査を使用して、これらの詳細なルールの一部を回避できます。ルールの数が少ないほど、トラフィックが速く評価されるようになり、ルールセット内の問題を見つけて修正することも容易になります。

ステップ 4 アクセス制御ルールのロギングを有効にします。

ロギングを有効にした場合にのみ、一致するトラフィックの統計が収集されます。ロギングを有効にしないと、モニタリングダッシュボードが不正確になります。

ステップ 5 より固有性の高いルールをポリシーの上の方に配置し、固有性の高いルールも一致する接続と一致する、より一般的なルールが、それらの固有性の高いルールよりも下になっていることを確認します。

ポリシーはトップダウンで評価され、最初の一致が優先されます。そのため、特定のサブネットへのすべてのトラフィックをブロックするルールを配置し、その後にそのサブネット内の単一 IP アドレスへのアクセスを許可するルールを配置しても、最初のルールによってブロックされるため、そのアドレスへのトラフィックは許可されません。

また、入力/出力インターフェイス、送信元/宛先 IP アドレス、ポート、地理位置情報などの従来の基準のみに基づいてトラフィックを評価するルールは、ユーザー基準、URL フィルタリング、アプリケーションフィルタリングなどに適用される、詳細な検査が必要なルールの前に配置してください。前者のルールは検査を必要としないため、それらのルールを前に配置することにより、接続の一致に関するアクセス制御の決定を迅速に行うことが可能になります。

その他の推奨事項については、アクセス制御ルールの順序のベスト プラクティス （607 ページ）を参照してください。

ステップ 6 トラフィックのターゲットサブセットに対するブロックルールと許可ルールをペアで設定します。

たとえば、多くの HTTP/HTTPS トラフィックを許可する一方で、望ましくないサイト（ポルノサイトやギャンブルサイトなど）へのアクセスをブロックしたい場合があります。これを実

現するには、次のルールを作成し、それらをポリシー内で順番に並べます（たとえば、ルール 11 とルール 12）。

- 内部セキュリティゾーン（送信元）および外部セキュリティゾーン（宛先）と、IPアドレス、ポート、または地理位置情報に適用される、望ましくない URL カテゴリを対象とした URL フィルタリング ブロック ルール。たとえば、ボットネット、児童虐待コンテンツ、クリプトジャッキング、DNS トンネリング、電子バンキング詐欺、エクスプロイト、エクストリーム、フィルタ回避、ギャンブル、ハッキング、ヘイトスピーチ、ハイリスクのサイト/場所、違法行為、違法ダウンロード、違法薬物、悪意のあるサイト、マルウェアサイト、モバイル脅威、P2P マルウェアノード、フィッシング、ポルノ、スパム、スパイウェア、およびアドウェアをブロックします。
- 内部セキュリティゾーン（送信元）および外部セキュリティゾーン（宛先）と、IPアドレス、ポート、または地理位置情報に適用される、HTTP および HTTPS アプリケーションのアプリケーションフィルタ処理許可ルール。この URL フィルタ処理ルールでは、望ましくない Web リソースへのアクセスをブロックした後、他のすべての HTTP/HTTPS アクセスが許可されます。

ステップ 7 高度な次世代ファイアウォール機能を使用して、IPアドレスやポートに関係なくトラフィックが評価されます。

攻撃者やその他の悪意のある人物は、IPアドレスとポートを頻繁に変更することにより、従来のアクセス制御トラフィックの一致基準を回避します。代わりに、次の次世代機能を使用してください。

- ユーザー基準：トラフィックを開始しているユーザーに関する情報を取得するようにアイデンティティポリシーを設定します。理想的には、Active Directory サーバーがユーザーをグループに編成します。これによって、ユーザー グループ メンバーシップに基づいてトラフィックを許可またはブロックするアクセス制御ルールを作成できます。たとえば、エンジニアユーザーには開発サブネットへのアクセスを許可しますが、エンジニアグループに属していないユーザーは暗黙的にブロックします。個別のユーザー名ではなくグループを使用するため、ユーザーがネットワークに追加されるたびにルールを更新する必要がありません。
- アプリケーション基準：アプリケーションフィルタ処理基準を使用して、アプリケーションのタイプを許可またはブロックします。これにより、ユーザーが HTTP 接続のポートを変更した場合、システムは、ポート 80 に接続していなくても HTTP であることを認識できます。その他の推奨事項については、アプリケーション フィルタリングのベスト プラクティス （597 ページ）を参照してください。
- URL カテゴリおよびレピュテーション基準：カテゴリに基づく URL フィルタ処理を使用して、サイトのタイプに基づいてサイトを動的に許可またはブロックします。サイトのタイプ（またはカテゴリ）内で、サイトのレピュテーション（正常または危険）に基づいてルールを微調整できます。URL によってサイトを手動でブロックしようとする場合には URL が変更されるたびにルールを調整する必要がありますが、カテゴリとレピュテーションを使用することにより、そのような調整が不要になります。その他の推奨事項については、効果的な URL フィルタリングのベスト プラクティス （602 ページ）を参照してください。

URL カテゴリ/レピュテーション フィルタリング ルールを DNS ルックアップ要求の FQDN に適用することもできます。システムは、ブロックされたカテゴリ/レピュテーションに対する DNS 応答を防止し、ユーザーの接続試行を効果的にブロックできます。詳細については、URL カテゴリとレピュテーションに基づいた DNS 要求のフィルタリング （605 ページ）を参照してください。

ステップ 8 すべての許可ルールに侵入検査を適用します。

次世代ファイアウォールの強力な機能の一つは、同じデバイスを使用して侵入検査とアクセス制御を適用できることです。侵入ポリシーを各許可ルールに適用してください。これにより、攻撃が通常は害のないパスを介してネットワークに侵入した場合でも、それを察知して攻撃接続をドロップできます。

デフォルトアクションが「許可」の場合は、デフォルトアクションに一致するトラフィックに侵入防御を適用することもできます。

ステップ 9 また、望ましくない IP アドレスおよび URL をブロックするようにセキュリティ インテリジェンス ポリシーを設定します。

セキュリティ インテリジェンス ポリシーはアクセス制御ポリシーの前に適用されるため、アクセス制御ルールが評価される前に望ましくない接続をブロックできます。これにより早い段階でのブロックを実現でき、アクセス制御ルールの複雑さを軽減するために役立ちます。

ステップ 10 SSL 復号ポリシーの実装を検討します。

システムは、暗号化されたトラフィックに対して詳細な検査を実行できません。SSL 復号ポリシーを設定すると、アクセス制御ポリシーが復号されたバージョンのトラフィックに適用されます。そのため、詳細な検査によって攻撃を識別でき（侵入ポリシーを使用）、アプリケーションおよび URL フィルタリングをより効果的に適用できるため、ルールの照合が強化されます。アクセス制御ポリシーで許可されたトラフィックは、デバイスから送信される前に再暗号化されるため、エンドユーザーが暗号化の保護を失うことはありません。

ステップ 11 オブジェクトグループ検索を有効にして、ルールの展開を簡素化します。

リリース 7.2 以降、この機能は新しい展開ではデフォルトで有効になっていますが、アップグレードされたシステムでは自動的に有効になりません。

オブジェクトグループ検索を有効にすると、ネットワークオブジェクトを含むアクセス コントロール ポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU 使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセス コントロール ポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

FlexConfig を使用してこのオプションを設定するには、**object-group-search access-control** コマンドを発行します。否定テンプレートでは、このコマンドの **no** 形式を使用します。

アクセス コントロールの概要

次に、アクセス コントロール ポリシーを説明します。

アクセス コントロール ルールとデフォルト アクション

ネットワーク リソースへのアクセスを許可またはブロックするには、アクセス コントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。

アクセスの制御は次に基づいて行われます。

- 送信元と宛先の IP アドレス、プロトコル、ポート、インターフェイスなど従来のネットワーク特性（セキュリティ ゾーンの形式で）。
- 送信元と宛先の完全修飾ドメイン名（FQDN）（ネットワーク オブジェクトの形式）。トラフィックの照合は、その名前に関して DNS ルックアップから返された IP アドレスに基づいて行われます。
- Cisco Identity Services Engine（ISE）によって送信元または宛先に割り当てられたセキュリティグループタグ（SGT）。
- 使用されているアプリケーション。アクセス コントロールは特定のアプリケーションに基づいて行うことも、アプリケーションのカテゴリ、特定の特性がタグ付けされたアプリケーション、アプリケーションのタイプ（クライアント、サーバー、Web）、またはアプリケーションのリスクやビジネスとの関連性の格付けを対象とするルールを作成できます。
- 汎用的な URL のカテゴリが含まれる Web 要求の宛先 URL。ターゲット サイトのパブリック レピュテーションに基づいて、カテゴリの一致を絞り込むことができます。
- DNS ルックアップ要求の FQDN の URL カテゴリとレピュテーション。不要なカテゴリや低いレピュテーションに対して DNS 応答をブロックして、その後の接続試行を効果的に防ぐことができます。
- 要求を作成したユーザ、またはユーザが所属するユーザ グループ。

ユーザーが許可する暗号化トラフィックの場合、IPSインスペクションを適用して脅威をチェックし、攻撃だと思われるトラフィックをブロックできます。また、禁止されたファイルやマルウェアをチェックするためにファイル ポリシーも使用できます。

アクセス ルールに一致しないすべてのトラフィックは、アクセス コントロールの [デフォルト アクション（Default Action）] によって処理されます。デフォルトでトラフィックを許可する場合は、侵入インスペクションをトラフィックに適用できます。ただし、デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。

アプリケーション フィルタリング

アクセス コントロール ルールを使用すると、接続で使用されるアプリケーションに基づいてトラフィックをフィルタリングできます。このシステムはさまざまアプリケーションを認識できるため、すべての Web アプリケーションをブロックせずに 1 つの Web アプリケーションをブロックする方法を探す必要はありません。

人気のあるアプリケーションでは、アプリケーションのさまざまな要素にフィルタ処理を行えます。たとえば、Facebook をブロックせずに、Facebook Games をブロックするルールを作成できます。

一般的なアプリケーション特性に基づいて、リスクまたはビジネスとの関連性、タイプ、タグを選択することでアプリケーション グループ全体をブロックまたは許可するルールを作成できます。**ただし、アプリケーション フィルタでカテゴリを選択するときは、目的のアプリケーション以外を含まないように一致するアプリケーションのリストをよく確認してください。**可能なグループ処理の詳細については、アプリケーション基準（619 ページ）を参照してください。

暗号化および復号トラフィックのアプリケーション制御

アプリケーションが暗号化を使用する場合、システムはアプリケーションを識別できない場合があります。

システムは StartTLS（SMTPS、POPS、FTPS、TelnetS、IMAPSなど）で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバー証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーション フィルタのダイアログボックスを使用し、次のタグを選択することでアプリケーションに復号が必要かどうかを決定してから、アプリケーションのリストを確認します。

- [SSLプロトコル（SSL Protocol）]：SSL プロトコルとしてタグ付けされたトラフィックを解釈する必要はありません。システムはこのトラフィックを認識し、アクセス コントロール操作を適用できます。リストされたアプリケーションのアクセス コントロール ルールは、想定される接続に一致する必要があります。
- [復号されたトラフィック（Decrypted Traffic）]：最初にトラフィックを復号する場合のみ、システムがこのトラフィックを特定できます。このトラフィックにSSL復号ルールを設定します。

Common Industrial Protocol（CIP）および Modbus アプリケーション（ISA 3000）でのフィルタリング

Cisco ISA 3000 デバイスで Common Industrial Protocol（CIP） および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write のように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。

プリプロセッサを有効にするには、CLIセッション（SSHまたはコンソール）でエキスパートモードに移行し、次のコマンドを発行して、これらの遠隔モニター制御 情報取得（SCADA）アプリケーションの一方または両方を有効にする必要があります。

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

たとえば、両方のプリプロセッサを有効にするには次の手順を実行します。

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

（注） このコマンドは、展開のたびに発行する必要があります。これらのプリプロセッサは、展開時には無効になります。

アプリケーション フィルタリングのベスト プラクティス

アプリケーションフィルタリングのアクセス制御ルールを設計する際は、次の推奨事項を覚えておいてください。

- アドバタイズメント トラフィックなどの Web サーバーによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。
- アプリケーションと URL の基準を同じルールで組み合わせることは避けてください（特に暗号化されたトラフィックの場合）。
- [復号トラフィック（Decrypted Traffic）] のタグが付けられたトラフィックにルールを作成する場合、一致するトラフィックを復号するSSL復号ルールがあることを確認します。これらのアプリケーションは、復号された接続でのみ識別できます。
- TLS 1.3 では、ほとんどのハンドシェイクメッセージが暗号化されるため、証明書情報を簡単に利用できません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに効果的に対応するには、システムがサーバーのクリアテキスト証明書を取得する必要があります。アクセス制御設定で [TLS 1.3証明書の可視性（TLS 1.3 Certificate Visibility）] を有効にすることをお勧めします。このオプションを有効にすると、システムは、クライアントの Hello パケットの IP アドレスおよび SNI（Server Name Indication）に基づいて、サイトの証明書がキャッシュに保存されているかどうかを確認します。保存されていない場合、システムは、TLS 1.2 プローブを使用して証明書を取得します。その後は、この証明書を使用して、接続を復号せずにアプリケーション/URL カテゴリおよびレピュテーションを識別することができます。
- システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skype トラフィックを制御するには、個々のアプリケーションを選択する代わりに、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。

- Zoho メールへのアクセスを制御するには、Zoho アプリケーションと Zoho Mail アプリケーションの両方を選択します。

URL フィルタリング

アクセス制御ルールを使用して、HTTP または HTTPS 接続に使用される URL に基づいてトラフィックをフィルタ処理できます。HTTPS は暗号化されるので、HTTP の URL フィルタリングは HTTPS の URL フィルタリングよりも簡単なものであることに注意してください。

次の手法を使用して、URL フィルタリングを実装できます。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリングライセンスにより、URL の一般的な分類（カテゴリ）とリスクレベル（レピュテーション）に基づいて、Web サイトへのアクセスを制御できます。これは、不要なサイトをブロックするのに最も簡単で効果的な方法です。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL および URL のグループを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。手動フィルタリングの主な目的はカテゴリベースのブロック ルールに例外を作成することですが、他の目的にも手動ルールを使用できます。

ここでは、URL フィルタリングについてさらに詳しく説明します。

カテゴリ別とレピュテーション別の URL のフィルタリング

URL フィルタリングライセンスを使用することにより、要求された URL のカテゴリおよびレピュテーションに基づいて Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、信頼できない（レベル 1）から信頼できる（レベル 5）の範囲です。

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス制御を使用して、ハッキング カテゴリの高リスク信頼できない URL をブロックできます。

カテゴリの説明については、https://www.talosintelligence.com/categories を参照してください。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。脅威を示すサイトや、望ましくないコンテンツを提供するサイトが現れては消えるペースが早すぎて、新しいポリシーを更新して適用するのが間に合わないこともあります。シスコが URL データベースで新しいサイト、変更された分類、変更されたレピュテーションについて更新すると、ルールは自動的に新しい情報に調整されます。新しいサイトを考慮するようにルールを編集する必要はありません。

定期的な URL データベースの更新を有効にすると、システムは最新の情報を使用して URL フィルタリングを行うことができます。また、Cisco Collective Security Intelligence（CSI）との通信を有効にすると、不明なカテゴリとレピュテーションについて URL の最新の脅威インテリジェンスを取得することもできます。詳細については、URL フィルタリングの設定 （959 ページ）を参照してください。

（注） イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。

カテゴリとレピュテーションでの URL の検索

特定の URL のカテゴリとレピュテーションを確認できます。アクセス制御ルールまたは SSL 復号ルールの [URL] タブに移動するか、**[デバイス（Device）] > [システム設定（System Settings）] > [URLフィルタリング設定（URL Filtering Preferences）]** に移動します。そこで、[確認するURL（URL to Check）] ボックスに URL を入力し、[移動（Go）] をクリックします。

ルックアップ結果を示す Web サイトが表示されます。この情報は、カテゴリおよびレピュテーション ベースの URL フィルタリング ルールの動作をチェックするために役立ちます。

分類に同意しない場合は、Device Manager で [URLカテゴリの異議を送信する（Submit a URL Category Dispute）] をクリックして、ご意見をお聞かせください。

手動 URL フィルタリング

個別の URL または URL のグループを手動でフィルタリングすることにより、カテゴリおよびレピュテーションベースの URL フィルタリングを補完または選択的にオーバーライドできます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行できます。

たとえば、アクセス制御を使用して、組織にとって不適切なカテゴリの Web サイトをブロックできます。ただし、カテゴリに適切な Web サイトが含まれ、アクセスを提供したい場合、そのサイトに対して手動の許可ルールを作成し、カテゴリのブロック ルールの前に配置できます。

手動で URL フィルタリングを設定するには、対象の URL を含む URL オブジェクトを作成します。この URL を解釈する方法は、次のルールに基づきます。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。
  - 文字列が URL の先頭にある。
  - 文字列がドットの後に続く。
  - 文字列の先頭にドットが含まれている。
  - 文字列が :// 文字の後に続く。

たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。

（注） サーバーは再構成でき、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。

- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、http://example.com ではなく example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

  ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

HTTPS トラフィックのフィルタリング

HTTPS トラフィックは暗号化されているために、HTTPS トラフィックに対して直接 URL フィルタリングを実行しても、HTTP トラフィックに対して行う場合ほどシンプルではありません。そのため、SSL 復号ポリシーを使用してフィルタリング対象のすべての HTTPS トラフィックを復号することを検討する必要があります。この方法では、URL フィルタリング アクセス コントロール ポリシーは復号されたトラフィックで機能し、通常の HTTP トラフィックの場合と同じ結果が得られます。

ただし、一部の HTTPS トラフィックが復号せずにアクセス コントロール ポリシーに渡されるようにする場合は、HTTPS トラフィックと一致するルールは HTTP トラフィックの場合と異なることを理解する必要があります。暗号化されたトラフィックをフィルタリングするには、システムはSSLハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。URL の Web サイトのホスト名とサブジェクト共通名の間には、ほとんど、またはまったく関係がないことがあります。

DNS 要求フィルタリングを有効にすると、カテゴリ/レピュテーションルールの HTTPS でのマッチングを改善できます。システムは、ユーザーがHTTPS接続の試行を開始する前に、DNS解決フェーズでカテゴリとレピュテーションを決定し、不要な組み合わせに対する DNS 応答をブロックできます。許可されたDNS応答の場合、システムは後続のHTTPS接続で使用可能なカテゴリ/レピュテーション情報を保持します。DNS要求のフィルタリング （604ページ）を参照してください。

HTTPSフィルタリングは、HTTPフィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。HTTPS の URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。また、サイトによって使用される証明書の内容を確認し、サブジェクト共通名で使用されるドメインが正しいこと、この名前が他のルールと競合しないことを確認してください（たとえば、ブロックするサイトの名前が許可する名前と重複する可能性があります）。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトはHTTPSトラフィックと一致しません。このため、慎重にURLオブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

暗号化プロトコルによるトラフィックの制御

システムは、URL フィルタリングの実行時に暗号化プロトコル（HTTP と HTTPS）を無視します。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングでは、次の Web サイトへのトラフィックが同様に処理されます。

- http://example.com
- https://example.com

両方ではなく、HTTP トラフィックのみまたは HTTPS トラフィックのみと一致するルールを設定するには、宛先の条件で TCP ポートを指定するか、アプリケーション条件をルールに追加します。たとえば、それぞれ、TCP ポートまたはアプリケーション条件と URL 条件を含む 2 つのアクセス制御ルールを作成することにより、サイトへの HTTPS アクセスを許可しながら、HTTP アクセスを禁止できます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

アクション：許可

TCP ポートまたはアプリケーション：HTTPS（TCP ポート 443）
URL：example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

アクション：ブロック
TCP ポートまたはアプリケーション：HTTP（TCP ポート 80）
URL：example.com

URL フィルタリングとアプリケーション フィルタリングの比較

URL フィルタリングとアプリケーション フィルタリングには類似点があります。しかし、それらは非常に異なる目的で使用する必要があります。

- URL フィルタリングは、Web サーバ全体へのアクセスをブロックまたは許可するのに適しています。たとえば、ネットワーク上であらゆるタイプのギャンブルを許可しないようにする場合は、ギャンブル カテゴリをブロックする URL フィルタリング ルールを作成できます。このルールでは、ユーザはカテゴリ内の Web サーバ上のどのページにもアクセスできません。
- アプリケーション フィルタリングは、ホスティング サイトに関係なく特定のアプリケーションをブロックするため、またはそうしないと許容される Web サイトの特定の機能をブロックするために便利です。たとえば、Facebook のすべてをブロックすることなく Facebook のゲーム アプリケーションだけをブロックできます。

アプリケーション基準と URL の基準を組み合わせると予期しない結果につながることがあるため、URL とアプリケーションの基準では別のルールを作成するのが良いポリシーです。1 つのルールでアプリケーション基準と URL の基準を組み合わせる必要がある場合は、アプリケーションと URL のルールがより一般的なアプリケーションのみまたは URL のみのルールの例外として機能する場合を除き、単純なアプリケーションのみまたは URL のみのルールの後に配置する必要があります。URL フィルタリング ブロック ルールはアプリケーション フィルタリングよりも広範になるため、アプリケーションのみのルールの上に配置する必要があります。

アプリケーション基準と URL の基準を組み合わせる場合、より慎重にネットワークをモニターし、不要なサイトやアプリケーションへのアクセスを許可しないようにする必要があります。

効果的な URL フィルタリングのベスト プラクティス

URL フィルタリングのアクセス制御ルールを設計するときは、次の推奨事項を覚えておいてください。

- カテゴリとレピュテーションブロックは可能な限り使用します。これにより、新しいサイトはカテゴリに追加されるとともに、自動的にブロックされ、そのレピュテーションに基づくブロックは、サイトの評判が上がる（または下がる）と調整されます。
- URL カテゴリのマッチングを使用するときは、サイトのログイン ページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は [Webベース電子メール（Web based Email）] カテゴリに含まれますが、ログインページは [検索エンジンとポータル（Search Engines and Portals）] カテゴリに含まれます。それらのカテゴリに関し

て異なるアクションを実行する異なるルールがある場合、意図しない結果が生じる可能性があります。

- URL オブジェクトを使用して、Web サイト全体を対象とし、カテゴリ ブロック ルールの例外を作成します。つまり、本来はカテゴリ ルールでブロックされる特定のサイトを許可します。
- （URL オブジェクトを使用して）Web サーバを手動でブロックする場合は、セキュリティ インテリジェンス ポリシーでこれを行うとより効果的です。セキュリティ インテリジェンスポリシーはアクセス制御ルールが評価される前に接続をドロップするので、より速くより効率的にブロックできます。
- HTTPS 接続の最も効果的なフィルタリングのために、記述しているアクセス制御ルールの対象のトラフィックを復号する SSL 復号ルールを実装します。復号された HTTPS 接続はアクセス制御ポリシーの HTTP 接続としてフィルタ処理されるので、HTTPS フィルタリングの制限はすべて回避されます。
- TLS 1.3 では、ほとんどのハンドシェイクメッセージが暗号化されるため、証明書情報を簡単に利用できません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに効果的に対応するには、システムがサーバーのクリアテキスト証明書を取得する必要があります。アクセス制御設定で [TLS 1.3証明書の可視性（TLS 1.3 Certificate Visibility）] を有効にすることをお勧めします。このオプションを有効にすると、システムは、クライアントの Hello パケットの IP アドレスおよび SNI（Server Name Indication）に基づいて、サイトの証明書がキャッシュに保存されているかどうかを確認します。保存されていない場合、システムは、TLS 1.2 プローブを使用して証明書を取得します。その後は、この証明書を使用して、接続を復号せずにアプリケーション/URL カテゴリおよびレピュテーションを識別することができます。
- URL のブロック ルールはアプリケーション フィルタリング ルールの前に配置します。URL フィルタリングは Web サーバー全体をブロックするのに対し、アプリケーション フィルタリングは Web サーバーに関係なく、特定のアプリケーションの使用を対象とするためです。
- カテゴリが不明な高リスクサイトをブロックする場合は、[未分類（Uncategorized）] カテゴリを選択し、評価スライダを [疑わしい（Questionable）] または [信頼できない（Untrusted）] に調整します。
- DNS 要求フィルタリングも有効にすることで、URL フィルタリング全般の有効性を向上させることができます。DNS 要求フィルタリングを使用すると、DNS ルックアップ時に FQDN の URL カテゴリとレピュテーションが決定されるため、後続の HTTP/HTTPS 要求が同じ宛先に送信される際にこの情報を使用できます。さらに、カテゴリ/レピュテーションをブロックすると、試行された接続は、Web セッションの確立段階ではなく、DNS 要求段階で停止します。DNS 要求のフィルタリング （604 ページ） を参照してください。

Web サイトのブロック時にユーザーに表示される内容

URL フィルタリング ルールで Web サイトをブロックした場合、ユーザーに表示される内容は、サイトが暗号化されているかどうかに基づいて異なります。

- HTTP接続：タイムアウトまたはリセットされた接続の場合、通常のブラウザページの代わりにシステムのデフォルトのブロック応答ページが表示されます。このページには、故意に接続がブロックされたことが明確に示されます。
- HTTPS（暗号化）接続：システムのデフォルトのブロック応答ページは表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルト ページが表示されます。エラーメッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

さらに、Webサイトは、明示的なURLフィルタリング ルールではないその他のアクセス コントロール ルールまたはデフォルトのアクションによってブロックされている場合があります。たとえば、ネットワーク全体または地理位置情報をブロックしている場合、ネットワーク上またはその地理的な位置にあるWebサイトもブロックされます。これらのルールによってブロックされたユーザーには、以下の制限で説明するとおり、応答ページが表示されることもあれば、表示されないこともあります。

URLフィルタリングを実装している場合、サイトが意図的にブロックされているときに表示されることがある内容と、どのタイプのサイトをブロックしているかについてエンドユーザーに説明することを検討してください。そうでないと、エンドユーザーがブロックされた接続のトラブルシューティングにかなりの時間を費やしてしまう場合があります。

HTTP 応答ページの制限

システムがWebトラフィックをブロックする場合に、常に、HTTP応答ページが表示されるわけではありません。

- Web トラフィックがプロモートされたアクセス コントロール ルール（単純なネットワーク条件のみの早期に適用されたブロッキング ルール）の結果としてブロックされている場合、システムは応答ページを表示しません。
- システムが要求された URL を特定する前に、Web トラフィックがブロックされている場合、システムは応答ページを表示しません。
- アクセス コントロール ルールによってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。

DNS 要求のフィルタリング

HTTP/HTTPS 以外の接続試行でも、URL カテゴリとレピュテーション データベースを DNS ルックアップ要求に適用できます。

たとえば、ユーザーが www.example.com に FTP 接続しようとすると、その完全修飾ドメイン名（FQDN）のDNSルックアップ要求が検出されたときに、www.example.comのカテゴリとレピュテーションを検索するようにシステムを設定できます。返されたカテゴリ/レピュテーションのDNS/URLフィルタリングルールがブロックルールの場合、システムはDNS応答をブロックします。そのため、ユーザーはFQDNのIPアドレスを取得できず、接続試行に失敗します。

DNS ルックアップ要求フィルタリングを有効にすることで、URL フィルタリングルールを HTTP/HTTPS 以外のプロトコルに拡張し、FTP、TFTP、SCP、ICMP などのプロトコルが Web アクセスをブロックしているサイトへの接続を確立しないようにできます。このフィルタリングは、ユーザーが FQDN 名を使用しており、DNS ルックアップを必要とする限り機能します。ユーザーが IP アドレスを使用する場合、DNS 要求は発生しないため、DNS 要求のブロックはできません。

HTTP/HTTPS トラフィックの場合、DNS 要求時にカテゴリ/レピュテーション ルックアップを実行すると、システムパフォーマンスが向上する可能性があります。これは、Web セッションの確立を試行する前に接続される事態を妨ぐことができるためです。これは、特に暗号化されている HTTPS に対して有効です。DNS 要求の段階で拒否することで、システムは HTTPS 接続を認識しないため、復号ルールを評価する必要がなくなり、暗号されたセッションを適切なアクセス制御ルールに一致させるというさらに難しいタスクを実行する必要もなくなります。

DNS 要求のフィルタリングのガイドライン

DNS 要求のフィルタリングを設定する際は、次の点に注意してください。

- DNS 要求のフィルタリングは、DNS セッションでのみ機能します。DNS 応答を許可する場合（つまり、URL フィルタリング ルール アクションが [許可（Allow）] の場合）、返された IP アドレスを使用してユーザーが確立する後続の接続は、アクセス制御ルールに対して個別に照合されます。接続が別のルールに一致するためブロックされることも、他の理由で許可されることもあります。たとえば、FTP が DNS ルックアップを介して IP アドレスを取得しようとすると、FTP 接続を禁止する別のアクセス制御ルールが存在するため接続が最終的にブロックされることがあります。
- URL/DNS 要求のフィルタリングルールの前にあるアクセス制御ルールに一致する DNS ルックアップ要求は、一致ルールに従って許可またはブロックされます。これらの接続では、カテゴリ/レピュテーション ルックアップは実行されません。
- この機能では、カテゴリ/レピュテーションに基づいて URL フィルタリングを実装する必要があります。このタイプの URL フィルタリングには、URL フィルタリングライセンスが必要です。カテゴリ/レピュテーションに基づく URL フィルタリングルールがない場合、DNS 要求のフィルタリングは関係ないため、有効にしないでください。
- DNS フィルタリングによって生成される接続イベントには、DNS クエリ、URL カテゴリ、および URL レピュテーションという特に重要なフィールドが含まれます。[DNS クエリ（DNS Query）] フィールドには、ルックアップ要求の完全修飾ドメイン名（FQDN）が表示されます。DNS フィルタリングイベントの場合、URL フィールドは空白になります。
- DNS 要求のフィルタリングは、URL カテゴリとレピュテーション データベースのみを使用します。一致するアクセス制御ルールで定義された URL オブジェクトまたはその他の手動 URL フィルタリングは無視されます。手動で DNS 名のブロックを実装する場合は、セキュリティ インテリジェンス DNS ポリシーを使用します。

URL カテゴリとレピュテーションに基づいた DNS 要求のフィルタリング

次の手順では、DNS ルックアップ要求フィルタリングを実装する方法について説明します。

始める前に

まだ有効になっていない場合は、URL ライセンスを有効にする必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択します。

ステップ 2 必要に応じて、[アクセスポリシー設定（Access Policy Settings）]（⚙）ボタンをクリックし、[DNSトラフィックへのレピュテーション適用（Reputation Enforcement on DNS Traffic）] オプションを選択して、[OK] をクリックします。

このオプションは、アクセス コントロール ポリシーの DNS 要求のフィルタリングを有効にします。このオプションは、デフォルトでは有効になっています。

ステップ 3 既存の URL フィルタリングルールを評価するか、新しいルールを作成して、DNS 要求にも適用される URL カテゴリとレピュテーションに基づくフィルタリングを実装します。

URL フィルタリングは通常、HTTP/HTTPS トラフィックにのみ適用されるため、アプリケーションやポートに基づいてこれらのルールを制限する必要はありません。ただし、次の制限がある場合は、ルールが DNS 要求にも適用できることを確認してください。

- [送信元/宛先（Source/Destination）] タブで、[宛先ポート（Destination Ports）] フィールドに [任意（Any）] が指定されている場合、変更は不要です。ポートを指定した場合は、[DNS over UDP] および [DNS over TCP] をリストに追加します。
- [アプリケーション（Applications）] タブで、アプリケーションリストに [任意（Any）] だけが指定されてる場合、変更は不要です。アプリケーションまたはアプリケーションフィルタを指定した場合は、[DNS] アプリケーションをリストまたはフィルタに追加します。その他の DNS 関連オプションは、この目的には関係ありません。

アクセス制御ルールの作成の詳細については、アクセス コントロール ルールの設定（614 ページ）を参照してください。

ステップ 4 DNS 要求がこれらのルールに一致しないことを確認するには、前述のルールを評価します。

カテゴリおよびレピュテーションの決定は、DNS 要求がカテゴリおよびレピュテーションの仕様を持つ URL フィルタリングルールと一致する場合にのみ行われます。URL フィルタリングルールよりも前のアクセス コントロール ポリシーのルールに一致する DNS 要求は、DNS 要求のフィルタリングをバイパスします。このような DNS 要求は、ブロックまたは許可された一致ルールに従って処理されます。

侵入、ファイル、マルウェアのインスペクション

侵入ポリシーとファイルポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイルポリシーは、システムのファイル制御機能とマルウェア防御機能を管理します。

他のトラフィック処理はすべて、侵入、禁止されたファイル、およびマルウェアについて、ネットワーク トラフィックが調べられる前に実行されます。侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックを [許可（allow）] するのみの侵入ポリシーおよびファイル ポリシーを設定できます。トラフィックを [信頼（trust）] または [ブロック（block）] するように設定されたルールではインスペクションは実行されません。さらに、アクセス コントロール ポリシーのデフォルトのアクションが [許可（allow）] の場合は、侵入ポリシーを設定できますが、ファイル ポリシーは設定できません。

アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。ファイルがセッションで検出されてブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。暗号化されていないトラフィックのみのインスペクションが実行されます。

アクセス制御ルールの順序のベスト プラクティス

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。次の推奨事項を考慮してください。

- 固有のルールは一般的なルールの前に来る必要があります（特に特定のルールが一般的なルールの例外である場合）。
- レイヤ 3/4 基準（IP アドレス、セキュリティ ゾーン、ポート番号など）にのみ基づいてトラフィックをドロップするルールはできるだけ早く来る必要があります。レイヤ 3/4 基準は迅速かつ検査なしで評価することができるので、アプリケーションや URL 基準などの検査を必要とするルールの前に来ることをお勧めします。もちろん、これらのルールの例外はこれらより上位に配置されなければなりません。
- 可能な限り、固有のドロップルールはポリシーの最上位近くに配置します。これにより、望ましくないトラフィックへの可能な限り早期の決定が保証されます。

- アプリケーションと URL の基準の両方を含むルールは、より一般的なアプリケーションのみまたは URL のみのルールの例外として機能している場合を除き、単純なアプリケーションのみまたはURLのみのルールの後に来る必要があります。アプリケーションとURLの基準を組み合わせることで、予期しない結果が生じることがある（特に暗号化されたトラフィックの場合）ため、可能な限り、URL とアプリケーションのフィルタリング用に個別のルールを作成することをお勧めします。

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバー 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバーに付与する場合は、この内部サーバーへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバーのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

その他のセキュリティ ポリシーがアクセス制御に影響する仕組み

その他のセキュリティ ポリシーは、アクセス制御ルールが機能し接続と一致する方法に影響を与えます。アクセス ルールを設定するときは、次の点に注意してください。

- [SSL復号（SSL Decryption）] ポリシー：SSL 復号ルールはアクセス制御の前に評価されます。したがって、暗号化された接続が、復号化のいくつかのタイプを適用する SSL 復号ルールと一致する場合、それはアクセス コントロール ポリシーによって評価されるプレーン テキスト（復号化）接続です。アクセス ルールは、暗号化されたバージョンの接続を参照しません。また、トラフィックをドロップするSSL復号ルールと一致するすべての接続はアクセス コントロール ポリシーによって参照されることがありません。最後に、復号しないルールと一致する暗号化された接続は、その暗号化された状態で評価されます。

- [アイデンティティ（Identity）] ポリシー：送信元 IP アドレスのユーザー マッピングがある場合にのみ接続はユーザー（およびユーザー グループ）と一致します。ユーザまたはグループ メンバーシップを重視するアクセス ルールは、ユーザ アイデンティティがアイデンティティ ポリシーによって正常に収集された接続のみと一致できます。

- [セキュリティ インテリジェンス（Security Intelligence）] ポリシー：アクセス コントロール ポリシーではドロップされた接続が参照されることはありません。ブロックリストに一致しない接続は、その後にアクセス制御ルールと照合され、最終的に、そのアクセス制御ルールによって、接続の処理方法（許可またはドロップ）が決定されます。

- [VPN]（サイト間またはリモート アクセス）：VPN トラフィックは常にアクセス コントロール ポリシーに対して評価され、一致するルールに基づいて接続は許可またはドロップされます。ただし、VPN トンネル自体はアクセス コントロール ポリシーが評価される前に復号化されます。アクセス コントロール ポリシーは、トンネル自体ではなく VPN トンネル内に組み込まれている接続を評価します。

アクセス制御のためのライセンス要件

アクセス制御ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、アクセス制御ポリシー内の特定の機能には、次のライセンスが必要です。ライセンスの設定については、オプション ライセンスの有効化または無効化（109ページ）を参照してください。

- **URL** ライセンス：URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するため。
- **IPS** ライセンス：アクセスルールまたはデフォルトアクションに侵入ポリシーを設定するため。ファイルポリシーを使用するには、このライセンスも必要です（マルウェア防御ライセンスも必要）。
- **マルウェア防御**ライセンス：アクセスルールにファイルポリシーを設定するため。IPS ライセンスは、ファイルポリシーにも必要です。

アクセスコントロールポリシーに関する注意事項と制限事項

アクセス制御のためのいくつかの追加の制限事項を次に示します。ルールから期待どおりの結果を得ているかどうかを評価してこれらを検討してください。

- URL データベースの更新にカテゴリの追加（新規、着信）、廃止（送信）、または削除が含まれている場合は、影響を受けるアクセス制御ルールを変更するための猶予期間があります。影響を受けるルールは情報メッセージと一緒にマークされ、メッセージにはルールに影響する問題についての説明と、カテゴリ変更に関する詳細情報がある Cisco Talos Intelligence Group（Talos）Web サイトへのリンクが記載されます。最新の URL データベースで使用可能な適切なカテゴリを使用するように、ルールを更新する必要があります。

  猶予期間に対応するため、廃止された送信カテゴリを削除せずに新しく追加された着信カテゴリを適切なルールに追加します。ルールは新旧のカテゴリの両方を含める必要があります。新しいカテゴリは、古いカテゴリが削除対象としてマークされている場合に有効になります。古いカテゴリが最終的に削除されたら、ルールを編集して削除されたカテゴリを除去し、設定を再展開する必要があります。削除されたカテゴリを使用するルールを修正するまで、設定の展開はブロックされます。注意が必要なルールをフィルタリングするには、テーブルの上の [問題のあるルールを表示する（See Problem Rules）] リンクをクリックします。

- Device Manager はディレクトリサーバーから最大 50,000 人のユーザーに関する情報をダウンロードできます。ディレクトリ サーバに 50,000 以上のユーザ アカウントが含まれる場合、アクセス ルールでユーザを選択するとき、またはユーザ ベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

50,000までの制限は、グループに関連付けられた名前にも適用されます。グループに50,000を超えるメンバーが含まれている場合は、ダウンロードした50,000個の名前だけをグループメンバーシップと照合できます。

- 脆弱性データベース（VDB）の更新によってアプリケーションが削除（廃止）される場合は、削除されたアプリケーションを使用するアクセス制御ルールまたはアプリケーションフィルタに変更を加える必要があります。これらのルールを修正するまで、変更は展開できません。さらに、システムソフトウェアの更新は、問題を修正するまでインストールできません。[アプリケーションフィルタ（Application Filters）] オブジェクト ページ、またはルールの [アプリケーション（Application）] タブでは、これらのアプリケーション名の後に「（廃止）（Deprecated）」と表示されます。

- 完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを送信元または宛先の基準として使用するには、**[デバイス（Device）] > [システム設定（System Settings）] > [DNSサーバー（DNS Server）]** でデータ インターフェイスの DNS も設定する必要があります。システムは、アクセス制御ルールで使用されているFQDNオブジェクトのルックアップを実行するために管理 DNS サーバ設定を使用しません。FQDN 解決のトラブルシューティングについては、DNSの一般的な問題のトラブルシューティング（946ページ）を参照してください。

  FQDNによるアクセスの制御はベストエフォート型のメカニズムであることに注意してください。次の点を考慮してください。

  - DNS応答はスプーフィングされる可能性があるため、完全に信頼できる内部DNSサーバーのみを使用します。

  - 一部のFQDNは、特に非常に人気の高いサーバーの場合、数千とはいかなくても、数百の IP アドレスを持つことがあり、それらが頻繁に変更されることがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザーはキャッシュに存在しないアドレスを取得する可能性があり、その接続はFQDNルールに合致しません。FQDN ネットワークオブジェクトを使用するルールは、100 未満のアドレスに解決される名前に対してのみ効果的に機能します。

    100 を超えるアドレスに解決される FQDN のネットワーク オブジェクト ルールを作成しないことを推奨します。接続のアドレスが解決され、デバイスのDNSキャッシュで使用可能である可能性は低いからです。このような場合は、FQDNネットワーク オブジェクト ルールの代わりに URL ベースのルールを使用します。

  - 人気のある FQDN では、異なる DNS サーバーが異なるセットの IP アドレスを返す場合があります。したがって、ユーザーが設定したものとは異なる DNS サーバーを使用している場合、FQDNベースのアクセス制御ルールがクライアントで使用されているサイトのすべての IP アドレスに適用されないことがあり、ルールで意図した結果が得られません。

  - 一部の FQDN DNS エントリには、非常に短い存続可能時間（TTL）値が設定されています。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。

- 実際に使用されているルールを編集する場合、その変更は、Snort によって検査されなくなった、確立されている接続には適用されません。新しいルールは、将来の接続に対する照合に使用されます。また、Snortによって接続がアクティブに検査されている場合、Snortは、変更された一致またはアクション基準を既存の接続に適用できます。現在のすべての接続に変更を確実に適用する必要がある場合は、デバイス CLI にログインし、**clear conn** コマンドを使用して、確立されている接続を終了させることができます。これは、その後に接続の送信元が接続を再確立を試み、そのために新しいルールに対して適切に照合されることを前提としています。

- 接続のアプリケーションまたは URL を識別するためにシステムは 3 ～ 5 パケットを使用します。したがって、正しいアクセス制御ルールでも特定の接続ではすぐに一致しない可能性があります。ただし、アプリケーション/URL が判明すると、接続は一致するルールに基づいて処理されます。暗号化された接続の場合、これはSSLハンドシェイクでのサーバ証明書の交換後に発生します。

- システムは、アプリケーションが識別される接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

- 可能な場合は常に、一致基準を空のままにします（特にセキュリティゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。たとえば、すべてのインターフェイスを含むゾーンを作成するのではなく、セキュリティゾーンの条件を空白のままにするだけで、システムはすべてのインターフェイスのトラフィックをより効率的に照合できます。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

- 送信元または宛先の基準に IP アドレスを指定する場合は、同じルールに IPv4 アドレスと IPv6 アドレスを混在させないでください。IPv4 アドレスと IPv6 アドレスに個別のルールを作成します。

- 動作中、Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されるか、または Device Manager にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。

  オブジェクトグループ検索を有効にすると、ネットワークオブジェクトを含むアクセス コントロール ポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPUに対する影響と、特定のアクセス コントロール ポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

  FlexConfig を使用してこのオプションを設定するには、**object-group-search access-control** コマンドを発行します。否定テンプレートでは、このコマンドの **no** 形式を使用します。

リリース 7.2 以降、この機能は新しい展開ではデフォルトで有効になっていますが、アップグレードされたシステムでは自動的に有効になりません。

- 関連 RFC に違反する GRE トンネルはドロップされます。たとえば、RFC に反して GRE トンネルの予約ビットにゼロ以外の値が含まれている場合、そのトンネルはドロップされます。非準拠の GRE トンネルを許可する必要がある場合は、リモートマネージャを使用して、そのセッションを信頼するプレフィルタルールを設定する必要があります。Device Manager を使用してプレフィルタルールを設定することはできません。

アクセス コントロール ポリシーを設定する

ネットワーク リソースへのアクセスを制御するには、アクセス コントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。トラフィックに一致するルールがない場合、ページ下部に表示されるデフォルトアクションが適用されます。

アクセス コントロール ポリシーを設定するには、**[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

アクセスコントロール表には、すべてのルールが順番に表示されます。各ルールで以下を実行します。

- 左側の列にあるルール番号の隣の [>] ボタンをクリックし、ルール図を開きます。この図は、ルールがトラフィックをどのように制御するかを視覚的に示します。ボタンを再度クリックして図を閉じます。
- ほとんどのセルはインライン編集が可能です。たとえば、アクションをクリックして別のものを選択したり、送信元ネットワークオブジェクトをクリックして送信元の条件を追加または変更したりできます。
- ルールを移動するには、[移動（move）] アイコン（）が表示されるまでルールにカーソルを合わせ、次にルールをクリックして新しいロケーションにドラッグし、ドロップします。また、ルールを編集して [順序（Order）] リストで新しいロケーションを選択することで、ルールを移動することもできます。希望する処理の順番にルールを配置することが重要です。具体的なルール（特に、より一般的なルールに対する例外を定義するルール）は上部近くに配置します。
- 右側の列には、ルールのアクションボタンが含まれます。セルにマウスを当てるとボタンが表示されます。ルールを編集（）または削除（）できます。
- [アクセスコントロールの設定（Access Control Settings）]（）ボタンをクリックして、ポリシー内の特定のルールではなく、アクセス コントロール ポリシーに適用される設定を行います。
- テーブルの上の [ヒットカウントの切り替え（Toggle Hit Counts）] アイコン（）をクリックし、テーブルの [ヒットカウント（Hit Count）] 列を追加または削除します。[ヒッ

トカウント（Hit Count）] 列は [名前（Name）] 列の右側にあり、ルールの合計ヒット数と最新のヒットの日付と時刻が表示されます。ヒットカウント情報は、切り替えボタンをクリックしたときに取得されます。最新情報を取得するには、更新アイコン（）をクリックします。

- URL カテゴリの削除または変更などが原因で特定のルールに問題が発生した場合、これらのルールのみを表示するには、検索ボックスの横にある [See Problem Rules] リンクをクリックしてテーブルをフィルタ処理します。これらのルールを編集および修正（または削除）して、必要とするサービスが提供されるようにします。

次に、ポリシーの設定方法について説明します。

デフォルト アクションの設定

接続が特定のアクセス ルールに一致しない場合、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

ステップ 2 [デフォルトアクション（Default Action）] フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [信頼（Trust）]：どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可（Allow）]：侵入ポリシーの対象となるトラフィックを許可します。
- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 4 アクションが [許可（Allow）] の場合、侵入ポリシーを選択します。

ポリシー オプションの説明については、侵入ポリシーの設定（624 ページ）を参照してください。

ステップ 5 （オプション）デフォルト アクションのロギングを設定します。

デフォルトアクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベント ビューアに記載されるようにするには、トラフィックのロギングを有効にする必要があります。ロギングの設定（625 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。

アクセス コントロール ポリシーの設定

ポリシー内の特定のルールではなく、アクセス コントロール ポリシーに適用される設定を行います。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択します。

ステップ 2 [アクセスポリシーの設定（Access Policy Settings）]（⚙）ボタンをクリックします。

ステップ 3 以下の設定項目を設定します。

- [TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）]：TLS 1.3 では、ほとんどのハンドシェイクメッセージが暗号化されるため、証明書情報を簡単に利用できません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに対応するには、システムにサーバーのクリアテキスト証明書がある必要があります。このオプションを有効にすると、システムは、クライアントの Hello パケットの IP アドレスおよび SNI（Server Name Indication）に基づいて、サイトの証明書がキャッシュに保存されているかどうかを確認します。保存されていない場合、システムは、TLS 1.2 プローブを使用して証明書を取得します。その後は、この証明書を使用して、アプリケーション/URL カテゴリおよびレピュテーションを識別することができます。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するために、このオプションを有効にすることを推奨します。この設定では、証明書のみが取得されます。接続は暗号化されたままになります。TLS 1.3 証明書を取得するには、このオプションを有効にするだけで十分です。対応する SSL 復号ルールを作成する必要はありません。ただし、キャッシュされた証明書は、アクセス制御処理に加えて、より効果的な復号ルール処理にも使用されます。
- [DNSトラフィックへのレピュテーション適用（Reputation Enforcement on DNS Traffic）]：URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用するには、このオプションを有効にします。ルックアップ要求の完全修飾ドメイン名（FQDN）にブロックしているカテゴリやレピュテーションがある場合、システムは DNS 応答をブロックします。ユーザーは DNS 解決を受信しないため、ユーザーは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーション フィルタリングを適用するには、このオプションを使用します。詳細については、DNS 要求のフィルタリング （604 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

アクセス コントロール ルールの設定

アクセス コントロール ルールを使用して、ネットワーク リソースへのアクセスを制御します。アクセス コントロール ポリシーのルールは、上から下に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（）をクリックします。

ステップ 3 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+ . _ -

ステップ 5 一致するトラフィックに適用するアクションを選択します。

- [信頼（Trust）]：どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可（Allow）]：ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。
- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/宛先（Source/Destination）]：トラフィックが通過するセキュリティゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的位置）、アドレスに割り当てられたセキュリティグループタグ（SGT）、またはトラフィックで使用されるプロトコルおよびポート。デフォルトは、すべてのゾーン、アドレス、地理的位置、SGT、プロトコル、およびポートです。送信元/宛先基準 （617 ページ）を参照してください。
- [アプリケーション（Application）]：アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトはすべてのアプリケーションです。アプリケーション基準 （619 ページ）を参照してください。
- [URL]：Web または DNS ルックアップ要求の URL または URL カテゴリ。デフォルトはすべての URL です。「URL 基準 （621 ページ）」を参照してください。

- [ユーザー（Users）]：アイデンティティ ソース、ユーザーまたはユーザー グループ。アイデンティティ ポリシーは、ユーザーとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。ユーザー基準 （623 ページ）を参照してください。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件をアクセス コントロール ルールに追加する場合は、次のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、特定のホストまたはネットワークの URL フィルタリングを行う単一のルールを使用できます。
- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはアプリケーション フィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。
- 一部の機能では、適切なライセンスを有効にする必要があります。

ステップ 7 （オプション）[許可（Allow）] アクションを使用するポリシーの場合、暗号化されていないトラフィックについてさらにインスペクションを設定できます。次のいずれかのリンクをクリックします。

- [侵入ポリシー（Intrusion Policy）]：トラフィックで侵入およびエクスプロイトを検査する場合は、**[侵入ポリシー（Intrusion Policy）] > [オン（On）]** を選択し、侵入検査ポリシーを選択します。「侵入ポリシーの設定 （624 ページ）」を参照してください。
- [ファイルポリシー（File Policy）]：マルウェアを含むファイルやブロックすべきファイルのトラフィックのインスペクションを実行するファイルポリシーを選択します。ファイル ポリシーの設定 （624 ページ）を参照してください。

ステップ 8 （任意）ルールのロギングを設定します。

デフォルトでは、ルールに一致するトラフィックに対して接続イベントは生成されませんが、ファイル ポリシーを選択した場合、ファイル イベントはデフォルトで生成されます。この動作は変更できます。ダッシュボード データまたはイベント ビューアに含まれるポリシーに一致するトラフィックのロギングを有効にする必要があります。ロギングの設定 （625 ページ）を参照してください。

マッチング アクセス ルールのログ構成に関係なくドロップまたはアラートするように設定されている侵入ルールについては、常に侵入イベントが生成されます。

ステップ 9 [OK] をクリックします。

送信元/宛先基準

アクセスルールの送信元/送信先条件は、トラフィックが通過するセキュリティゾーン（インターフェイス）、IP アドレスまたは IP アドレスの国/大陸（地理的位置）、アドレスに割り当てられたセキュリティグループタグ（SGT）、またはトラフィックで使用されるプロトコルおよびポートを定義します。デフォルトは、すべてのゾーン、アドレス、地理的位置、SGT、プロトコル、およびポートです。

条件を変更するには、その条件内の [+] ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティ ゾーン オブジェクト。1 つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、ホスト内部に向かうすべてのトラフィックが侵入検査を受けるようにする場合は、内部ゾーンを [送信先ゾーン（Destination Zones）] として選択し、送信元ゾーンは空白のままにします。侵入フィルタリングをルールに含めるには、ルールのアクションを [許可（Allow）] にし、ルールで侵入ポリシーを選択する必要があります。

（注） 1 つのルールにパッシブ セキュリティ ゾーンとルーテッド セキュリティ ゾーンを混在させることはできません。さらに、パッシブセキュリティゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IPアドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）] : 制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。完全修飾ドメイン名（FQDN）を使用してアドレスを定義するオブジェクトを使用できます。このアドレスは DNS ルックアップによって判別されます。
- [地理位置情報（Geolocation）] : 位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

（注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、これにポートを含めることができます。ICMP では、コードとタイプを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。宛先ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。ICMP およびその他の非 TCP/UDP 仕様は、宛先ポートでのみ許可されます。送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから発生し、特定の TCP/UDP ポートに向かうトラフィックを照合するには、両方設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみ

を追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックを対象にできます。

送信元 SGT グループ、宛先 SGT グループ

Identity Services Engine（ISE）からダウンロードされた、トラフィックに割り当てられた SGT を識別するセキュリティグループタグ（SGT）グループオブジェクト。これらのオブジェクトは、ISE アイデンティティソースを定義する場合にのみ使用できます。それ以外の場合、このセクションは表示されません。アクセス制御のために SGT を使用する方法の詳細については、Trustsec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法 （631 ページ） を参照してください。

- 送信元がグループで定義された SGT のいずれかを持つトラフィックを照合するには、[送信元SGTグループ（Source SGT Groups）] を設定します。
- 宛先がグループで定義された SGT のいずれかを持つトラフィックを照合するには、[宛先SGTグループ（Destination SGT Groups）] を設定します。
- 送信元 SGT 条件と宛先 SGT 条件の両方をルールに追加する場合、指定されたタグのいずれかを持つ送信元から発信され、宛先タグのいずれかに送信されるトラフィックのみが照合されます。

アプリケーション基準

アクセス ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタが規定されます。デフォルトは任意のアプリケーションです。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

また、シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加します。そのため、ルールを手動で更新せずに、高リスクアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーション フィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタ リストを変更するには、条件内の [+] ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーション フィルタ オブジェクトを選択してから、ポップアップ表示されるダイアログボックスで [OK] をクリックします。いずれかのタブで [詳細フィルタ（Advanced Filte）] をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存（Save As

Filter）]リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーション フィルタ オブジェクトとして保存します。

（注） 選択したアプリケーションが VDB の更新によって削除された場合は、アプリケーション名の後に「Deprecated（廃止）」が表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

次の [詳細フィルタ（Advanced Filter）] 基準を使用すると、ルールに一致するアプリケーションまたはフィルタを特定できます。これらはアプリケーション フィルタ オブジェクトで使用されるものと同じ要素です。

（注） 1 つのフィルタ条件内での複数の選択はOR関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（VeryHigh）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。

リスク

アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーションプロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル。
- [クライアントプロトコル（Client Protocol）]：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Webアプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も重要な機能を説明する一般分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは[SSLプロトコル（SSL Protocol）] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）] タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

URL 基準

アクセス ルールの URL 基準は、Web 要求で使用される URL または要求された URL が属するカテゴリを定義します。カテゴリが一致する場合は、許可またはブロックするためのサイトの相対レピュテーションも指定できます。デフォルトでは、すべての URL が許可されます。

DNS ルックアップ要求フィルタリングを有効にすると、カテゴリとレピュテーションの設定は、ルックアップ要求の完全修飾ドメイン名（FQDN）にも適用されます。DNS 要求フィルタリングには、カテゴリとレピュテーションの設定のみが適用されます。手動 URL フィルタリングは無視されます。

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成できます。たとえば、すべてのギャンブルサイトをブロックしたり、信頼できないソーシャル ネットワーキング サイトをブロックしたりできます。ユーザがそのカテゴリとレピュテーションの組み合わせでURLを閲覧しようとすると、セッションがブロックされます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と出没する可能性があります。

URL リストを変更するには、条件内の [+] ボタンをクリックし、次の手法のいずれかを使用して、目的のカテゴリまたは URL を選択します。ポリシーからカテゴリまたはオブジェクトを削除するには、対応する [x] をクリックします。

[URL] タブ

[+] をクリックし、URL オブジェクトまたはグループを選択して、[OK] をクリックします。必要なオブジェクトが存在しない場合は、[URLの新規作成（Create New URL）] をクリックします。

（注） 特定のサイトをターゲットにするようにURLオブジェクトを設定する前に、手動URLフィルタリングに関する情報を注意深く読みます。

[カテゴリ（Categories）] タブ

[+] をクリックし、目的のカテゴリを選択して、[OK] をクリックします。

カテゴリの説明については、https://www.talosintelligence.com/categoriesを参照してください。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべての URL にルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意（Any）]チェックボックスを選択解除し、[レピュテーション（Reputation）] スライダを使用してレピュテーション レベルを選択します。レピュテーション スライダの左側は許可されるサイトを、右側はブロックされるサイトを示しています。レピュテーションがどのように使用されるかは、ルールアクションによって異なります。

- ルールによって Web アクセスをブロックまたは監視する場合は、レピュテーション レベルを選択することで、そのレベルより深刻なすべてのレピュテーションも選択されます。たとえば、**[問題のあるサイト（Questionable sites）]**（レベル 2）をブロックまたは監視するルールを設定した場合、**[信頼できない（Untrusted）]**（レベル 1）サイトも自動的にブロックまたは監視されます。
- ルールが Web アクセスを許可する場合は、レピュテーション レベルを選択すると、そのレベルより深刻でないすべてのレピュテーションも選択されます。たとえば、**[好ましいサイト（Favorable sites）]**（レベル 4）を許可するルールを設定した場合、**[信頼できる（Trusted）]**（レベル 5）サイトも自動的に許可されます。

レピュテーションが不明な URL をレピュテーション一致に含めるには、[レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] オプションを選択します。通常、新しいサイトは評価されていません。また、その他の理由でサイトのレピュテーションが不明である（または判断できない）場合もあります。

URL のカテゴリの確認

特定の URL のカテゴリとレピュテーションを確認できます。[確認するURL（URL to Check）] ボックスに URL を入力し、[移動（Go）] をクリックします。結果を表示するには、外部の Web サイトに移動します。分類に同意しない場合は、[URLカテゴリの異議を送信する（Submit a URL Category Dispute）] リンクをクリックしてお知らせください。

ユーザー基準

アクセス ルールのユーザ基準は、IP 接続のユーザまたはユーザ グループを定義します。アクセス ルールにユーザーまたはユーザー グループの基準を含めるには、アイデンティティ ポリシーと関連付けられたディレクトリ サーバーを設定する必要があります。

アイデンティティ ポリシーは、特定の接続に関してユーザー アイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストの IP アドレスに識別されたユーザーが関連付けられます。したがって、送信元 IP アドレスがユーザーにマッピングされているトラフィックは、そのユーザーからのものとみなされます。IP パケット自体にはユーザー アイデンティティ情報は含まれていないため、この IP アドレスとユーザー間のマッピングが使用可能な中での最良近似となります。

1 つのルールに最大 50 のユーザーまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザーを選択するより有意義です。たとえば、エンジニアリング グループに開発ネットワークへのアクセスを許可するルールを作成し、それに続くルールとして、そのネットワークへの他のすべてのアクセスを拒否するルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバーのエンジニアリング グループに追加するだけです。

そのソース内のすべてのユーザーに適用するアイデンティティ ソースを選択することもできます。したがって、複数の Active Directory ドメインをサポートする場合は、ドメインに基づいてリソースへの差分アクセスを提供できます。

ユーザーリストを変更するには、条件の中にある [+] ボタンをクリックし、次のいずれかの方法で必要なアイデンティティを選択します。ポリシーからアイデンティティを削除するには、該当する [x] をクリックします。

- [アイデンティティ ソース（Identity Sources）]：AD レルムやローカル ユーザー データベースなど、選択したソースから取得したすべてのユーザーにルールを適用するアイデンティティ ソースを選択します。必要なレルムがまだ存在しない場合、[新規アイデンティティ レルムの作成（Create New Identity Realm）] をクリックして作成します。
- [グループ（Groups）]：目的のユーザー グループを選択します。グループは、ディレクトリ サーバーにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセス ルールを作成し、それをアクセス コントロール ポリシー内で親グループのルールの上に配置する必要があります。
- [ユーザー（Users）]：個々のユーザーを選択します。ユーザー名には、Realm\username などのアイデンティティ ソースがプレフィックスとして付けられます。

  Special-Identities-Realm の下にはいくつかの組み込みユーザーがあります。

  - [認証失敗（Failed Authentication）]：ユーザーは認証を求められましたが、最大許容試行回数内に有効なユーザー名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザーのネットワークへのアクセスは妨げられませんが、これらのユーザーのネットワーク アクセスを制限するためのアクセス ルールを記述できます。

- [ゲスト（Guest）]：ゲストユーザーは、これらのユーザーをゲストと呼ぶようにアイデンティティルールが設定されている点を除き、認証失敗ユーザーと同様です。ゲストユーザーは認証を求められましたが、最大試行回数内に認証されることができませんでした。
- [認証不要（No Authentication Required）]：ユーザーの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザーは認証を求められませんでした。
- [不明（Unknown）]：IPアドレスのユーザーマッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

侵入ポリシーの設定

ファイアウォールシステムには複数の侵入ポリシーが付属しています。Cisco Cisco Talos Intelligence Group（Talos）によって提供されるいくつかの侵入ポリシーはシスコによって設計されています。Talos によって、侵入およびプリプロセッサルール状態と詳細設定が規定されています。トラフィックを許可するアクセス制御ルールでは、侵入ポリシーを選択して、トラフィックにおける侵入およびエクスプロイトを検査することができます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。

Snort 2 を実行している場合、これらは使用可能な唯一のポリシーであり、変更できません。ただし、侵入ルールのアクションの変更（Snort 2）（672 ページ）で説明しているように、特定のルールに対して実行するアクションを変更することは可能です。

Snort 3 を実行している場合は、これらのポリシーのいずれかを選択するか、独自の侵入ポリシーを作成できます。

侵入検査を有効化するには、**[侵入ポリシー（Intrusion Policy）]** > **[オン（On）]** を選択し、必要なポリシーを選択します。各ポリシーの説明を表示するには、ドロップダウンリストでポリシーの情報アイコンをクリックします。

定義済みポリシーの詳細については、システム定義のネットワーク分析および侵入ポリシー（640 ページ）を参照してください。

ファイル ポリシーの設定

ファイルポリシーにより、マルウェア防御を使用して悪意のあるソフトウェア（マルウェア）を検出することができます。ファイル制御を実行するファイルポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

マルウェア防御は、ネットワークトラフィックで検出された潜在的なマルウェアの性質を取得し、ローカルマルウェアファイル分析と事前分類の更新を取得するために Secure Malware Analytics Cloudを使用します。Secure Malware Analytics Cloud にアクセスし、マルウェアルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について Secure Malware Analytics Cloud に問い合わせます。可能な性質を次に示します。

- マルウェア（Malware）：Secure Malware Analytics Cloudはファイルをマルウェアとして分類しました。ファイル内のいずれかのファイルがマルウェアである場合、アーカイブ ファイル（たとえば zip ファイル）はマルウェアとしてマークされます。
- クリーン（Clean）：Secure Malware Analytics Cloudはファイルをマルウェアが含まれないクリーンな状態であると分類しました。その中のすべてのファイルがクリーンであれば、アーカイブ ファイルはクリーンであるとマークされます。
- 不明（Unknown）：Secure Malware Analytics Cloudはまだファイルの性質を指定していません。その中のすべてのファイルが不明であれば、アーカイブ ファイルは不明であるとマークされます。
- 使用不可（Unavailable）：システムは Secure Malware Analytics Cloudに対し、このファイルの性質を問い合わせることができませんでした。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。複数の「利用不可」イベントが連続して発生している場合、管理アドレスのインターネット接続が正常に機能していることを確認します。

使用可能なファイル ポリシー

次のいずれかのファイル ポリシーを選択できます。

- [なし（None）]は、送信したファイルでマルウェアの評価を行わず、特定のファイルをブロックしません。このオプションは、ファイル送信が信頼されている、またはファイル送信の可能性が低い（または不可能である）、あるいはアプリケーションを信頼している、または URL フィルタリングがネットワークを適切に保護しているルールに対して選択します。
- [マルウェアをすべてブロック（Block Malware All）]：Secure Malware Analytics Cloudに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [クラウドをすべてルックアップ（Cloud Lookup All）]：Secure Malware Analytics Cloudに問い合わせてネットワークを通過するファイルの傾向を取得して記録したうえでその伝送を許可します。
- **（カスタムファイルポリシー）**：脅威に対する防御 API filepolicies リソース、およびその他の FileAndMalwarePolicies リソース（filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections など）を使用して、独自のファイルポリシーを作成できます。ポリシーを作成して変更を展開した後、Device Manager でアクセス制御ルールを編集するときにポリシーを選択できます。ポリシーを選択すると、ポリシーの下にポリシーの説明が表示されます。

ロギングの設定

アクセス ルールのロギング設定は、接続イベントがルールに一致するトラフィックに対して発行されるかどうかを決定します。イベント ビューアでルールに関連するイベントを確認するには、ロギングを有効にする必要があります。また、一致するトラフィックがシステムをモニ

ターするために使用できるさまざまなダッシュボードに反映されるようにするためにも、ロギングを有効にする必要があります。

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。

注意 サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイスを対象としているかどうかを検討します。

次のロギング オプションを設定できます。

ログ アクションの選択

次のいずれかのアクションを選択できます。

- [接続の開始時と終了時にログを記録する（Log at Beginning and End of Connection）]：接続の開始時と終了時にイベントを発行します。接続終了イベントには接続開始イベントに含まれるすべての情報と、接続中に拾うことができるすべての情報が含まれているため、許可しようとしているトラフィックではこのオプションを選択しないことをお勧めします。両方のイベントのロギングは、システムパフォーマンスに影響する可能性があります。ただし、これはブロックされているトラフィックに許可されている唯一のオプションです。
- [接続終了時にログを記録する（Log at End of Connection）]：接続の終了時に接続ログの記録を許可する場合は、このオプションを選択します。これは許可されている、または信頼されているトラフィックに推奨されます。
- [接続のロギングなし（No Logging at Connection）]：ルールのロギングを無効にするには、このオプションを選択します。これがデフォルトです。

（注） アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。侵入がブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）]、理由は [侵入ブロック（Intrusion Block）] ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ファイル イベント

禁止されたファイルまたはマルウェア イベントのロギングを有効にするには、[ファイルのロギング（Log Files）] を選択します。このオプションを設定するには、ルールでファ

イル ポリシーを選択する必要があります。ルールにファイル ポリシーを選択している場合、このオプションはデフォルトで有効になっています。シスコは、このオプションを有効のままにすることを推奨します。

システムが禁止されたファイルを検出すると、次のタイプのイベントの1つを自動的にロギングします。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

ファイルがブロックされた接続の場合、接続ログにおける接続のアクションは [ブロック（Block）] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイルモニター（File Monitor）]（ファイル タイプまたはマルウェアが検出された）、あるいは [マルウェアブロック（Malware Block）] または [ファイルブロック（File Block）]（ファイルがブロックされた）です。

接続イベントの送信先

外部 syslog サーバーにイベントのコピーを送信するには、syslog サーバーを定義するサーバー オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslog サーバーの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバーへのロギングを無効にするには、サーバー リストから [任意（Any）] を選択します）。

デバイスのイベント ストレージは限られているため、外部 syslog サーバーへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

この設定は、接続イベントのみに適用されます。侵入イベントを syslog に送信するには、侵入ポリシーの設定でサーバーを設定します。Syslog にファイル/マルウェア イベントを送信するには、**[デバイス（Device）] > [システム設定（System Settings）] > [ロギング設定（Logging Settings）]** でサーバーを設定します。

アクセス コントロール ポリシーのモニタリング

以下のトピックでは、アクセス制御ポリシーのモニター方法について説明します。

ダッシュボードでのアクセス制御統計情報のモニタリング

[モニタリング（Monitoring）] ダッシュボードの大半のデータは、アクセス コントロール ポリシーに直接関連しています。「トラフィックのモニタリングおよびシステム ダッシュボード（123 ページ）」を参照してください。

- **[モニタリング（Monitoring）]** > **[アクセスおよびSIルール（Access And SI Rules）]** には最もヒットしたアクセス ルールと関連する統計情報が表示されます。
- 一般的な統計情報は、[ネットワーク概要（Network Overview）]、[送信先（Destinations）] および [ゾーン（Zones）] ダッシュボードで確認できます。
- URL フィルタリングの結果は [Webカテゴリ（Web Categories）]、[URLカテゴリ（URL Categories）]および [送信先（Destinations）] ダッシュボードで確認できます。[Webカテゴリ（Web Categories）]、[URLカテゴリ（URL Categories）]ダッシュボードに情報を表示するには、少なくとも 1 つの URL フィルタリング ポリシーが必要です。
- アプリケーション フィルタリングの結果は、[アプリケーション（Applications）] および [Webアプリケーション（Web Applications）] ダッシュボードで確認できます。
- [ユーザー（Users）] ダッシュボードでは、ユーザーベースの統計情報を確認できます。ユーザ情報を収集するには、アイデンティティ ポリシーを実装する必要があります。
- [攻撃者（Attackers）] および [ターゲット（Targets）] ダッシュボードでは、侵入ポリシーの統計情報を確認できます。これらのダッシュボードで情報を表示するには、少なくとも 1 つのアクセス コントロール ルールに侵入ポリシーを適用する必要があります。
- ファイル ポリシーおよびマルウェア フィルタリング統計情報は、[ファイルログ（File Logs）] および [マルウェア（Malware）] ダッシュボードで確認できます。このダッシュボードに情報を表示するには、ファイル ポリシーを 1 つ以上のアクセス制御ルールに適用する必要があります。
- **[モニタリング（Monitoring）]** > **[イベント（Events）]** には、アクセス コントロール ルールに関連する接続とデータのイベントも表示されます。

ルール ヒット カウントの調査

各アクセス制御ルールのヒットカウントを表示することができます。ヒットカウントは、接続がルールに一致する頻度を示します。この情報を使用して、最もアクティブなルールとアクティブの度合いが低いルールを特定できます。

このカウントは、再起動やアップグレードの後も維持されます。

また、デバイス CLI で **show rule hits** コマンドを使用してルールヒットカウント情報を表示することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択します。

ステップ 2 [ヒットカウントの切り替え（Toggle Hit Counts）] アイコン（  ）をクリックします。

[ヒットカウント（Hit Count）] 列は [名前（Name）] 列の右側にあり、ルールの合計ヒット数と最新のヒットの日付と時刻が表示されます。ヒットカウント情報は、切り替えボタンをクリックしたときに取得されます。

ヒットカウントの情報を使用して、次を行うことができます。

- ボタンの左側には、ヒットカウントが最後に更新されたときの情報が表示されます。最新の数字を取得するには、更新アイコン（）をクリックします。
- 特定のルールのヒット カウントの詳細表示を開くには、テーブルのヒット カウント番号をクリックして [ヒットカウント（Hit Count）] ダイアログ ボックスを開きます。ヒットカウント情報には、ヒットの回数と、ルールに一致した最後の接続の日付と時刻が含まれます。カウンタをゼロにリセットするには、[リセット（Reset）] をクリックします。

  一度にすべてのルールのヒットカウントをリセットする場合は、デバイスへの SSH セッションを開き、**clear rule hits** コマンドを発行します。
- 再度 [ヒットカウントの切り替え（Toggle Hit Counts）] アイコン（）をクリックし、テーブルから [ヒットカウント（Hit Count）] 列を削除します。

アクセス制御に関する Syslog メッセージのモニタリング

イベントはイベントビューアで確認するだけでなく、アクセス制御ルール、侵入ポリシー、ファイル/マルウェアポリシー、およびセキュリティ インテリジェンス ポリシーを設定してイベントを Syslog サーバーに送信することができます。イベントでは、次のメッセージ ID が使用されます。

- 430001：侵入イベント。
- 430002：接続の開始時にログに記録される接続イベント。
- 430003：接続の終了時にログに記録される接続イベント。
- 430004：ファイルイベント。
- 430005：マルウェア イベント。

CLI でのアクセス コントロール ポリシーのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、アクセス制御ポリシーと統計情報に関する詳細情報を取得することもできます。

- **show access-control-config** はアクセス制御ルールに関する概要情報とルールごとのヒット数を表示します。
- **show access-list** はアクセス制御ルールから生成されたアクセス制御リスト（ACL）を表示します。ACL は初期フィルタを提供し、できる限り迅速な決定を実現しようとするため、ドロップされる接続を調査する（および、そのために不必要にリソースを消費する）必要はありませんこの情報には、ヒット数が含まれます。

- **show rule hits** は、**show access-control-config** および **show access-list** で表示されるカウントよりも正確な、統合されたヒットカウントを表示します。ヒットカウントをリセットするには、**clear rule hits** コマンドを使用します。
- **show snort statistics** は主要なインスペクタである Snort インスペクションエンジンに関する情報を表示します。Snort は、アプリケーション フィルタリング、URL フィルタリング、侵入からの保護、ファイルおよびマルウェア フィルタリングを実装します。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィックフローに関する統計情報を表示します。
- **show ipv6 traffic** はデバイスを介した IPv6 トラフィックフローに関する統計情報を表示します。

アクセス制御の例

使用例の章には、アクセス制御ルールのいくつかの実装例が含まれています。次の例を参照してください。

- ネットワーク トラフィックを調べる方法 （55 ページ）。この例では、全体的な接続およびユーザ情報を収集するための基本的な考え方が示されています。
- 脅威をブロックする方法 （64 ページ）。この例では、侵入ポリシーを適用する方法が示されています。
- マルウェアをブロックする方法 （70 ページ）。この例では、ファイル ポリシーを適用する方法が示されています。
- アクセプタブル ユース ポリシー（URL フィルタリング）の実装方法 （73 ページ）。この例では、URL フィルタリングを実行する方法が示されています。
- アプリケーションの使用を制御する方法 （79 ページ）。この例では、アプリケーション フィルタリングを実行する方法が示されています。
- サブネットを追加する方法 （83 ページ）。この例では、トラフィック フローを許可するために必要なアクセスルールを含め、新しいサブネットをネットワーク全体に統合する方法が示されています。
- ネットワーク上のトラフィックをパッシブにモニタする方法 （90 ページ）

次に、その他の例を示します。

Trustsecセキュリティ グループ タグを使用したネットワーク アクセスの制御方法

Cisco TrustSec ネットワークでトラフィックを分類するために Cisco Identity Services Engine（ISE）を使用してセキュリティ グループ タグ（SGT）を定義して使用する場合は、一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、直接 IP アドレスではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。

セキュリティ グループ タグ（SGT）について

Cisco Identity Services Engine（ISE）では、セキュリティグループタグ（SGT）を作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。また、ユーザーアカウントに SGT を割り当て、SGT がユーザーのトラフィックに割り当てられるようにすることもできます。ネットワーク内のスイッチおよびルータがそのように設定されている場合、これらのタグは、ISE、Cisco TrustSec クラウドによって制御されるネットワークに入るときにパケットに割り当てられます。

Device Manager で ISE アイデンティティソースを設定すると、脅威に対する防御 システムは自動的に ISE から SGT のリストをダウンロードします。その後、アクセス制御ルールでトラフィックの一致条件として SGT を使用できます。

たとえば、[実稼働ユーザー（Production Users）] タグを作成し、192.168.7.0/24 ネットワークをタグに関連付けることができます。これは、ラップトップ、Wi-Fi クライアントなどのユーザーエンドポイントにそのネットワークを使用する場合に適しています。実稼働サーバー用に別のタグを作成し、関連するサーバーまたはサブネットの IP アドレスをそのタグに割り当てることができます。次に、脅威に対する防御 では、タグに基づいてユーザーネットワークから実稼働サーバーへのアクセスを許可またはブロックすることができます。ISE でタグに関連付けられているホストまたはネットワーク アドレスを後で変更する場合、脅威に対する防御 デバイスに定義されているアクセス制御ルールを変更する必要はありません。

脅威に対する防御 は、アクセス制御ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

1. パケット内で定義されている送信元 SGT タグ（存在する場合）。SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチとルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。

2. ISE セッションディレクトリからダウンロードされるユーザー セッションに割り当てられた SGT。この種の SGT 照合では、セッションディレクトリ情報をリッスンするオプションを有効にする必要がありますが、このオプションは最初に ISE アイデンティティソースを作成するときにデフォルトでオンになっています。SGT は、送信元または宛先と照合することができます。必須ではありませんが、通常は ISE アイデンティティソースを AD レルムとともに使用してパッシブ認証アイデンティティルールを設定し、ユーザ ID 情報を収集します。

3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックはSGTを使用するアクセス制御ルールと一致します。SGT は、送信元または宛先と照合することができます。

   ISE は、セキュリティグループ交換プロトコル（SXP）を使用して、SGT マッピングデータベースをネットワークデバイスに伝播します。ISE サーバーを使用するように 脅威に対する防御デバイスを設定する場合は、ISE から SXP トピックをリッスンするオプションをオンにする必要があります。そのため、脅威に対する防御 デバイスは、ISE からセキュリティグループタグとマッピングについて直接学習し、ISEが更新されたセキュリティグループタグとマッピングを公開するたびに通知を受け取ります。これにより、デバイス上でセキュリティグループタグのリストが最新の状態に維持されるため、脅威に対する防御は、ISE で定義されたポリシーを効果的に適用できるようになります。

セキュリティ グループ タグ（SGT）に基づくアクセス制御の設定

セキュリティ グループ タグ（SGT）を一致基準として使用するアクセス制御ルールを設定するには、最初に ISE サーバーから SGT マッピングを取得するようにデバイスを設定する必要があります。

次の手順では、SXP で公開されている SGT から IP アドレスへのマッピングを含め、ISE で定義されているすべてのマッピングを取得するという前提に基づいたエンドツーエンドのプロセスについて説明します。または、下記の手順も実行できます。

- パケット内の SGT 情報のみを使用し、ISE からダウンロードされたマッピングを使用しない場合は、単に SGT グループ ダイナミック オブジェクトを作成し、それらをアクセス制御ルールの送信元 SGT 条件として使用します。この場合、送信元条件としてのみ SGT タグを使用できます。これらのタグは、宛先の基準に一致しません。
- パケットとユーザーセッション SGT のマッピングのみで SGT を使用する場合は、ISE アイデンティティソースの SXP トピックを登録するオプションを有効にする必要はなく、SXP マッピングを公開するように ISE を設定する必要もありません。この情報は送信元と宛先の両方の一致条件に使用できます。

始める前に

ここでは、ネットワークに Cisco TrustSec がすでに設定されていて、ポリシー適用ポイントとして 脅威に対する防御デバイスを追加するだけであることを前提としています。Cisco TrustSec を展開していない場合は、ISE から開始し、ネットワークを設定してから、この手順に戻ります。Cisco TrustSec の説明は、このドキュメントの範囲外です。

手順

ステップ 1 SGT が定義されていること、ISE が SXP トピックをパブリッシュするように正しく設定されていること、および必要な静的マッピングが設定されていることを確認します。

ISE でのセキュリティ グループと SXP パブリッシングの設定（634 ページ）を参照してください。

ステップ 2 SXP トピックをリッスンするように Identity Services Engine オブジェクトを更新します。

ISE を使用して、ユーザーセッション SGT マッピング、SXP を介したスタティック SGT から IP アドレスへのマッピング、またはその両方を取得できます。デフォルトでは、ISE アイデンティティソースを設定すると、ユーザーセッションマッピングのみが取得されます。ISE から SXP トピックをリッスンするには、オプションを有効にする必要があります。

a) **[オブジェクト（Objects）]**>**[アイデンティティソース（Identity Sources）]** を選択します。
b) ISE オブジェクトを編集します。まだ設定していない場合は、**[+]**>**[Identity Services Engine]** をクリックし、Identity Services Engine の設定 （206 ページ）を参照してください。
c) [サブスクライブ対象（Subscribe To）] で、[SXP トピック（SXP Topic）] を選択します。

パッシブ認証を使用している場合またはユーザーと SGT のマッピングが必要な場合は、[セッションディレクトリのトピック（Session Directory Topic）] が選択されていることも確認してください。

d) [OK] をクリック

ステップ 3 変更を展開し、システムが ISE からタグとマッピングをダウンロードするのを待ちます。

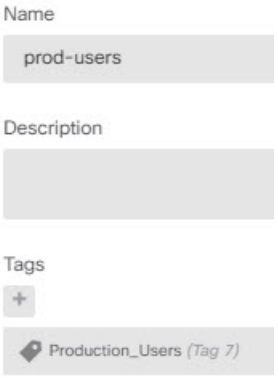
ISE アイデンティティソースを設定して変更を展開すると、ISE サーバーからセキュリティグループタグ（SGT）情報が取得されます。ダウンロードは、変更を展開するまで行われません。

ステップ 4 アクセス制御ルールに必要な SGT グループオブジェクトを作成します。

ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

オブジェクトの数と内容は、作成するアクセス制御ルールによって異なります。次のプロセスを繰り返して、必要なすべてのオブジェクトを作成してください。

a) **[オブジェクト（Objects）]** > **[SGTグループ（SGT Groups）]** を選択します。
b) [+] をクリックして新しいオブジェクトを追加するか、既存のオブジェクトを編集します。
c) 新しいオブジェクトの場合、名前を入力し、任意で説明を入力します。
d) [タグ（Tags）] で、[+] をクリックし、グループに含める必要があるすべてのタグを選択します。



e) [OK] をクリック

ステップ 5 SGT グループオブジェクトを使用するアクセス制御ルールを作成します。

たとえば、以下のルールにより、実稼働ユーザーから実稼働サーバーへのトラフィックが許可されます。ルールは SGT に完全に依存します。送信元/宛先インターフェイスやその他の基準によって制限を受けることはありません。そのため、ルールはさまざまなインターフェイスからのトラフィックに動的に適用され、ISE でセキュリティグループのメンバーシップを変更するときに適用されます。パケットに送信元 SGT が明示的に含まれていない場合は、パケットの IP アドレスを、ユーザーセッション情報または SXP 公開マッピングから取得される、SGT から IP アドレスへのマッピングと比較することによって、送信元/宛先の照合が行われます。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。
b) [+] をクリックして新しいルールを作成するか、既存のルールを編集します。
c) ルール名を入力し、アクションとして [許可（Allow）] を選択します。
d) [送信元/宛先（Source/Destination）] タブで、**[送信元（Source）]** > **[SGTグループ（SGT Groups）]** の [+] をクリックし、実稼働ユーザー用に作成したオブジェクトを選択します。
e) [送信元/宛先（Source/Destination）] タブで、**[宛先（Destination）]** > **[SGTグループ（SGT Groups）]** の [+] をクリックし、実稼働サーバー用に作成したオブジェクトを選択します。
f) 必要に応じて他のオプションを設定します。たとえば、ロギングを有効にして、侵入ポリシーを適用することができます。
g) [OK] をクリック

ステップ 6 設定を展開します。

ISE でのセキュリティ グループと SXP パブリッシングの設定

Cisco Identity Services Engine（ISE）では、TrustSec ポリシーとセキュリティグループタグ（SGT）を作成するために実行を必要とする設定が多数あります。TrustSec の実装の詳細については、ISE のマニュアルを参照してください。

次の手順では、脅威に対する防御 デバイスがスタティック SGT から IP アドレスへのマッピングをダウンロードして適用できるようにするために ISE で設定する必要があるコア設定のハイライトを示します。これは、アクセス制御ルールでの送信元と宛先 SGT の照合に使用できます。詳細については、ISE のマニュアルを参照してください。

この手順のスクリーンショットは、ISE 2.4 に基づいています。これらの機能にアクセスするための正確な手順は後続のリリースで変更される可能性がありますが、概念と要件は同じです。ISE 2.4 以降、特に 2.6 以降が推奨されますが、ISE 2.2 パッチ 1 以降でもこの設定は動作します。

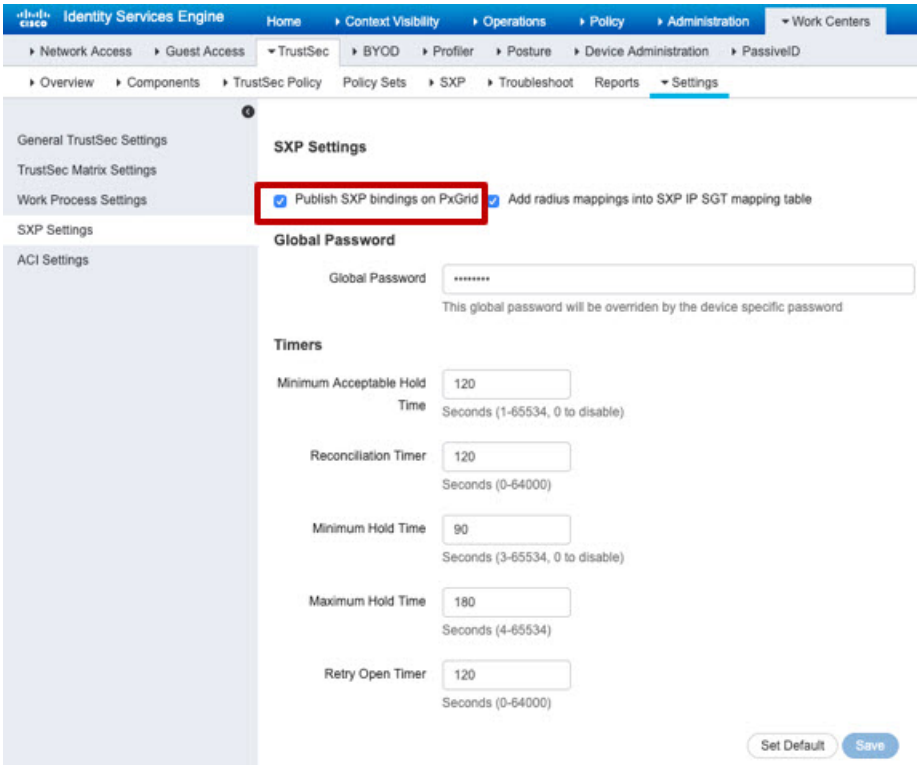
始める前に

SGT から IP アドレスへのスタティックマッピングを公開し、ユーザーセッションからと SGT へのマッピングを取得して脅威に対する防御デバイスがそれらを受信できるようにするには、ISE Plus ライセンスが必要です。

手順

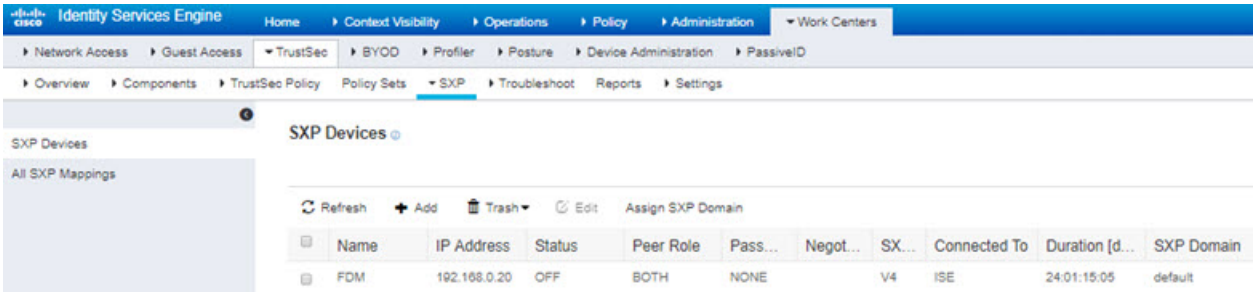
ステップ 1 **[ワークセンター（Work Centers）]** > **[TrustSec]** > **[設定（Settings）]** > **[SXP設定（SXP Settings）]** を選択し、[PxGridでSXPバインディングを公開（Publish SXP Bindings on PxGrid）] オプションを選択します。

このオプションにより、ISE は SXP を使用して SGT マッピングを送信します。リストから SXP トピックまでを "確認する" には、Threat Defense デバイスに対してこのオプションを選択する必要があります。このオプションは、Threat Defense デバイスが静的 SGT-to-IP アドレスマッピング情報を取得するために選択する必要があります。単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

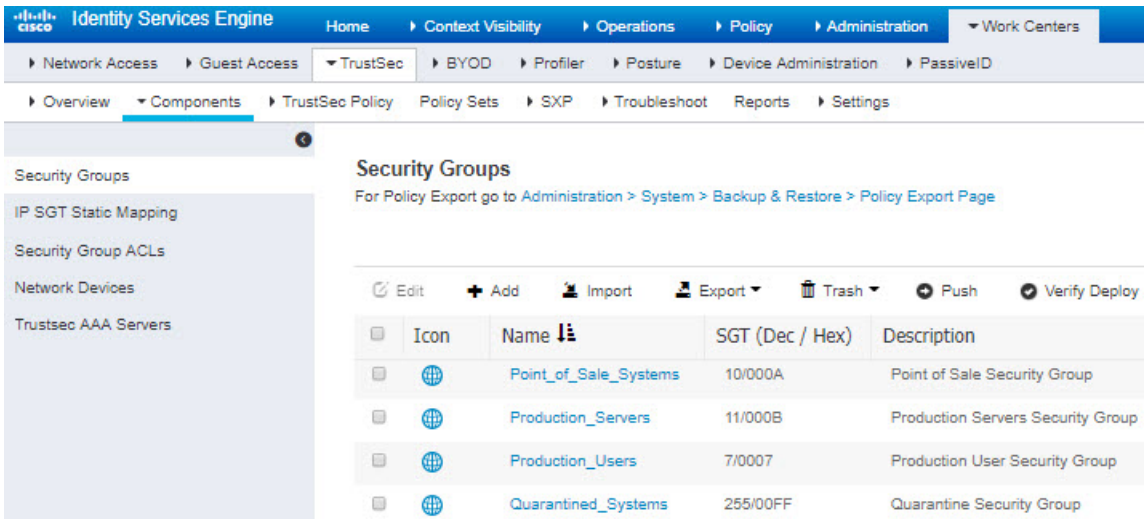


ステップ 2 **[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）]** を選択し、デバイスを追加します。

これは実際のデバイスである必要はありませんが、脅威に対する防御 デバイスの管理 IP アドレスを使用することもできます。このテーブルには、ISE が静的 SGT-to-IP アドレスマッピングをパブリッシュするためのデバイスが 1 つ以上必要です。単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

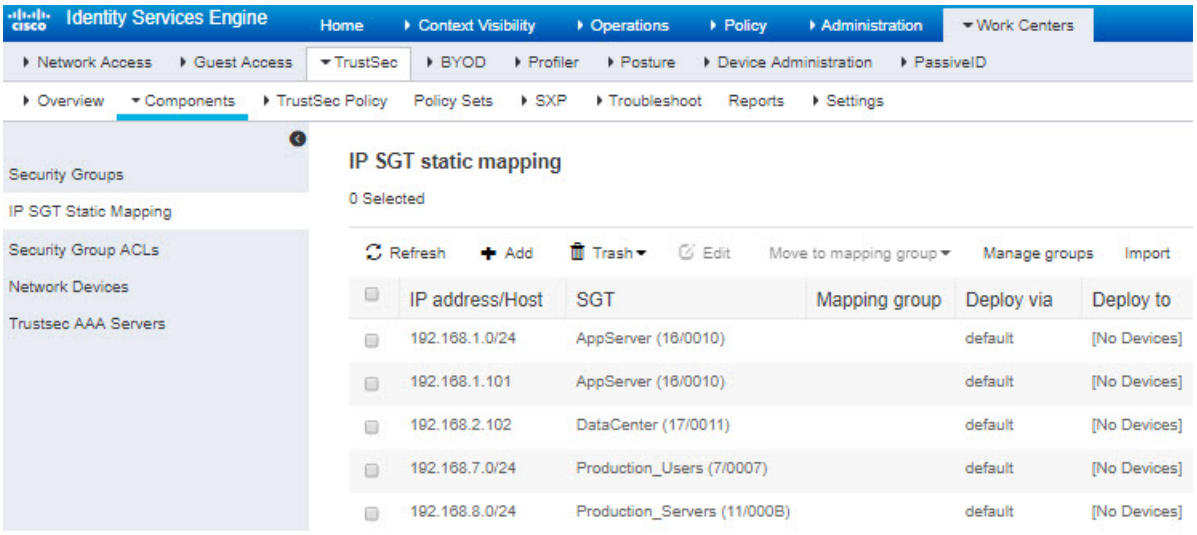


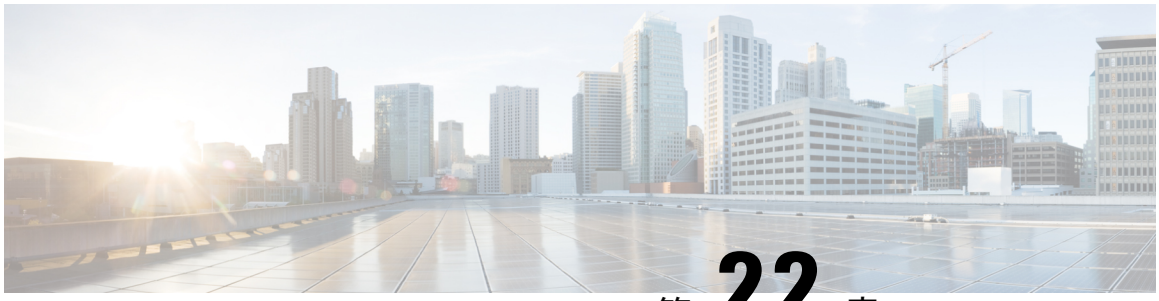
ステップ 3 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]** の順に選択し、セキュリティグループタグが定義されていることを確認します。必要に応じて新しいタグを作成します。



ステップ 4 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）]** を選択し、ホストとネットワーク IP アドレスをセキュリティ グループ タグにマッピングします。

単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Components
TrustSec Policy
Policy Sets
SXP
Troubleshoot
Reports
Settings
Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers
IP SGT static mapping
0 Selected
Refresh
Add
Trash
Edit
Move to mapping group
Manage groups
Import
IP address/Host
SGT
Mapping group
Deploy via
Deploy to
192.168.1.0/24
AppServer (16/0010)
default
[No Devices]
192.168.1.101
AppServer (16/0010)
default
[No Devices]
192.168.2.102
DataCenter (17/0011)
default
[No Devices]
192.168.7.0/24
Production_Users (7/0007)
default
[No Devices]
192.168.8.0/24
Production_Servers (11/000B)
default
[No Devices]



第 22 章

侵入ポリシー

次のトピックでは、侵入ポリシーと密接に関連付けられているネットワーク分析ポリシー（NAP）について説明します。侵入ポリシーには、脅威についてトラフィックをチェックし、攻撃が判明したトラフィックをブロックするルールが含まれます。ネットワーク分析ポリシーは、トラフィックを正規化してプロトコルの異常を識別することによってさらに検査するためにトラフィックの準備を行う、トラフィックの前処理を制御します。

前処理と侵入検査を非常に密接に関連しているため、1 つのパケットを調べるネットワーク分析と侵入ポリシーはお互いを補完する必要があります。

侵入ポリシーとネットワーク分析ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、共同で侵入の脅威を検出し、防ぎます。

- ネットワーク分析ポリシー（NAP）では、トラフィックの復号化および前処理の方法について、特に侵入の試行を示す可能性がある異常なトラフィックをさらに評価できるよう、制御します。
- 侵入ポリシーでは、侵入ルールと呼ばれる侵入やプリプロセッサのルールを使用し、パターンに基づいて攻撃がないかデコードされたパケットを調べます。ルールでは、脅威となるトラフィックを防いで（ドロップして）イベントを生成したり、単に検出（警告）してイベントの生成のみを行うことができます。

システムがトラフィックを分析するとき、ネットワーク分析の復号化および前処理のフェーズは、侵入防御のフェーズより前に、個別に発生します。ネットワーク分析ポリシーと侵入ポリシーは、共同で広範かつ深いパケット検査を提供します。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、通知および防御に役立ちます。

システム定義のネットワーク分析および侵入ポリシー

システムには、相互に補完して動作する、同じ名前のネットワーク分析と侵入ポリシーのいくつかのペアが含まれています。たとえば「バランスのとれたセキュリティと接続性」という名前の NAP と侵入ポリシーの両方があり、一緒に使用されることを意図しています。システム提供のポリシーは、Cisco Talos Intelligence Group（Talos）によって設定されます。これらのポリシーに対して Talos は侵入とプリプロセッサルールの状態を設定し、プリプロセッサの最初の設定とその他の高度な設定を行います。

新たな脆弱性が既知になると、Talos は侵入ルールの更新をリリースします。これらのルール更新により、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやプリプロセッサルールの新規作成または更新、既存ルールのステータスの変更、デフォルトのポリシー設定の変更が実施されます。ルールの更新はまた、システム提供のポリシーからルールを削除、新しいルールのカテゴリを提供、デフォルトの変数セットを変更できます。

手動で、ルールデータベースを更新したり、定期的な更新スケジュールを設定できます。有効にするには更新を展開する必要があります。システムデータベースの更新についての詳細は、システム データベースの更新 （973 ページ）を参照してください。

次にシステム提供のポリシーについて示します。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。これらを一緒に使用すると、ほとんどの種類のネットワークおよび展開に適した出発点として機能します。[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーがデフォルトとして使用されます。

[セキュリティよりも接続性を優先（Connectivity Over Security）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続性、すべてのリソースを取得する機能が、ネットワークインフラストラクチャのセキュリティよりも優先されるネットワーク向けに作られています。この侵入ポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

[接続性よりもセキュリティを優先（Security over Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先されるネットワーク向けに作られています。この侵入ポリシーは、正式なトラ

フィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

[最大検出（Maximum Detection）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティが、運用に対する影響が大きい、[接続性よりもセキュリティを優先（Security Over Connectivity）] ポリシーで考慮されるセキュリティよりもさらに重視されるネットワーク向けに作られています。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイトキット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

検査モード：防御と検出

デフォルトでは、侵入防御システム（IPS）を実装するため、すべての侵入ポリシーが防御モードで動作します。防御インスペクションモードでは、トラフィックを切断するアクションの侵入ルールと接続が一致する場合、接続は能動的にブロックされます。

一方、ネットワーク上で侵入ポリシーの影響をテストするには、侵入検知システム（IDS）を実装する「検出」にモードを変更します。このインスペクションモードでは、ドロップルールはアラートルールと同様に扱われます。この場合、一致する接続が通知されますが、アクションの結果がブロックされ、実際に接続がブロックされることはありません。

侵入ポリシーごとにインスペクションモードを変更するため、防御と検出を混在させることができます。

Snort 3 ネットワーク分析ポリシー（NAP）にもインスペクションモードがあります。侵入ポリシーとは異なり、NAP ポリシーはグローバルであるため、すべての NAP 処理を防御モードまたは検出モードで実行する必要があります。侵入ポリシーに使用するのと同じモードを使用する必要があります。防御ポリシーと検出ポリシーが混在している場合は、最も制限の厳しい侵入ポリシーに一致するように [防御（Prevention）] を選択します。

侵入ルールおよびプリプロセッサ ルール

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

システムには、Cisco Talos Intelligence Group（Talos）によって作成された次のタイプのルールが含まれています。

- 侵入ルール。共有オブジェクト ルールおよび標準のテキスト ルールに細分されます。
- プリプロセッサルール。プリプロセッサと、ネットワーク分析ポリシーのパケットデコーダ検出オプションが関連付けられたルールです。デフォルトではほとんどのプリプロセッサ ルールは無効です。

ここでは、侵入ルールについてより詳細に説明します。

侵入ルール属性

侵入ポリシーを表示すると、脅威を特定するために利用できるすべての侵入ルールのリストが示されます。

各ポリシーのルールのリストは同じです。異なる点は、各ルールに設定されたアクションです。30,000 を超えるルールがあるため、リスト全体をスクロールするには時間がかかります。ルールは、リストをスクロールしていくと順に表示されます。

次に、各ルールを定義する属性を示します。

> (シグニチャの説明)

左の列の [>] ボタンをクリックして、署名の説明を開きます。説明は、トラフィックとルールを照合するために、Snort インスペクション エンジンによって使用されます。コードの説明はこのドキュメントの範囲外ですが、『Management Center Configuration Guide』で詳しく説明しています。http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html からご使用のソフトウェアのバージョン用のブックを選択してください。侵入ルールの編集についての情報を探します。

署名には、特定の項目の変数が含まれています。詳細については、デフォルトの侵入変数セット （643 ページ）を参照してください。

GID

ジェネレータ識別子（ID）。この数は、ルールを評価し、イベントを生成する、システムコンポーネントを示します。1 は標準テキスト侵入ルール、3 は共有オブジェクト侵入ルールを示します（これらのルールタイプの違いは Device Manager ユーザーにとって意味はありません）。これらは、侵入ポリシーを設定するときに対象となる主なルールです。その他の GID の詳細については、ジェネレータ識別子 （644 ページ）を参照してください。

SID

Snort 識別子（ID）。署名 ID とも呼ばれます。1000000 より小さい Snort ID が Cisco Talos Intelligence Group（Talos） によって作成されました。

操作（Action）

選択した侵入ポリシーでのこのルールの状態。各ルールに対し、このポリシー内のルールのデフォルトアクションに「（デフォルト）」が追加されます。ルールをデフォルトの設定に戻すには、このアクションを選択します。指定できるアクションは、次のとおりです。

- [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。

ステータス（Status）

Snort 2 ルールの場合、[ステータス（Status）] は個別の列になっています。ルールに対するデフォルトのアクションを変更すると、この列に「上書き済み」と表示されます。それ以外の場合は、この列は空です。

Snort 3 ルールの場合、[上書き済み（Overridden）] ステータスは [アクション（Action）] 属性の下部に表示されます（変更した場合）。

メッセージ（Messages）

これはルールの名前で、ルールによってトリガーされたイベントにも表示されます。メッセージは通常、署名が一致した脅威を識別します。それぞれの脅威の詳細についてインターネットで検索できます。

デフォルトの侵入変数セット

侵入ルールの署名には、特定の項目の変数が含まれます。変数のデフォルト値を次に示します。$HOME_NET と $EXTERNAL_NET が最もよく使用される変数です。プロトコルはポート番号とは別々に指定されるため、ポート変数は数字のみです。

- $DNS_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $EXTERNAL_NET = 任意の IP アドレス。
- $FILE_DATA_PORTS = $HTTP_PORTS、143、110。
- $FTP_PORTS = 21、2100、3535。
- $GTP_PORTS = 3386、2123、2152。
- $HOME_NET = 任意の IP アドレス。
- $HTTP_PORTS = 次の番号の 144 個のポート：36、80 ～ 90、311、383、443、555、591、593、631、666、801、808、818、901、972、1158、1212、1220、1414、1422、1533、1741、1830、1942、2231、2301、2381、2578、2809、2980、3029、3037、3057、3128、3443、3507、3702、4000、4343、4848、5000、5117、5222、5250、5450、5600、5814、6080、6173、6767、6988、7000、7001、7005、7071、7080、7144、7145、7510、7770、7777 ～ 7779、8000、8001、8008、8014、8015、8020、8028、8040、8060、8080 ～ 8082、8085、8088、8118、8123、8161、8180 ～ 8182、8222、8243、8280、8300、8333、8344、8400、8443、8500、8509、8787、8800、8888、8899、8983、9000、9002、9060、9080、9090、9091、9111、9290、9443、9447、9710、9788、9999、10000、11371、12601、13014、15489、19980、23472、29991、33300、34412、34443、34444、40007、41080、44449、50000、50002、51423、53331、55252、55555、56712。
- $HTTP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $ORACLE_PORTS = 任意。
- $SHELLCODE_PORTS = 180。
- $SIP_PORTS = 5060、5061、5600。

- $SIP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SMTP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SNMP_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SQL_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $SSH_PORTS = 22。
- $SSH_SERVERS = $HOME_NET（任意の IP アドレスを示します）。
- $TELNET_SERVERS = $HOME_NET（任意の IP アドレスを示します）。

ジェネレータ識別子

ジェネレータ識別子（GID）は、侵入ルールを評価し、イベントを生成するサブシステムを識別します。標準のテキスト侵入ルールのジェネレータ ID は 1、共有オブジェクト侵入ルールのジェネレータ ID は 3 です。また、各種プリプロセッサに対して複数のルール セットがあります。次の表で、GID について説明します。

表 *11 :* ジェネレータ *ID*

ID	コンポーネント
1	標準テキスト ルール。
2	タグ付きパケット。 （タグ付きセッションからパケットを生成するタグ ジェネレータのルール。）
3	共有オブジェクト ルール。
102	HTTP デコーダ。
105	バック オリフィス探知機。
106	RPC デコーダ。
116	パケット デコーダ。
119、120	HTTP インスペクト プリプロセッサ （GID 120 ルールは、サーバ固有の HTTP トラフィックに関連しています）。
122	ポートスキャン ディテクタ。
123	IP 最適化。
124	SMTP デコーダ。 （SMTP 動詞に対するエクスプロイト。）

ID	コンポーネント
125	FTP デコーダ。
126	Telnet デコーダ。
128	SSH プリプロセッサ。
129	ストリーム プリプロセッサ。
131	DNS プリプロセッサ。
133	DCE/RPC プリプロセッサ。
134	ルール遅延、パケット遅延。 （これらのルールのイベントは、ルール遅延中断（SID 1）または侵入ルールのグループの再有効化（SID 2）のとき、またはパケット遅延のしきい値を超えた（SID 3）ためにシステムがパケットの検査を中止したときに生成されます）。
135	レートベースの攻撃ディテクタ。 （ネットワーク上のホストへの過剰な接続。）
137	SSL プリプロセッサ。
138、139	機密データ プリプロセッサ。
140	SIP プリプロセッサ。
141	IMAP プリプロセッサ。
142	POP プリプロセッサ。
143	GTP プリプロセッサ。
144	Modbus プリプロセッサ。
145	DNP3 プリプロセッサ。

ネットワーク分析ポリシー

ネットワーク分析ポリシーはトラフィック前処理を制御します。プリプロセッサは、トラフィックを正規化し、プロトコル異常を識別することにより、トラフィックがさらに検査されるように準備します。ネットワーク分析関連の前処理が行われるのは、セキュリティインテリジェンスによるドロップとSSL復号の後ですが、アクセス制御と侵入またはファイル検査の前です。

デフォルトでは、システムは [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーを使用して、アクセス制御ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、アクセス制御ルールで侵入ポリシーを設

定する場合、システムは、適用される最も積極的な侵入ポリシーに一致するネットワーク分析ポリシーを使用します。たとえば、アクセス制御ルールで [接続性よりセキュリティを優先（Security over Connectivity）] ポリシーと [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーの両方を使用する場合、システムはすべてのトラフィックに対して [接続性よりセキュリティを優先（Security over Connectivity）] NAP を使用します。Snort 3 カスタム侵入ポリシーの場合、この割り当ては、侵入ポリシーに割り当てられた基本テンプレートポリシーに従って行われます。

Snort 3 を使用している場合、ポリシーを明示的に選択し、オプションで設定をカスタマイズできます。侵入ポリシーを直接使用するか、カスタム侵入ポリシーのベースポリシーとして使用するかにかかわらず、デバイスを通過するほとんどのトラフィックに使用する侵入ポリシーと名前が一致するポリシーを選択することを推奨します。その後、インスペクションモードを変更したり、ネットワーク上のトラフィックを考慮して特定のインスペクタまたはバインダ設定を調整したりできます。

さらに、侵入ポリシーでプリプロセッサルールを有効にしているかどうかも考慮します。プリプロセッサを必要とするルールを有効にする場合は、NAP で対応するインスペクタも有効にしてください。インスペクタごとに、検査対象のポート（バインダ）を含むインスペクタの属性を調整して、ネットワークのインスペクタの動作もカスタマイズできます。

（注） Snort 2 を使用している場合、アクセス制御ルールで適用する最も制限の厳しい侵入ポリシーとして同じ名前の NAP ポリシーが使用されるため、インスペクタやバインダの設定は編集できません。

侵入ポリシーのためのライセンス要件

アクセス制御ルールの侵入ポリシーを適用するには、**IPS** ライセンスを有効にする必要があります。ライセンスの設定については、オプション ライセンスの有効化または無効化（109 ページ）を参照してください。

ネットワーク分析ポリシーには追加ライセンスは必要ありません。

アクセス制御ルールでの侵入ポリシーの適用

侵入ポリシーをネットワーク トラフィックに適用するには、トラフィックを許可するアクセス制御ルール内でポリシーを選択します。侵入ポリシーを直接指定しません。

保護するネットワークの相対的なリスクに基づいた可変の侵入保護を提供する別の侵入のポリシーを割り当てることができます。たとえば、内部ネットワークと外部ネットワーク間のトラフィックには、より厳しい [接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーを使用する場合があります。一方で、内部ネットワーク間のトラフィックに対しては、より緩やかな [セキュリティよりも接続性を優先（Connectivity over Security）] ポリシーを適用する場合があります。

また、すべてのネットワークに対して同じポリシーを使用することで、構成を簡略化することもできます。たとえば、[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーは、接続に過度に影響を与えずに良好な保護を提供するための設計です。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

ステップ 2 トラフィックを**許可**する、新しいルールを作成するか、既存のルールを編集します。

既定のアクションを許可する場合は、既定のアクションで侵入ポリシーを指定することもできます。

トラフィックを信頼またはブロックするルールに侵入ポリシーを適用することはできません。

ステップ 3 [侵入ポリシー（Intrusion Policy）] タブをクリックします。

ステップ 4 **[侵入ポリシー（Intrusion Policy）] > [オン（On）]** を選択し、トラフィックの照合に使用する侵入検査ポリシーを選択します。

Snort 2 と Snort 3 の切り替え

Snort は製品の主要インスペクションエンジンです。Snort のバージョンは自由に切り替えることができますが、Snort 2.0 の一部の侵入ルールは Snort 3.0 に存在しない場合があり、その逆の場合もあります。これらのルールのいずれか 1 つのルールアクションを変更した場合、Snort 3 に切り替えて Snort 2 に戻るか、再度 Snort 3 に戻ると、その変更は保持されません。両方のバージョンに存在するルールのルールアクションに対する変更は保持されます。Snort 3 と Snort 2 のルール間マッピングは 1 対 1 または 1 対多にすることができるため、変更の保存はベストエフォートベースで行われることに注意してください。

Snort バージョンを変更すると、システムは自動展開を実行して変更を実装します。タスクリストに進行状況が表示されます。これらのタスクは、Snortバージョンの変更と自動展開（Snortバージョン切り替え）です。展開と、Snort を停止して再起動する必要があるため、VPN を含むすべての既存の接続がドロップされ、再確立する必要があります。これにより、一時的なトラフィック損失が発生します。

（注） Snort のバージョンを切り替えようとして失敗した場合、破棄できない保留中の変更が残り、後続の切り替えを試みることができなくなります。この場合は、ToggleInspectionEngine API を使用して切り替えを完了する必要があります。これは API Explorer から使用できます。bypassPendingChangeValidation 属性を TRUE に設定する必要があります。

始める前に

現在有効になっているSnortのバージョンを確認するには、次の手順を使用するか、**[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。テーブルの上にある [Snortバージョン（Snort Version）] 行を探します。現在のバージョンは、完全なバージョン番号の最初の番号です。たとえば、2.9.17-95 は Snort 2 バージョンです。

デバイスがエアギャップネットワークにある場合は、バージョンを切り替える前に、新しいバージョン用の最新のルールパッケージを手動でアップロードすることを検討してください。

2.0 にダウングレードすると、作成したカスタム侵入ポリシーはすべて、カスタムポリシーで使用される基本ポリシーに変換されます。可能なかぎり、ルール アクション オーバーライドは保持されます。複数のカスタムポリシーが同じ基本ポリシーを使用する場合は、最も多くのアクセス制御ポリシーで使用されるカスタムポリシーのオーバーライドが保持され、その他のカスタムポリシーのオーバーライドは失われます。これらの「重複」ポリシーを使用していたアクセス制御ルールは、最もよく使用されるカスタムポリシーから作成された基本ポリシーを使用するようになります。すべてのカスタムポリシーが削除されます。カスタムポリシーを、後でインポートできるように保存しておくには、Snort 3 に切り替えた後に、Threat Defense API を使用して設定をエクスポートします。

さらに、2.0 にダウングレードすると NAP のカスタマイズがすべて削除され、システムはアクセス制御ルールで使用される侵入ポリシーに基づいて最適な NAP を使用するように切り替わります。

アクティブ認証のホスト名リダイレクトには Snort 3 も必要で、Snort 2 に切り替えると削除されます。

Snort のバージョンを切り替えるには、保留中の変更を展開する必要があります。

手順

ステップ 1 [デバイス（Device）] を選択してから、[更新（Updates）] のサマリーで [設定の表示（View Configuration）] をクリックします。

[侵入ルール（Intrusion Rule）] グループを確認します。Snort の現在のバージョンが表示されます。

ステップ 2 [侵入ルール（Intrusion Rule）] グループで、[Snort 3.0へのアップグレード（Upgrade to Snort 3.0）] または [Snort 2.0へのダウングレード（Downgrade to Snort 2.0）] をクリックして、Snort のバージョンを変更できます。

ステップ 3 アクションを確認するプロンプトが表示されたら、最新の侵入ルールパッケージを取得するオプションを選択し、[はい（Yes）] をクリックします。

最新のルールパッケージを入手することをお勧めします。システムはアクティブな Snort バージョンのパッケージのみをダウンロードするため、切り替え先のSnortバージョン用の最新パッケージがインストールされている可能性は低くなります。

侵入ポリシーを編集するには、バージョンを切り替えるタスクが完了するまで待つ必要があります。

侵入イベントの Syslog の設定

侵入ポリシーの外部 syslog サーバを設定して Syslog サーバに侵入イベントを送信できます。サーバに送信される侵入イベントを取得するために侵入ポリシーで Syslog サーバを設定する必要があります。アクセス ルールで syslog サーバを設定し、侵入イベントではなく、接続イベントのみ syslog サーバに送信します。

複数の syslog サーバーを選択する場合、イベントは各サーバーに送信されます。

侵入イベントのメッセージ ID は 430001 です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** の順に選択します。

ステップ 2 **[侵入ポリシーの設定（Intrusion Policy Settings）]** ボタン（⚙）をクリックして syslog を設定します。

ステップ 3 [侵入イベント送信先（Send Intrusion Events To）] の下にある [+] ボタンをクリックして、syslog サーバーを定義するサーバーオブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しい Syslog サーバーの作成（Create New Syslog Server）] をクリックして作成します。

ステップ 4 [OK] をクリックします。

ネットワーク分析ポリシーの設定（Snort 3）

ネットワーク分析ポリシー（NAP）は、デバイスで許可されているすべての接続に適用されます。NAP は、有効になっているインスペクタと、インスペクタで使用される属性の値を決定します。バインダは、さまざまなインスペクタに関連付ける必要があるポートとプロトコルを決定します。

アクセス制御ルールで適用する侵入ポリシーと NAP を調整します。

- アクセス制御ルールで単一の侵入ポリシーを使用する場合は、同じ名前の NAP を選択します。次に、侵入ポリシーの設定に基づいてインスペクタと属性を調整します。たとえば、CIP などの特定のインスペクタに対して侵入ルールを有効にする場合は、NAP でそのインスペクタを有効にしてください。
- 複数の侵入ポリシーを使用する場合は、使用する最も厳密な侵入ポリシーに一致する NAP を選択します。

- カスタム侵入ポリシーを使用する場合は、カスタム侵入ポリシーの基本侵入ポリシーに基づいて NAP を選択します。
- インスペクタやバインダをカスタマイズする必要がない場合は、侵入ポリシーの使用に基づいて最適な NAP を自動的に選択するようにシステムを設定することを検討してください。これがデフォルトのオプションです。

始める前に

これを防止しない限り、システムは定期的にインスペクションルールに LSP の更新をダウンロードします。LSP の更新では、インスペクタと属性を追加または削除したり、属性のデフォルト設定を変更したりできます。削除されたインスペクタをオーバーライドした場合、それらのオーバーライドは保持され、インスペクタがサポートされなくなったことを示す警告が表示されます。この場合、インスペクタを削除し、その他のフラグ付き調整を行って、NAP が完全に有効であることを確認します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

テーブルの上に表示されている Snort のバージョンが 3.x であることを確認します。

ステップ 2 [侵入ポリシーの設定（Intrusion Policy Settings）]（⚙）ボタンをクリックします。

ステップ 3 [デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）] で、次のいずれかを選択します。

- [自動（Auto）]：アクセス制御ルールで適用される最も使用されている侵入ポリシー（またはカスタムルールの基本ポリシー）に一致する NAP を自動的に選択します。侵入ポリシーを適用しない場合は、Balanced Security および Connectivity NAP が使用されます。NAP は防御モードで実行され、侵入またはバインダの設定はカスタマイズできません。この手順の残りの部分は、自動モードで実行している場合は当てはまりません。
- [カスタム（Custom）]：使用する NAP を明示的に選択します。別のポリシーを選択するには、ポリシー名の横にある [編集（Edit）] リンクをクリックします。次に、インスペクションモードを選択し、次の手順の説明に従い、インスペクタとバインダの設定をカスタマイズできます。

ステップ 4 [ネットワーク分析ポリシーの編集（Edit Network Analysis Policy）] ダイアログボックスで、ポリシーを選択し、設定を行います。

a) [ネットワーク分析ポリシー（Network Analysis Policy）] で、許可されたすべての接続にグローバルに適用するポリシーを選択します。

b) [インスペクションモード（Inspection Mode）] を選択します。

インスペクションモードは、非準拠トラフィックの処理方法を決定します。最適な結果を得るには、侵入ポリシーで使用するものと同じインスペクションモードを使用します。

- [防御（Prevention）]：ポリシーの設定に基づいて、デコーダ、正規化、またはプロトコルの異常をブロックします。SSL復号ポリシーを有効にする場合またはアクセスコントロール ポリシー設定で [TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）] オプションを有効にする場合は、このオプションを使用する必要があります。
- [検出（Detection）]：デコーダ、正規化、またはプロトコルの異常についてアラートを発行するだけです。トラフィックはブロックしないでください。

c) （オプション）インスペクタとバインダへのオーバーライドを設定および管理します。

- オーバーライドを編集するには、インスペクタおよびバインダオーバーライドの設定（651 ページ）を参照してください。
- スキーマまたはオーバーライドをダウンロードするには、オーバーライドとスキーマのダウンロード（654 ページ）を参照してください。
- オーバーライドをアップロードするには、オーバーライドのアップロード（654 ページ）を参照してください。
- すべてのオーバーライドをリセットするには、NAP ファイルの上にある [インスペクタ/バインダのオーバーライドのリセット（Reset Inspector/Binder Overrides）] リンクをクリックします。リセットの確認を求められます。コマンド名に示されているように、削除はインスペクタまたはバインダに限定されます。たとえば、すべてのバインダオーバーライドを削除しても、インスペクタオーバーライドは変更されません。
- 選択したインスペクタに対するすべての変更を元に戻すには、[インスペクタをデフォルトにリセット（Reset Inspector to Defaults）] をクリックします。
- オーバーライドがあるインスペクタだけが表示されるようにビューをフィルタ処理するには、[オーバーライドのみ表示（Show Only Overrides）] をクリックします。[すべてのインスペクタを表示（Show All Inspectors）] をクリックして、フィルタを削除します。

d) [OK] をクリックします。

インスペクタおよびバインダオーバーライドの設定

基本 NAP を選択すると、その基準ポリシーに含まれるインスペクタ設定が選択されます。ほとんどの場合、これらは適切な設定です。

ただし、選択した NAP の設定はオーバーライドできます。たとえば、個々のインスペクタを有効または無効にしたり、属性やバインダの値を変更したりできます。

次の手順では、オーバーライドを直接設定する方法について説明します。または、スキーマをダウンロードし、オフラインで変更を行い、オーバーライドをアップロードできます。別のデバイスからダウンロードしたオーバーライドをアップロードすることもできます。

始める前に

各インスペクタ、バインダ、および属性の説明は、このドキュメントの範囲外です。例などの詳細については、https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference.html にある Snort 3 インスペクタリファレンス [英語] を参照してください。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択し、[侵入ポリシーの設定（Intrusion Policy Settings）] ボタン（⚙）をクリックし、NAP 設定に [カスタム（Custom）] を選択し、ポリシー名の横にある [編集（Edit）] リンクをクリックします。

ステップ 2 変更する設定を含むタブをクリックします。

- [インスペクタ（Inspectors）]：インスペクタは、FTP などの特定のタイプのトラフィックについてプロトコル異常を検査します。
- [バインダ（Binders）]：バインダインスペクタは、サービスインスペクタを使用してトラフィックを検査する必要があるタイミングを決定します。バインダインスペクタの設定には、ネットワーク分析ポリシーの別のインスペクタがトラフィックを検査する必要がある場合に定義するポート、ホスト、CIDR、およびサービスが含まれます。

ステップ 3 必要に応じて、設定を編集します。

- JSON エディタで表示を制御するには、次を使用します。
  - JSON ファイルの全文検索を実行するには、[フィルタ（Filter）] 編集ボックスを使用します。
  - JSON ファイル内のすべてのフォルダを開くには、[すべてのフィールドを展開（Expand All Fields）] ボタン（⇕）をクリックします。
  - JSON ファイル内のすべてのフォルダを閉じるには、[すべてのフィールドを折りたたむ（Collapse All Fields）]（⇕）ボタンをクリックします。
  - 最新の変更を元に戻すには、[最後のアクションを元に戻す（Undo Last Action）]（↩）ボタンをクリックします。
  - 最後に元に戻した変更をやり直すには、[やり直し（Redo）]（↪）ボタンをクリックします。
  - [ツリー（Tree）] を選択すると、JSON ファイルのフォーマットビューが表示されます。このビューには、アクションメニュー、エラーフラグ、および編集をガイドするその他の機能が含まれています。
  - 未処理の JSON ファイルを表示するには、[コード（Code）] を選択します。

- [ツリー（Tree）] ビューで、[メニュー（Menu）] (▮) ボタンをクリックしてファイルの内容を操作します。次の操作を実行できます。
  - 属性を挿入します。[自動（Auto）] を使用して、エディタに適切なデータ型を決定させます。それ以外の場合は、配列、オブジェクト、または文字列を追加します。無効な属性を追加すると、インスペクタまたはバインダに、解決する必要がある問題があることがマークされます。
  - 属性を追加します。このアクションは挿入と同じですが、属性をセクションの最後に配置します。
  - 選択した属性を複製します。
  - 選択した属性を削除します。属性を編集するときに、ポップアップメッセージにDeleteコマンドが表示される場合もあります。
- 現在無効になっているインスペクタを有効にしたり、ブール属性の設定を変更したりするには、属性値の前にあるチェックボックスをクリックします。たとえば、インスペクタを有効にするには、enabled : false 属性を次のように変更します。

- 文字列または数値属性の値を変更するには、属性をクリックし、必要に応じて値を編集します。エントリがフィールドのルールに違反している場合は、エラーメッセージに不一致の説明が表示されます。たとえば、範囲外の値を入力した場合、有効な値の範囲が数値で示されます。
- オーバーライドをリセットするには、次の手順を実行します。
  - [インスペクタ/バインダオーバーのライドのリセット（Reset Inspector/Binder Overrides）] をクリックして、すべてのインスペクタまたはバインダに対するすべての変更を削除し、デフォルト値に戻します。コマンド名に示されているように、削除はインスペクタまたはバインダに限定されます。たとえば、すべてのバインダオーバーライドを削除しても、インスペクタオーバーライドは変更されません。
  - [インスペクタをデフォルトにリセット（Reset Inspector to Defaults）] をクリックして、選択したインスペクタのみに対するすべての変更を元に戻します。
- オーバーライドがあるインスペクタだけが表示されるようにビューをフィルタ処理するには、[オーバーライドのみ表示（Show Only Overrides）] をクリックします。[すべてのインスペクタを表示（Show All Inspectors）] をクリックして、フィルタを削除します。
- インスペクタがサポートされなくなった場合、インスペクタにメッセージとともにフラグが付けられます。メッセージ内の [インスペクタの削除（Delete Inspector）] リンクをクリックして、インスペクタを削除します。

ステップ 4 完了したら、[OK] をクリックします。

オーバーライドとスキーマのダウンロード

NAPスキーマをダウンロードするか、ポリシーに設定したオーバーライドをダウンロードできます。

以前の設定に戻す場合に備えて、基本 NAP を変更するたびにオーバーライドをダウンロードすることをお勧めします。さらに、1 つのデバイスで JSON エディタを使用して、すべてのデバイスで使用するオーバーライドを実装し、オーバーライドをダウンロードして、そのオーバーライドファイルを他のデバイスにアップロードできます。

オフラインでファイルを編集し、このデバイスまたは複数のデバイスにオーバーライドをアップロードする場合は、スキーマをダウンロードすると便利です。ファイル全体をアップロードするのではなく、変更が必要なセクションのみをコピーして貼り付け、変更内容のみがオーバーライドと見なされるようにします。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択し、[侵入ポリシーの設定（Intrusion Policy Settings）] ボタン（⚙）をクリックし、NAP設定に [カスタム（Custom）] を選択し、ポリシー名の横にある [編集（Edit）] リンクをクリックします。

ステップ 2 次のいずれかを実行します。

- 現在選択されている NAP のスキーマをダウンロードするには、歯車アイコン（⚙）をクリックし、**[ダウンロード（Download）]** > **[ポリシースキーマ（Policy Schema）]** を選択します。
- 現在の編集セッションの前に存在していた一連の保存済みオーバーライドをダウンロードするには、歯車アイコン（⚙）をクリックし、**[ダウンロード（Download）]** > **[最後に保存されたオーバーライド（Last Saved Overrides）]** を選択します。ファイルには、オーバーライドされた属性に加えて、属性に含まれるオブジェクトが含まれます。
- 現在の編集セッションで作成したオーバーライドをダウンロードするには、歯車アイコン（⚙）をクリックし、**[ダウンロード（Download）]** > **[現在未保存のオーバーライド（Current Unsaved Overrides）]** を選択します。ファイルには、オーバーライドされた属性に加えて、属性に含まれるオブジェクトが含まれます。

オーバーライドのアップロード

組み込みのJSONエディタを使用して属性を編集する代わりに、NAPポリシースキーマをダウンロードし、ファイルをオフラインで編集してから、ファイルをアップロードできます。アップロードしたファイルに設定されているオーバーライドは、選択した NAP に適用されます。

別のデバイスでオーバーライドを設定した後にダウンロードしたファイルもアップロードできます。

オーバーライドをアップロードすると、同じファイルを複数のデバイスにアップロードして、同じオーバーライドを簡単に適用できます。

始める前に

ネットワーク分析ポリシーでインスペクタ設定をオーバーライドするには、必要な変更のみをアップロードする必要があります。オーバーライドが本質的にスティッキになるため、設定全体をアップロードしないでください。その場合、LSP 更新の一部としてのデフォルト値や設定に対する後続の変更は適用されません。アップロードしたオーバーライドが、変更する属性だけに集中していることを確認します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択し、[侵入ポリシーの設定（Intrusion Policy Settings）] ボタン（⚙）をクリックし、NAP 設定に [カスタム（Custom）] を選択し、ポリシー名の横にある [編集（Edit）] リンクをクリックします。

ステップ 2 歯車アイコン（⚙）をクリックし、**[アップロード（Upload）]**>**[オーバーライド（Overrides）]** を選択します。

ステップ 3 （オプション）既存のオーバーライドのコピーを保存するには、[ダウンロード（Download）] リンクのいずれかをクリックします。

最後に保存されたオーバーライド（現在の編集セッションの前に作成されたオーバーライド）または現在未保存のオーバーライド（現在の編集セッション中に作成されたオーバーライド）をダウンロードできます。

ステップ 4 [アップロードのオーバーライドの確認（Confirm Upload Overrides）] ダイアログボックスで [はい（Yes）] をクリックして、続行することを確認します。

ステップ 5 [参照（Browse）] をクリックするか、ドラッグアンドドロップしてオーバーライドを含む JSON ファイルを選択し、[OK] をクリックします。

侵入ポリシーの管理（Snort 3）

Snort 3 を検査エンジンとして使用する場合は、独自の侵入ポリシーを作成し、それらを目的に応じてカスタマイズすることができます。システムには、同じ名前の Cisco Talos Intelligence Group（Talos）定義のポリシーに基づく事前定義されたポリシーが付属しています。これらのポリシーを編集することもできますが、基盤となる Talos ポリシーに基づいて独自のポリシーを作成し、ルールアクションを調整する必要がある場合にはそれを変更することをお勧めします。

これらの各事前定義ポリシーには同じ侵入ルール（署名とも呼ばれます）のリストが含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるポリシーでは有効化され、別のポリシーでは無効化されるルールがあります。

適用されている特定のルールであまりにも誤検出が多く、そのルールでブロックして欲しくないトラフィックがブロックされている場合、安全性の低い侵入ポリシーに切り替えることなく、ルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

逆に、特定の攻撃に対して保護する必要があるにもかかわらず、関連するルールが選択した侵入ポリシーで無効になっている場合は、より安全なポリシーに変更せずに、ルールを有効にすることができます。

侵入に関連するダッシュボードおよびイベント ビューアを使用して（両方、[モニタリング（Monitoring）]ページ）、侵入ルールがトラフィックに与えている影響を評価します。警告や削除に設定された侵入ルールに一致したトラフィックに対してのみ、侵入イベントや侵入データが表示されることに注意してください。無効になっているルールは評価されません。

（注） Snort 2 に切り替える場合、カスタムポリシーを作成できなくなり、侵入ポリシーの使用方法も少し異なります。このトピックの代わりに、侵入ポリシーの管理（Snort 2） （671 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

テーブルの上に表示されている Snort のバージョンが 3.x であることを確認します。

ステップ 2 次のいずれかを実行します。

- [検索/フィルタ（Search/Filter）] ボックスを使用してポリシーを検索します。名前でのみ検索できます。
- 歯車アイコン（⚙）をクリックし、syslog サーバーへのロギングを有効にします。侵入イベントの Syslog の設定 （649 ページ）を参照してください。
- 歯車アイコン（⚙）をクリックし、ネットワーク分析ポリシー（NAP）を設定します。ネットワーク分析ポリシーの設定（Snort 3） （649 ページ）を参照してください。
- [+] をクリックし、新しいポリシーを作成します。カスタム侵入ポリシーの設定（Snort 3） （657 ページ）を参照してください。
- 編集アイコン（✎）をクリックしてポリシーのプロパティとルールを表示し、それらを編集します。侵入ポリシーのプロパティの表示または編集（Snort 3） （658 ページ）を参照してください。
- 削除アイコン（🗑）をクリックしてポリシーを削除します。

カスタム侵入ポリシーの設定（Snort 3）

事前定義ポリシーがニーズに合わない場合は、新しい侵入ポリシーを作成してルールの動作をカスタマイズできます。一般に、事前定義ポリシーを変更するのではなく、事前定義ポリシーに基づいてカスタムポリシーを作成することをお勧めします。これにより、カスタマイズによって必要な結果が得られない場合に、Cisco Talos 定義のポリシーの一つを簡単に実装できます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいポリシーを作成するには、[+] をクリックします。
- 既存のポリシーを編集するには、そのポリシーの編集アイコン（  ）をクリックします。ポリシーの詳細が表示されたら、ページの上部にあるポリシープロパティのセクションの [編集（Edit）] リンクをクリックします。

ステップ 3 ポリシーの [名前（Name）] を入力し、必要に応じて、説明を入力します。

ステップ 4 ポリシーの [検査モード（Inspection Mode）] を設定します。

- [防止（Prevention）]：侵入ルールのアクションが常に適用されます。切断ルールに一致する接続はブロックされます。
- [検出（Detection）]：侵入ルールはアラートのみを生成します。切断ルールに一致する接続はアラートメッセージを生成しますが、接続はブロックされません。

ステップ 5 ポリシーの [基本テンプレート（Base Template）] を選択します。

基本テンプレートはCisco Talosによって提供されます。ポリシーの詳細を表示するには、それぞれの情報アイコンをクリックします。新しいルールパッケージがインストールされると、ポリシー名が変更される場合があり、新しいポリシーも表示されることに注意してください。

- [最大検出（Cisco Talos）（Maximum Detection (Cisco Talos)）]：このポリシーはセキュリティを最重要としています。ネットワーク接続とスループットは保証されず、誤検出が発生する可能性があります。このポリシーは、高度なセキュリティを要するエリアでのみ使用する必要があります。また、アラートを調査し、その有効性を判別できるように、セキュリティモニターを準備する必要があります。
- [接続性よりもセキュリティを優先（Cisco Talos）（Security Over Connectivity (Cisco Talos)）]：このポリシーはセキュリティに重点を置いており、ネットワーク接続とスループットが犠牲になる場合があります。トラフィックはより綿密に検査され、より多くのルールが評価されるため、理に適った範囲内での、誤検出と遅延の増加の両方が予期されます。

- [バランスのとれたセキュリティと接続性（Cisco Talos）（Balanced Security and Connectivity (Cisco Talos)）]：（デフォルト）このポリシーは、ネットワーク接続およびスループットとセキュリティニーズの間での微妙なバランスの確立を試みます。このポリシーは、[接続性よりもセキュリティを優先（Security Over Connectivity）]ほど厳格ではありませんが、通常のトラフィックの中断を減少させながら、ユーザーのセキュリティを保持しようとします。
- [セキュリティよりも接続性を優先（Cisco Talos）（Connectivity Over Security (Cisco Talos)）]：このポリシーは、ネットワーク接続とスループットに重点を置いており、セキュリティが犠牲になる場合があります。トラフィックは綿密に検査されず、評価されるルール数は少なくなります。
- [アクティブなルールなし（Cisco Talos）（No Rules Active (Cisco Talos)）]：このポリシーは、一般的なプリプロセッサ設定を指定する基本ポリシーですが、ルールや組み込みアラートは有効になっていません。適用するポリシーのみを有効にする場合は、このポリシーをベースとして使用します。

ステップ 6 [OK] をクリック

侵入ポリシーリストに戻ります。これで、新しいポリシーを表示し、必要に応じてルールアクションを調整することができます。

侵入ポリシーのプロパティの表示または編集（Snort 3）

[侵入ポリシー（Intrusion Policy）] ページには、事前定義されたポリシーとユーザー定義のポリシーの両方を含むポリシーのリストとその説明が表示されます。ポリシーを編集するには、まずポリシーのプロパティを表示する必要があります。

手順

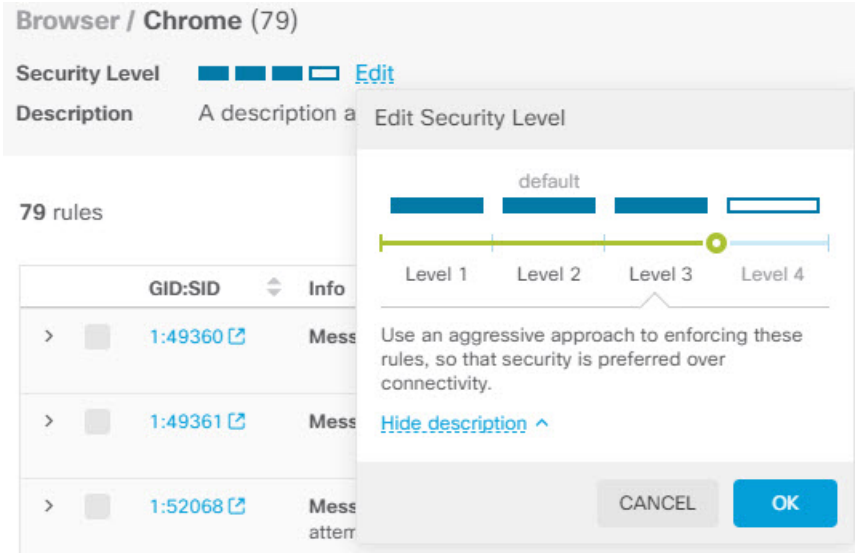
ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（  ）をクリックします。

ポリシーには、次のセクションが含まれています。

- [ポリシー名（Policy Name）] ドロップダウンリスト。
  - ドロップダウンリストから選択することで別のポリシーに簡単に切り替えたり、戻るボタン（  ）をクリックしてポリシーのリストに戻ることができます。
  - このポリシーを削除するには、ポリシー名の横にある削除アイコン（  ）をクリックします。

- [一般プロパティ（General Properties）]。このセクションには、侵入モード、基本ポリシー、および説明が示されます。これらのプロパティまたはポリシー名を変更するには、[編集（Edit）] をクリックします。
- [ルールグループ（Rule Group）] の目次。このリストには、ポリシーにアクティブなルールがあるすべてのルールグループが表示されます。グループには階層があり、親グループには、より大きな親グループ内のルールのサブセットを編成する子グループが含まれます。各グループはルールの論理的な集合であり、特定のルールが複数のグループに含まれる場合があります。
  - 現在ポリシーにアクティブなルールがないグループを追加するには、[+]**[+] > [既存のルールグループの追加（Add Existing Rule Group）]** をクリックして、そのグループを選択します。侵入ポリシーのルールグループの追加または削除（Snort 3）（661 ページ）を参照してください。
  - グループのセキュリティレベルを変更するには、リストから子グループを選択します。ルールリストが変更され、セキュリティレベルが上部に表示され、グループ内のルールが下に一覧表示されます。セキュリティレベルの横にある [編集（Edit）] リンクをクリックし、新しいレベルを選択します。各セキュリティレベルに関する情報を取得するには、編集時に [説明の表示（View Description）] をクリックします。レベルを変更すると、アクティブなルールが（および特定のルールのアクションも）変更される可能性があることに注意してください。よりセキュアなレベルでは、アクティブなルールが多くなり、ドロップアクションを持つルールが多くなる傾向があります。[OK] をクリックして変更を確定します（セキュリティレベルはカスタムルールグループには適用されません）。



  - グループ内のすべてのルールを削除するには、リストから子グループを選択します。次に、グループ名の右端にある [除外（Exclude）] リンクをクリックし、グループを除外することを確認します。グループを除外すると、グループ内のすべてのルールが無効になるだけです。グループは削除されません。

ただし、グループに、有効になっている他のグループと共有しているルールが含まれている場合、共有ルールでは、現在もアクティブであるグループによって適用されるアクションがすべて保持されます。すべての場合において、グループメンバーシップに関係なく、個々のルールに対して最も積極的な設定が保持されます。

- カスタムルールの新しいカスタムルールグループを追加するには、**[+]>[カスタムルールのアップロード（Upload Custom Rules）]**をクリックします。詳細については、カスタム侵入ルールのアップロード （666 ページ）を参照してください。
- カスタムルールグループの名前または説明を変更するには、[編集（Edit）] をクリックします。
- カスタムルールグループを削除するには、[削除（Delete）] をクリックします。詳細については、「カスタム侵入ルールとルールグループの管理 （665 ページ）」を参照してください。
- カスタムルールグループに新しいカスタムルールを追加するには、ルールテーブルの上にある [+] をクリックします。個別のカスタム侵入ルールの設定 （669 ページ）を参照してください。
- カスタムルールのグループメンバーシップを編集、複製、削除、または管理するには、ルールの右側にカーソルを合わせ、適切なボタンまたはコマンドをクリックします。詳細については、「個別のカスタム侵入ルールの設定 （669 ページ）」を参照してください。

- [ルールのリスト（List of rules）]。検索フィールドを使用すると、全文検索でルールを検索できます。フィルタリング項目を選択して、GIDまたはSIDの任意の組み合わせで検索したり、（追加した）ユーザー定義のルールのみ表示したり、アクションがオーバーライドされたルールのみ表示したり、単にアクション（無効、アラート、ドロップ）に基づいてルールを表示したりもできます。ルールは遅延ロードされるため、フィルタ処理されていないリスト全体のスクロールにはかなりの時間がかかります。リストをフィルタ処理する場合は、更新ボタンをクリックして、フィルタ処理されたビューをリロードしてください。
  - ルールのアクションを変更するには、ルールの [アクション（Action）] セルをクリックし、新しいアクションを選択します。アラートのみにする場合は [アラート（Alert）]、一致するトラフィックをブロックする場合は [ブロック（Block）]、ルールを無効にする場合は[無効（Disable）] を選択してください。各ルールのデフォルトアクションが示されます。
  - 一度に複数のルールのアクションを変更するには、変更するルールの左の列にあるチェックボックスをクリックし、ルールテーブルの上にある [アクション（Action）] ドロップダウンリストから新しいアクションを選択します。GID:SIDヘッダーのチェックボックスをクリックしてリスト内のすべてのルールを選択します。最大5000のルールを一度に変更できます。
  - カスタムルールグループ内のルールを更新するには、[ルールファイルのアップロード（Upload Rule File）] をクリックします。詳細については、「カスタム侵入ルールのアップロード （666 ページ）」を参照してください。

- ルールに関する詳細情報を取得するには、[GID：SID] セルのリンクをクリックします。リンクをクリックすると Snort.org に移動します。
- 一覧表示されるルールを変更するには、ルールグループの目次から子グループ（親グループではなく）をクリックします。ルールグループリストの上部にある [すべてのルール（ALL RULES）] をクリックすると、すべてのルールのリストに戻ることができます。
- ソート順序を変更するには、カラムのテーブルヘッダーをクリックします。ルールのデフォルトのソートは、上書きされたルール、ドロップルール、アラートルールの順です。
- 侵入ルール（LSP）の更新で行われた変更を確認するには、[フィルタ（Filter）] フィールドで [LSPの更新（LSP Update）] を選択し、変更を表示する更新を選択し、すべての変更を表示するか、またはルールに対する追加や変更のみ表示するかを指定します。

侵入ポリシーのルールグループの追加または削除（Snort 3）

侵入ルールはローカルグループで編成されます。グループには階層があり、親グループには関連する子グループが含まれます。ルール自体は子グループにのみ表示されます。親グループは単に組織的な構成要素です。特定のルールが複数のグループに表示される場合があります。

作成したカスタムルールグループは、[ユーザー定義グループ（User Defined Groups）] フォルダにあります。カスタムルールグループには階層がありません。

侵入ポリシーのルールを追加または削除する最も簡単な方法は、グループを追加または削除することです。グループ内のルールは論理的に関連しているため、高い確率で、特定のグループ内のすべてではないにしてもほとんどのルールを使用することになります。

次の手順では、グループを追加し、グループのセキュリティレベルを変更する方法について説明します。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 変更するポリシーの編集アイコン（）をクリックします。

ステップ 3 （グループの追加）ルールグループのリストにグループが表示されない場合は、**[+] > [既存のルールグループの追加（Add Existing Rule Group）]** をクリックして、次の手順を実行します。

a) 子グループを検索します。

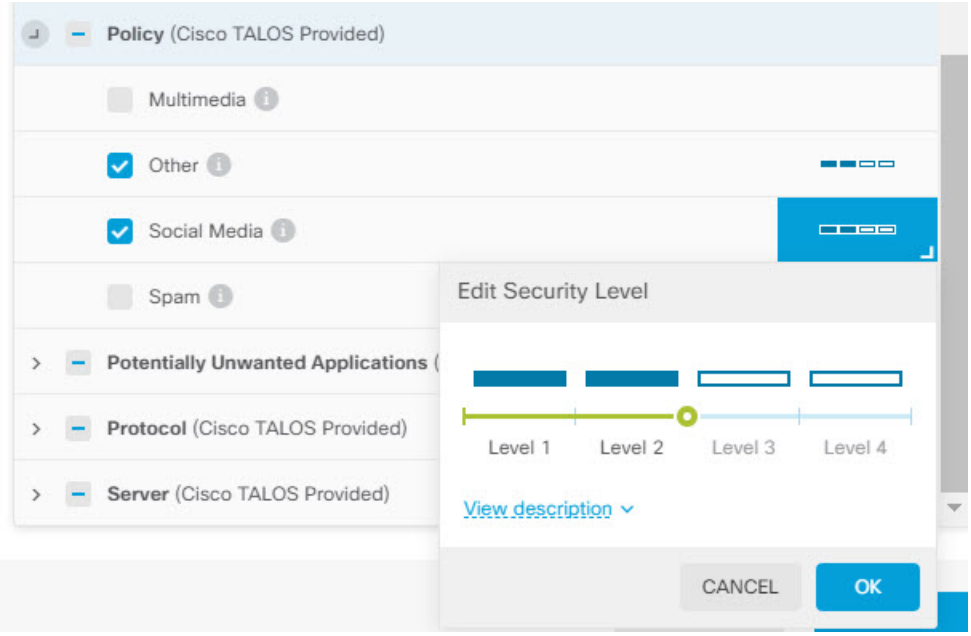
- 親グループ名の横のチェックマークは、その親グループに含まれるすべての子グループがすでに選択されていることを示します。

- 親グループ名の横のマイナス記号は、1 つ以上の子グループがこのポリシーに対して有効なルールを持っていないことを示します。これらは追加できるグループです。
- 子グループ名の横のチェックマークは、そのグループがすでに選択されていることを示します。

b) 追加するグループを選択します（チェックボックスをオンにする）。

c) （オプション、カスタムルールグループには適用されません）各グループには、カスタムポリシーに使用される基本ポリシーに応じたデフォルトのセキュリティレベルがあります。変更する場合は、セキュリティレベルのアイコンをクリックし、新しいレベルを選択して、[OK] をクリックします。

レベル 1 は最も安全性の低いセキュリティ態勢であり、セキュリティよりも接続性が重視されます。一方、レベル 4 は最も積極的なセキュリティ態勢であり、最大のセキュリティを提供します。[説明の表示（View Description）] をクリックすると、選択した各レベルの説明が表示されます。



d) すべての変更が完了するまで、グループの選択（または選択解除）を続けます。

e) [OK] をクリック

ステップ 4 （グループの削除）グループに含まれるすべてのルールを無効にするには、次のいずれかの方法を使用できます。

- ルールのリストの上で、グループを選択し、グループ名の右端にある [除外（Exclude）] リンクをクリックします。
- グループを追加する手法を使用しますが、代わりに、不要なグループの選択を解除し（チェックボックスをオフする）、[OK] をクリックします。

- カスタムルールグループを削除して、システムおよびそのルールを使用するすべての侵入ポリシーから完全に削除できます。グループを選択してから、[削除（Delete）] をクリックします。

侵入ルールのアクションの変更（Snort 3）

各侵入ポリシーには同じルールがあります。違いは、各ルールで取られるアクションがポリシーごとに異なる場合があることです。

ルールアクションを変更して、誤検出が多すぎるルールを無効にすることができます。またはルールが、一致するトラフィックのアラートを発するか、そのトラフィックを切断するかどうかを変更できます。また、無効になっているルールを有効にして、一致するトラフィックをアラートまたは切断することもできます。

ルールアクションを変更する最も簡単な方法は、ルールグループのセキュリティレベルを変更することです。グループのセキュリティレベルを変更すると、グループ内のルールのアクションが変更されます。選択するセキュリティ態勢により、これが一部のルールを有効（または無効）にすることを意味する場合もあれば、アクションがアラートとドロップの間で変化する場合もあります。ただし、必要に応じて、個々のルールアクションを変更できます。

（注） 特定のルールのデフォルトアクションは、グループとシビラティ（重大度）の全体的な選択に基づいて決まります。グループのシビラティ（重大度）を変更したり、グループを除外したりすると、ルールのデフォルトアクションが変化する場合があります。

始める前に

カスタムルールグループにはセキュリティレベルがありません。セキュリティレベルの手法を使用して、カスタムルールのルールアクションを変更することはできません。

手順

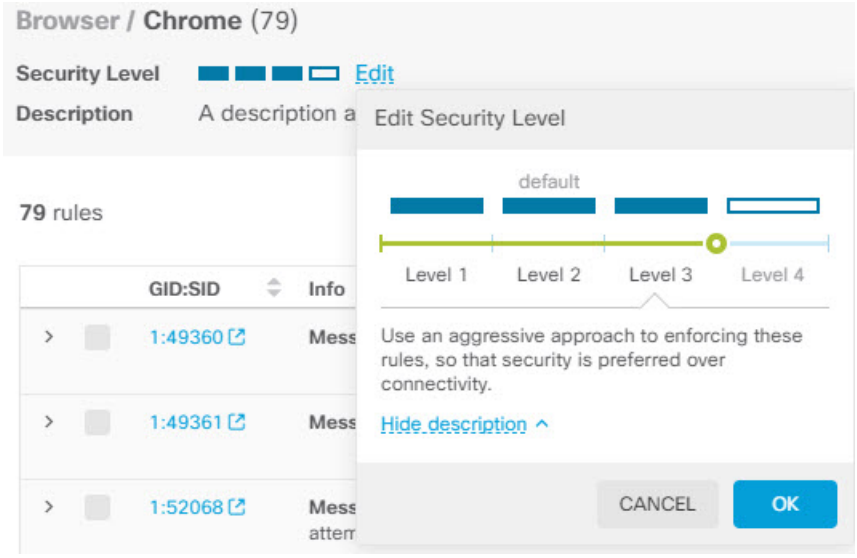
ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 ルールアクションを変更するポリシーの表示アイコン（）をクリックします。

ステップ 3 （推奨される方法）グループのセキュリティレベルを変更します。

a) ルールグループリストの子ルールグループをクリックします。

b) ルールのリストの上で、グループのセキュリティレベルの横にある [編集（Edit）] をクリックします。



（注） グループ内のすべてのルールを無効にする場合は、[編集（Edit）] をクリックしないでください。代わりに、[除外（Exclude）] をクリックし、グループを除外することを確認します。グループは削除されず、そのルールが単に無効になります。残りの手順はスキップしてください。

c) グループの新しいレベルを選択します。[説明の表示（View Description）] をクリックして、選択した各レベルの説明を表示します。

レベル 1 は最も安全性の低いセキュリティ態勢であり、セキュリティよりも接続性が重視されます。一方、レベル 4 は最も積極的なセキュリティ態勢であり、最大のセキュリティを提供します。

d) [OK] をクリック

ステップ 4 （手動の方法）1 つ以上のルールのアクションを変更します。

a) 変更するアクションのルールを検索します。

ルール情報内の文字列を検索するには、[検索/フィルター（Search/Filter）] ボックスを使用します。フィルタ処理項目を選択して、GID または SID の任意の組み合わせで検索したり、単にそれらのアクション（無効、アラート、ドロップ）に基づいてルールを表示したりすることもできます。ルールは遅延ロードされるため、フィルタ処理されていないリスト全体のスクロールにはかなりの時間がかかります。リストをフィルタ処理する場合は、更新ボタンをクリックして、フィルタ処理されたビューをリロードしてください。

理想的には、連携して問題に取り組んでいる場合にイベントやシスコ テクニカル サポートから Snort 識別子（SID）とジェネレータ識別子（GID）を取得できます。これにより、ルールを正確に検索できます。

b) アクションを変更するには、次のいずれかを実行します。

- ルールを 1 つずつ変更：ルールの [アクション（Action）] 列をクリックし、必要なアクションを選択します。

- [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。

- 一度に複数のルールを変更：変更するルールのチェックボックスをクリックし、表の上にある [一括（Bulk）] ドロップダウンをクリックして、目的のアクションを選択します。GID:SID ヘッダーのチェックボックスをクリックしてリスト内のすべてのルールを選択します。最大 5000 のルールを一度に変更できます。

カスタム侵入ルールとルールグループの管理

システムには、Cisco Talos Intelligence Group（Talos）によって定義された何千もの侵入ルールが付属しています。追加の攻撃を把握している場合は、カスタム侵入ルールを作成してアップロードし、それらの攻撃をスクリーニングして、アラートを発出したり、攻撃をドロップしたりすることができます。ルールを 1 つずつ作成、編集、削除することもできます。

アップロードするルールの場合、テキストエディタを使用してルールをオフラインで作成します。アップロードする各テキストファイルにカスタムルールのグループを含めることをお勧めします。これにより、ルールへの変更を簡単にアップロードし、新しいルールをカスタムルールグループにマージしたり、ルールを新しい編集済みコピーに置き換えたりできます。

こうしたルールの作成方法の説明は、このドキュメントの対象範囲に含まれていません。Snort 2 ルールを Snort 3 形式に変換する方法など、Snort 用の侵入ルールの作成方法に関する詳細については、https://snort.org/documents のガイドを参照してください。たとえば、https://snort.org/documents/rules-writers-guide-to-snort-3-rules で『*Snort 3*ルールを作成するルール作成者のための手引き』を参照してください。

始める前に

カスタムルールグループは、カスタム侵入ルールのアップロード（666ページ）で説明されているようにカスタムルールをアップロードするプロセスで作成するか、個々のルールを作成するか、またはルールメンバーシップを管理するときに作成します。グループを作成した後は、グループとその内容を管理できます。

カスタムグループは、グループを作成したときに編集していたポリシーだけでなく、すべての侵入ポリシーで使用できることに注意してください。そのため、グループに加えた変更はすべてのポリシーに対しても加えられます。たとえば、カスタムルールグループを削除すると、そのグループはすべてのポリシーから削除され、どのポリシーでも使用できなくなります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（  ）をクリックします。

いずれかの組み込みポリシーではなくカスタム侵入ポリシーに、カスタムルールを追加することをお勧めします。

ステップ 3 次のいずれかを実行します。

- グループを作成するには、**[+]** > **[カスタムルールのアップロード（Upload Custom Rules）]** をクリックします。カスタム侵入ルールのアップロード（666 ページ）を参照してください。
- グループの名前または説明を編集するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。[編集（Edit）] をクリックして変更を加えることができます。
- ポリシーからグループとそのルールを除外するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。選択後、[除外（Exclude）] をクリックしてグループを削除できます。
- システムからグループを削除するとともに、そのグループを使用するすべてのポリシーを削除するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。さらに [Delete] をクリックします。あるルールが削除されたグループのみに存在する場合、そのルールはシステムからも削除されることに注意してください。他方、削除していない他のカスタムルールグループにも同じルールが存在する場合、そのルールはそれらのグループに残されます。
- グループ内のルールを一括で置換または更新するには、[ユーザー定義グループ（User Defined Groups）] フォルダのグループ目次でグループを選択します。次に、グループのルールテーブルの上にある [アクション（Action）] ドロップダウンリスト横の [ルールファイルのアップロード（Upload Rule File）] をクリックします。このプロセスは、カスタム侵入ルールのアップロード（666 ページ）で説明されたものと同じです。
- 個々のルール、およびルールグループへの割り当てを作成および管理するには、個別のカスタム侵入ルールの設定（669 ページ）を参照してください。

カスタム侵入ルールのアップロード

現在他のルールでカバーされていない攻撃を把握している場合は、カスタム侵入ルールを作成してアップロードし、それらの攻撃をスクリーニングして、アラートを発出したり、攻撃をドロップしたりすることができます。インポートされたルールのアクションはアラートまたはドロップのいずれかである必要があります。ルールのデフォルトアクションはインポートされたファイルのアクションによって定義されます。インポートしたら、ルールアクションを変更し、必要に応じてルールを無効にすることができます。

これらのルールはオフラインで作成する必要があります。Device Manager では、ルールファイルをアップロードするだけで、ルールを直接設定するわけではありません。ルールファイルはテキストファイルである必要があります。改行を使用してルールを読みやすい形式にしたり、1行にルールを入力したりできます。空の行は許可されます。ルールの形式については、snort.org を参照してください。

たとえば、3 つのルールのアップロードファイルは次のようになります。

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
 connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
 PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
   rev:1;
)
```

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（）をクリックします。

いずれかの組み込みポリシーではなくカスタム侵入ポリシーに、カスタムルールを追加することをお勧めします。

ステップ 3 次のいずれかを実行します。

- グループのリストの上にある **[+]** > **[カスタムルールのアップロード]** をクリックします。
- 作成済みのカスタムルールグループにルールをアップロードする場合は、カスタムルールグループを選択して、グループのルールテーブルの上にある [アクション（Action）] ドロップダウンリストの横にある [ルールファイルのアップロード（Upload Rule File）] をクリックします。

ステップ 4 [参照（Browse）] をクリックしてカスタムルールファイルを選択するか、ファイルを [ファイルのアップロード（Upload File）] ダイアログボックスにドラッグアンドドロップします。

アップロードが完了するまで待ちます。

ステップ 5 競合の処理方法を選択します。

競合は、追加するルールがシステムにすでに存在するルールと同じ場合に発生します。これは、以前にアップロードしたのと同じルールまたは編集したバージョンのルールをアップロードする場合にのみ発生します。

次のオプションのいずれか 1 つを選択します。

（注） [マージ（Merge）] と [置換（Replace）] は基本的に同じものです。既存のルールに変更を加えるには、アップロードしたルールのリビジョン番号が、アップロード済みのルールのリビジョン番号よりも大きい必要があります。唯一の違いは、[置換（Replace）] オプションを使用すると、アップロードファイルに対象のカスタムルールグループ内のルールがない場合、それらのルールがルールグループから削除されることです。[マージ（Merge）] オプションでは、これらの "欠落している" ルールがそのまま残ります。

- [マージ（Merge）]：アップロードされたファイルのルールのリビジョン番号が大きい場合、アップロードされたファイル内の変更されたルールのうち、選択したグループにも存在するものは、それらの変更がマージされます。変更されていないルール、またはアップロードに対応するルールがないグループ内のルールは変更されません。アップロード内の新しいルールが追加されます。これがデフォルトのオプションです。
- [置換（Replace）]：アップロードされたファイルのルールは、アップロードされたルールのリビジョン番号が大きい場合、選択したグループのルールを置き換えます。アップロードされたファイルに存在しない既存のルールは、グループから削除されます。アップロードされたバージョンのリビジョン番号が同じかそれ以下の既存のルールは変更されません。アップロード内の新しいルールが追加されます。

ステップ 6 [+] をクリックし、アップロードしたルールのカスタムルールグループを選択します。

使用するカスタムルールグループが存在しない場合は、[新しいグループの作成（Create New Group）] をクリックしてすぐに作成します。新しいグループには名前と、必要に応じて説明が必要です。その後、新しいグループを選択できます。

ルールを置き換える場合は、1つのグループのみを選択できます。ルールをマージする場合は、複数のグループを選択できます。

ステップ 7 [OK] をクリック

ファイルがアップロードされ、新しいグループに配置されます。アップロードされたルールの数と、更新、削除、または無視されたルールの数の概要が表示されます。

ファイルにエラーがある場合、アップロードは失敗します。[ダウンロードエラーファイル（Download Error File）] リンクをクリックすると、エラーの詳細情報を取得できます。

グループは、この侵入ポリシーで自動的にアクティブ化されます。グループと新しいルールは他のポリシーに追加できますが、グループとルールが他のポリシーで自動的に有効になることはありません。他のポリシーへのグループの追加については、侵入ポリシーのルールグループの追加または削除（Snort 3） （661 ページ）を参照してください。

個別のカスタム侵入ルールの設定

カスタム侵入ルールは、ファイルアップロードによって一括で行うのではなく、一度に1つずつ設定できます。この方法は、あるルールをすばやく調整する必要がある場合や、一度に少数のルールを作成または変更する必要がある場合に適しています。

侵入ルールを設定する場合は、次の点に注意してください。

- すべてのカスタムルールの GID は 1 である必要があります。
- ルールの SID は、システム内のすべてのルールで一意である必要があります。また、100万（1000000）以上である必要があります。
- ルールを編集する場合は、ルールのバージョンを変更する必要があります。通常、バージョン番号は 1 ずつ増加します。
- Cisco Talos Intelligence Group（Talos）ルールを複製して独自のバージョンのルールを作成できますが、重複する SID を変更して一意にする必要があります。

ルールが適切に形成されていることを確認するためにいくつかの有効性チェックが実行され、問題に関するエラーメッセージが表示されます。ただし、システムはルールが適切かどうかを判断できません。

Snort 2 ルールを Snort 3 形式に変換する方法など、Snort 用の侵入ルールの作成方法に関する詳細については、https://snort.org/documents のガイドを参照してください。たとえば、https://snort.org/documents/rules-writers-guide-to-snort-3-rules で『*Snort 3*ルールを作成するルール作成者のための手引き』を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの編集アイコン（  ）をクリックします。

いずれかの組み込みポリシーではなくカスタム侵入ポリシーに、カスタムルールを追加することをお勧めします。

ステップ 3 次のいずれかを実行します。

- 侵入ルールを追加するには、ルールテーブルの上にある [新しい侵入ルールの追加（Add New Intrusion Rule）] ボタン（+）をクリックします。ルールを追加する場合、新しいルールを含める 1 つ以上のカスタムルールグループを選択する必要があります。必要に応じて、ルールを追加しながら新しいグループを作成できます。
- 既存のルールを複製および編集してルールを追加するには、ルールの右端にマウスを合わせ、[複製（Duplicate）] （）ボタンをクリックします。ボタンは、マウスオーバーでのみ表示されます。カスタムルールの場合、[複製（Duplicate）] コマンドはその他のオプション（...）ボタンの下にあります。
- カスタムルールを編集するには、カスタムルールグループでルールを検索し、ルールの編集（）ボタンをクリックします。編集内容は、ルールが存在するすべてのグループに適用されます。変更を行う場合は、ルールのバージョン番号を少なくとも 1 つ増やしてください。
- カスタムルールを削除するには、ルールの削除（）ボタンをクリックします。ルールが含まれるすべてのルールグループから、そのルールが削除されます。あるグループから 1 つのルールだけを削除する場合は、ルールを削除する代わりに [グループ割り当ての管理（Manage Group Assignments）] オプションを使用します。
- ルールを含むグループを変更するには、その他のオプション（...）ボタンをクリックし、[グループ割り当ての管理（Manage Group Assignments）] を選択します。その後、グループを追加または削除できます。変更はグループメンバーシップに影響するだけで、ルールの変更や削除は行いません。

ステップ 4 新しいルールとグループの場合は、ルールをポリシーに追加します。

新しいルールの作成時または既存のルールの編集時に新しいグループを作成すると、そのグループはポリシーに自動的に追加されず、ルールも自動的に有効になりません。編集するポリシーにグループを追加するように求められます。ルールの追加または編集中にグループを追加しない場合は、次のプロセスを使用して後でグループを追加できます。

a) グループの目次の上にある **[+]** > **[既存のルールグループを追加（Add Existing Rule Group）]** をクリックします。
b) [ユーザー定義グループ（User Defined Groups）] フォルダでグループを見つけて選択し、[OK] をクリックします。
c) 目次でグループを選択し、新しいルールがグループ内にあり、目的のアクションがあることを確認します。

侵入ポリシーの管理（Snort 2）

あらかじめ定義された侵入ポリシーのいずれかを適用できます。これらの各ポリシーには同じ侵入ルール（署名とも呼ばれます）の一覧が含まれていますが、各ルールに対して実行する操作は異なります。たとえば、あるルールは1つのポリシーでアクティブになる可能性がありますが、別のポリシーでは無効化されます。

適用されている特定のルールであまりにも誤検出が多く、そのルールでブロックして欲しくないトラフィックがブロックされている場合、安全性の低い侵入ポリシーに切り替えることなく、ルールを無効にできます。または、トラフィックをドロップせずに、一致すると警告するように変更することもできます。

逆に、特定の攻撃に対して保護する必要があるにもかかわらず、関連するルールが選択した侵入ポリシーで無効になっている場合は、より安全なポリシーに変更せずに、ルールを有効にすることができます。

侵入に関連するダッシュボードおよびイベント ビューアを使用して（両方、[モニタリング（Monitoring）]ページ）、侵入ルールがトラフィックに与えている影響を評価します。警告や削除に設定された侵入ルールに一致したトラフィックに対してのみ、侵入イベントや侵入データが表示されることに注意してください。無効になっているルールは評価されません。

ここでは、侵入ポリシーおよびルールの調整について詳しく説明します。

侵入ポリシーのインスペクションモードの設定（Snort 2）

デフォルトでは、侵入防御システム（IPS）を実装するため、すべての侵入ポリシーが防御モードで動作します。防御インスペクションモードでは、トラフィックを切断するアクションの侵入ルールと接続が一致する場合、接続は能動的にブロックされます。

一方、ネットワーク上で侵入ポリシーの影響をテストするには、侵入検知システム（IDS）を実装する「検出」にモードを変更します。このインスペクションモードでは、切断ルールはアラートルールと同様に扱われます。この場合、一致する接続が通知されますが、アクションの結果は「ブロック相当」となり、実際に接続がブロックされることはありません。

侵入ポリシーごとにインスペクションモードを変更するため、防御と検出を混在させることができます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** の順に選択します。

ステップ 2 インスペクションモードを変更する侵入ポリシーのタブをクリックします。

[インスペクションモード（Inspection Mode）] は、ルールテーブルの上に表示されます。

ステップ 3 インスペクションモードの横にある [編集（Edit）] リンクをクリックし、ポリシーのモードを変更して、[OK] をクリックします。

次のオプションがあります。

- [防止（Prevention）]：侵入ルールのアクションが常に適用されます。切断ルールに一致する接続はブロックされます。
- [検出（Detection）]：侵入ルールはアラートのみを生成します。切断ルールに一致する接続はアラートメッセージを生成しますが、接続はブロックされません。

侵入ルールのアクションの変更（Snort 2）

事前定義された各侵入ポリシーには同じルールがあります。違いは、各ルールで取られるアクションがポリシーごとに異なる場合があることです。

ルールアクションを変更して、誤検出が多すぎるルールを無効にすることができます。またはルールが、一致するトラフィックのアラートを発するか、そのトラフィックを切断するかどうかを変更できます。また、無効になっているルールを有効にして、一致するトラフィックをアラートまたは切断することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** の順に選択します。

ステップ 2 変更するルール アクションの侵入ポリシーのタブをクリックします。

事前定義されているポリシーは次のとおりです。

- セキュリティよりも接続性を優先
- バランスのとれたセキュリティと接続性
- 接続性よりもセキュリティを優先
- 最大検出

ステップ 3 変更するアクションのルールを検索します。

ルールは上書き済みが一番上に並べ替えられ、また上書きされたルールのグループ内でアクション順に並べ替えられます。それ以外の場合、ルールは、GID、次に SID で並べ替えられます。

変更するルールを検索するには検索ボックスを使用します。理想的には、連携して問題に取り組んでいる場合にイベントやシスコ テクニカル サポートから Snort 識別子（SID）とジェネレータ識別子（GID）を取得できます。

各ルールの要素の詳細については、侵入ルール属性 （642 ページ）を参照してください。

このリストを検索するには、次の手順を実行します。

a) [検索（Search）] ボックス内でクリックして、[検索属性（search attributes）] ダイアログボックスを開きます。

b) ジェネレータ ID（[GID]）、Snort ID（[SID]）、またはルール[アクション（Action）] の組み合わせを入力し、[検索（Search）] をクリックします。

たとえば [アクション=ドロップ（Action = Drop）] を選択して、一致する接続をドロップするポリシーのすべてのルールを表示できます。検索ボックスの横にあるテキストは、条件に一致するルールの数が表示されます（たとえば「9416 中 8937 ルールが見つかりました」）。

検索条件をクリアするには、検索ボックスの条件の [x] をクリックします。

ステップ 4 ルールの [アクション（Action）] の列をクリックして、必要なアクションを選択します。

- [アラート（Alert）]：このルールがトラフィックと一致するとイベントを作成しますが、接続はドロップしません。
- [ドロップ（Drop）]：このルールがトラフィックと一致するとイベントを作成し、接続をドロップします。
- [無効（Disabled）]：このルールではトラフィックは一致しません。イベントは生成されません。

ルールのデフォルトのアクションは、アクションに加えて「（デフォルト）」と表示されます。デフォルトを変更すると、状態の列にそのルールに対して「上書き済み」と表示されます。

侵入ポリシーのモニタリング

侵入ポリシー統計情報は、[モニタリング（Monitoring）] ページの [攻撃者（Attackers）] および[ターゲット（Targets）] ダッシュボードで確認できます。これらのダッシュボードで情報を表示するには、少なくとも 1 つのアクセス コントロール ルールに侵入ポリシーを適用する必要があります。「トラフィックのモニタリングおよびシステム ダッシュボード（123 ページ）」を参照してください。

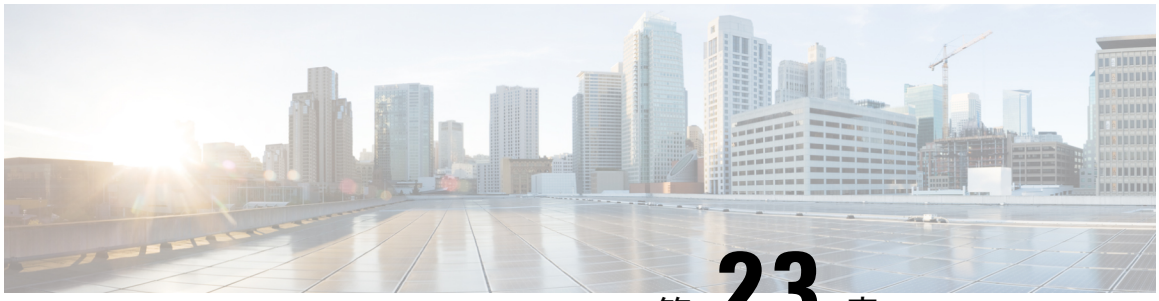
侵入イベントを表示するには、**[モニタリング（Monitoring）]** > **[イベント（Events）]** を選択して、[侵入（Intrusion）] タブをクリックします。イベントの上にマウスを置き、[詳細の表示（View Details）] へのリンクをクリックして、詳細情報を表示できます。詳細ページから、[IPS ルールの表示（View IPS Rule）] をクリックして、関連する侵入ポリシーのルールへ移動し、そこでルールアクションを変更できます。ルールによりブロックされる適切な接続が多すぎる場合に、アクションをドロップから警告に変更することにより、誤検出の影響を軽減できます。逆に、ルールに対する攻撃トラフィックが多い場合は、アラート ルールをドロップ ルールに変更できます。

侵入ポリシーの syslog サーバーを設定した場合、侵入イベントのメッセージ ID は 430001 です。

侵入ポリシーの例

使用例の章には、次の侵入ポリシーの実装例が含まれています。

- 脅威をブロックする方法 （64 ページ）
- ネットワーク上のトラフィックをパッシブにモニタする方法 （90 ページ）



第 23 章

Network Address Translation（NAT）

ここでは、ネットワーク アドレス変換（NAT）とその設定方法について説明します。

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるためです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。

- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換できます。

（注） NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常通りに適用されます。

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続されている任意のネットワークに変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピング アドレス/ホスト/ネットワーク/インターフェイス：マッピング アドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換中、デバイス インターフェイスに設定された IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。

- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

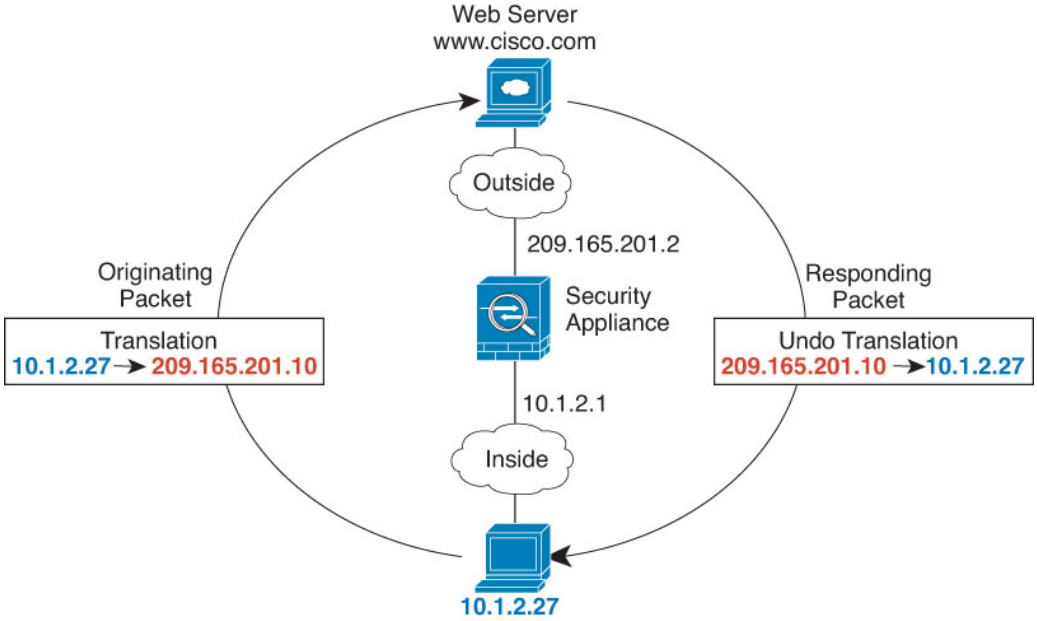
NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。ダイナミック NAT （692 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。ダイナミック PAT （698 ページ）を参照してください。
- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。スタティック NAT （704 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。アイデンティティ NAT （714 ページ） を参照してください。

ルーテッド モードの NAT

次の図は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。

図 *35 : NAT* の例：ルーテッド モード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピング アドレス 209.165.201.10 に変換されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、Threat Defense デバイス がそのパケットを受信します。これは、Threat Defense デバイス がプロキシ ARP を実行してパケットを要求するためです。
3. Threat Defense デバイス はその後、パケットをホストに送信する前に、マッピング アドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

自動 NAT および 手動 NAT

自動 *NAT* および 手動 *NAT* という 2 種類の方法でアドレス変換を実装できます。

手動 NAT の追加機能を必要としない場合は、自動 NATを使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP（VoIP）などのアプリケーションでは信頼性が高い場合があります（VoIP では、ルールで使用されているオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります）。

自動 NAT

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、自動 *NAT* ルールと見なされます。これは、ネットワーク オブジェクトに NAT を設定するための迅速かつ簡単な方法です。しかし、グループ オブジェクトに対してこれらのルールを作成することはできません。

これらのルールはオブジェクト自体の一部として設定されますが、オブジェクトマネージャを通してオブジェクト定義内の NAT 設定を確認することはできません。

パケットがインターフェイスに入ると、送信元 IP アドレスと宛先 IP アドレスの両方が 自動 NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元アドレスと宛先アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないため、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

手動 NAT

手動 NAT では、1 つのルールで送信元アドレスと宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポートアドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

自動 NAT と 手動 NAT の比較

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
  - 自動 NAT：NAT ルールがネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは、元の（実）アドレスとして機能します。
  - 手動 NAT：実際のアドレスとマッピングアドレス両方のネットワークオブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT 設定のパラメータとなります。実際のアドレスのネットワーク オブジェクト グループを使用できることは、手動 NAT がよりスケーラブルであることを意味します。
- 送信元および宛先 NAT の実装方法。

- 自動 NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような2つのルールを1つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
- 手動 NAT：1 つのルールにより送信元と宛先の両方が変換されます。1 つのパケットは1つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは、1 つの 手動 NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるため、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、送信元 A/宛先 A のペアには、送信元 A/宛先 B のペアとは異なる変換を適用できます。

- NAT ルールの順序。
  - 自動 NAT：NAT テーブルで自動的に順序付けされます。
  - 手動NAT：NATテーブルで手動で順序付けします（自動NATルールの前または後）。

NAT ルールの順序

自動 NAT および 手動 NAT ルールは、1 つのテーブルに保存されます。このテーブルは 3 つのセクションに分割されます。最初にセクション1のルール、次にセクション2、最後にセクション3というように、一致が見つかるまで順番に適用されます。たとえば、セクション1で一致が見つかった場合、セクション2とセクション3は評価されません。次の表に、各セクション内のルールの順序を示します。

（注） セクション 0 もあり、このセクションには、システムが使用するために作成される NAT ルールが含まれています。これらのルールは、他のすべてのルールよりも優先されます。これらのルールはシステムで自動的に作成され、必要に応じて xlate がクリアされます。セクション 0 では、ルールの追加、編集、または変更はできません。

表 *12 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	手動 NAT	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、手動NATルールはセクション 1 に追加されます。 「固有のルールを前に」とは、次のことを意味します。 • 静的ルールは動的ルールの前に配置する必要があります。 • 宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。 送信元アドレスまたは宛先アドレスに基づいて複数のルールが適用される可能性がある重複するルールを排除できない場合は、これらの推奨事項に従うように特に注意してください。
セクション 2	自動 NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 **1.** スタティック ルール **2.** ダイナミック ルール **各ルール タイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 3	手動 NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）
- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

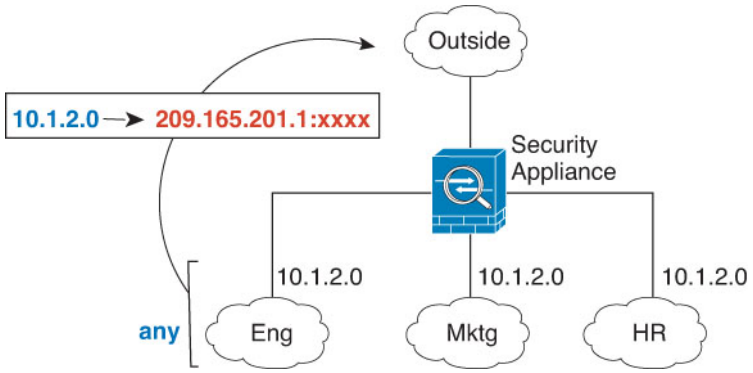
NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用されるNATルールを設定したり、特定の実際のインターフェイスとマッピング インターフェイスを識別したりできます。実際のアドレスには任意のインターフェイスを指定できます。マッピングインターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベートアドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバルプールに変換する場合、実際のアドレスに

任意のインターフェイスを指定し、マッピング アドレスには outside インターフェイスを指定します。

図 *36* : 任意のインターフェイスの指定



ただし、「任意」のインターフェイスの概念は、ブリッジ グループ メンバー インターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジ グループ メンバー インターフェイスが除外されます。そのため、ブリッジ グループ メンバーに NAT を適用するには、メンバー インターフェイスを指定する必要があります。この結果、1 つのインターフェイスのみが異なる同様のルールが多数作成されることになります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできず、メンバー インターフェイスにのみ NAT を設定できます。

パッシブ インターフェイスでは NAT を設定できません。

NAT のルーティング設定

脅威に対する防御デバイスは、変換された（マッピング）アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際の出力インターフェイスの決定に、指定した場合はその宛先インターフェイスが使用され、指定していない場合はルーティング テーブル ルックアップが使用されます。アイデンティティ NAT の場合は、宛先インターフェイスを指定している場合でも、ルート ルックアップの使用を選択できます。

必要となるルーティング設定のタイプは、マッピング アドレスのタイプによって異なります。以下の各トピックでは、その詳細について説明します。

マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、Threat Defense デバイス はプロキシ ARP を使用してマッピング アドレスの ARP 要求に応答し、マッピング アドレス宛てのトラフィックを代行受信します。この方法では、Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリー アドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変

換の数が大幅に拡張されるため、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

一意のネットワーク上のアドレス

宛先（マッピング）インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。アップストリーム ルータには、Threat Defense デバイス を指しているマッピング アドレスのスタティック ルートが必要です。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリーム ルータに適切なルートがあることを確認する必要があります。

アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。たとえば、「任意」の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP を有効のままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（「任意」のアドレスと一致する）NAT ルールと一致します。このとき、実際にはThreat Defense デバイス 向けのパケットでない場合でも、Threat Defense デバイス はこのアドレスの ARP をプロキシします（この問題は、手動 NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に Threat Defense デバイス の ARP 応答を受信した場合、トラフィックは誤って Threat Defense デバイス に送信されます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

インターフェイスのガイドライン

NAT は標準のルーテッド物理インターフェイスまたはルーテッド サブインターフェイスでサポートされます。

ただし、ブリッジ グループ メンバー インターフェイス（ブリッジ仮想インターフェイス、BVI の一部であるインターフェイス）での NAT の設定には次の制限があります。

- ブリッジ グループのメンバーに NAT を設定するには、メンバー インターフェイスを指定します。NAT をブリッジ グループ インターフェイス（BVI）自体に設定することはできません。

- ブリッジ グループ メンバー インターフェイス間で NAT を行う場合、送信元インターフェイスと宛先インターフェイスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、宛先インターフェイスがブリッジ グループのメンバー インターフェイスである場合、インターフェイス PAT を設定することはできません。
- 送信元インターフェイスと宛先インターフェイスが同じブリッジグループのメンバーである場合、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）同士を変換することはできません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66、およびダイナミック PAT44 のみが許可されている方法であり、ダイナミック PAT66 はサポートされません。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッド モードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 同じブリッジ グループのメンバーであるインターフェイスでは、IPv4 と IPv6 の間の変換はできません。2 つの IPv6 ネットワーク間または 2 つの IPv4 ネットワーク間でのみ変換できます。この制限は、ブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。
- 同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6対応のダイナミック PAT（NAT66）は使用できません。この制限は、ブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT のベストプラクティス

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます （手動 NAT のみ）。

- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（手動 NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。
- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するためにインスペクションが実行されます。

- ピンホールの作成：一部のアプリケーション プロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くため、ユーザーはそれらを許可するアクセス コントロール ルールを作成する必要はありません。
- NAT の書き換え：プロトコルの一部としてのパケット データ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制：一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用するインスペクション対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていないインスペクション対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。

（注） NAT の書き換えは、リストされているポートでのみサポートされます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 *13 : NAT* のサポート対象アプリケーション インスペクション

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	対応
Diameter	TCP/3868 TCP/5868（TCP/TLS 用） SCTP/3868	NAT/PAT なし。	対応
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	なし
ESMTP	TCP/25	NAT64 なし。	非対応
FTP	TCP/21	制限なし。	対応
GTP	UDP/3386 （GTPv0） UDP/2123（GTPv1+）	拡張 PAT はサポートされません。 NAT は使用できません。	—
H.323 H.225（コールシグナリング） H.323 RAS	TCP/1720 UDP/1718 RAS の場合、UDP/1718 ～ 1719	NAT64 なし。	対応
ICMP ICMP エラー	ICMP （デバイス インターフェイスに送信される ICMP トラフィックのインスペクションは実行されません）	制限なし。	非対応
IP オプション	RSVP	NAT64 なし。	非対応
M3UA	SCTP/2905	埋め込まれたアドレスに対する NAT または PAT はなし。	—
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	NAT64 なし。	非対応
RSH	TCP/514	PAT なし。 NAT64 なし。	対応

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
RTSP	TCP/554 （HTTP クローキングは処理しません）	NAT64 なし。	対応
SIP	TCP/5060 UDP/5060	拡張 PAT なし NAT64 または NAT46 なし	対応
Skinny（SCCP）	TCP/2000	NAT64、NAT46、または NAT66 なし	対応
SQL*Net （バージョン 1、2）	TCP/1521	NAT64 なし。	対応
SCTP	SCTP	SCTP トラフィックでスタティック ネットワーク オブジェクト NAT を実行できますが（ダイナミック NAT/PAT なし）、インスペクション エンジンは NAT には使用されません。	非対応
Sun RPC	TCP/111 UDP/111	NAT64 なし。	対応
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	対応
XDMCP	UDP/177	NAT64 なし。	対応

FQDN 宛先のガイドライン

IP アドレスの代わり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して、手動 NAT ルールに変換済み（マッピング）宛先を指定できます。たとえば、www.example.com Web サーバーを宛先とするトラフィックに基づいてルールを作成できます。

FQDN を使用すると、システムは DNS 解決を取得し、返されたアドレスに基づいて NAT ルールを書き込みます。DNS サーバーから複数のアドレスを取得する場合、使用されるアドレスは次の情報に基づきます。

- 指定したインターフェイスと同じサブネット上にアドレスがある場合は、そのアドレスが使用されます。同じサブネットに存在しない場合は、最初に返されたアドレスが使用されます。
- 変換後の送信元と変換後の宛先の IP タイプは一致している必要があります。たとえば、変換後の送信元アドレスが IPv6 の場合、FQDN オブジェクトはアドレスタイプとして IPv6 を指定する必要があります。変換後の送信元が IPv4 の場合、FQDN オブジェクトは IPv4 または IPv4 と IPv6 の両方を指定できます。この場合、IPv4 アドレスが選択されます。

手動 NAT 宛先に使用されるネットワークグループに FQDN オブジェクトを含めることはできません。NAT では、1 つの宛先ホストだけがこのタイプの NAT ルールに適しているため、FQDN オブジェクトは単独で使用する必要があります。

FQDN を IP アドレスに解決できない場合、DNS 解決が取得されるまでルールは機能しません。

NAT のその他のガイドライン

- ブリッジ グループのメンバーであるインターフェイスの場合は、メンバー インターフェイス用の NAT ルールを記述します。ブリッジ仮想インターフェイス（BVI）自体に対する NAT ルールは記述できません。
- サイト間 VPN で使用される仮想トンネルインターフェイス（VTI）の NAT ルールは作成できません。VTI の送信元インターフェイスのルールを作成すると、NAT は VPN トンネルに適用されません。VTI でトンネリングされた VPN トラフィックに適用される NAT ルールを作成するには、インターフェイスとして [any] を使用する必要があります。インターフェイス名を明示的に指定することはできません。
- （自動 NAT のみ）。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- インターフェイスで VPN が定義されている場合、そのインターフェイスの着信 ESP トラフィックには NAT ルールは適用されません。システムは、確立済みの VPN トンネルに対してのみ ESP トラフィックを許可し、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制約は、ESP および UDP のポート 500 と 4500 に適用されます。
- ダイナミック PAT を適用するデバイスの背後のデバイス（VPN UDP ポート 500 と 4500 は実際に使用されるポートではない）でサイト間 VPN を定義した場合、PAT デバイスの背後にあるデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンダはセキュリティ アソシエーション（SA）を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションを使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

  既存の接続（VPN トンネルなど）に適用する新しい NAT ルールを作成する場合は、**clear conn** を使用して接続を終了する必要があります。その後、接続を再確立しようとすると、NAT ルールが適用され、接続が正しく NAT 変換されます。

（注） ダイナミック NAT または PAT ルールを削除し、削除したルールに含まれるアドレスと重複するマッピングアドレスを含む新しいルールを追加すると、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** または **clear conn** コマンドを使用してクリアされるまで、新しいルールは使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを含めることはできません。オブジェクト グループには、1 つのタイプのアドレスのみを含める必要があります。
- アドレスやサブネットの範囲内で明示的に指定するか暗黙的に指定するかにかかわらず、NAT で使用されるネットワークオブジェクトに 131,838 を超える IP アドレスを含めることはできません。アドレス空間をより狭い範囲に分割し、小さなオブジェクトに対して個別のルールを作成します。
- （手動 NATのみ）。NAT ルールで送信元アドレスとして **any** を使用する場合、「any」トラフィックの定義（IPv4 と IPv6）はルールによって異なります。Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Threat Defense デバイス は、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。"any" から "any" へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピング インターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。
  - マッピング インターフェイスの IP アドレス。ルールに「any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合は、インターフェイス アドレスの代わりにインターフェイス名を指定します。
  - フェールオーバー インターフェイスの IP アドレス。
  - （ダイナミック NAT）VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。

- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。
- NATは、通過トラフィックにのみ適用されます。システムによって生成されたトラフィックは、NAT の対象外です。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- Protocol Independent Multicast（PIM）レジスタの内部ペイロードで NAT を使用することはできません。
- （手動 NAT）デュアル ISP インターフェイス セットアップ（ルーティング設定でサービス レベルアグリーメントを使用するプライマリインターフェイスとバックアップインターフェイス）のNATルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリインターフェイスのルールがバックアップインターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリインターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 nat-no-xlate-to-pat-pool が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。

NAT の設定

ネットワーク アドレス変換は非常に複雑な場合があります。変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。次の手順では、基本的なアプローチを示します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** を選択します。

ステップ 2 必要なルールを決定します。

ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールを作成できます。概要については、「NAT タイプ （677 ページ）」を参照してください。

ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。

これらの 2 つの実装オプションの比較については、自動 NAT および 手動 NAT （678 ページ）を参照してください。

ステップ 4 次の項で説明するルールを作成します。

- ダイナミック NAT （692 ページ）
- ダイナミック PAT （698 ページ）
- スタティック NAT （704 ページ）
- アイデンティティ NAT （714 ページ）

ステップ 5 NAT ポリシーとルールを管理します。

ポリシーとそのルールを管理するには、次のことを行います。

- ルールを編集するには、ルールの編集アイコン（）をクリックします。
- ルールを削除するには、ルールの [削除（delete）] アイコン（）をクリックします。

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

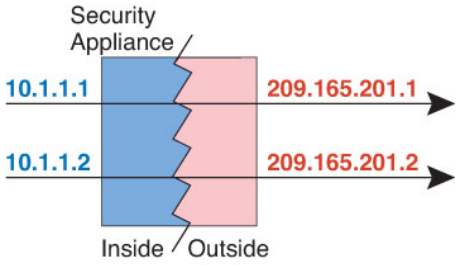
ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス ルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

（注） 変換が継続している間、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

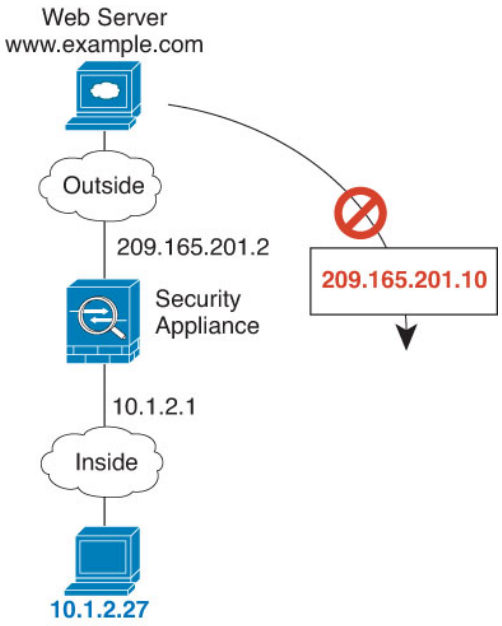
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 *37* : ダイナミック *NAT*



次の図に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 *38* : マッピング アドレスへの接続開始を試みているリモート ホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  PAT では、1 つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持ち、オープン スタンダードではないアプリケーションでも機能しません。

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールを使用して、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

[オブジェクト（Objects）] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス（Original Address）]：ネットワーク オブジェクト（グループではなく）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [元のアドレス（Original Address）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。

ステップ 5 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え （762 ページ）」を参照してください。
- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 6 [OK] をクリックします。

ダイナミック手動 NAT の設定

自動 NAT では要件を満たせない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

[オブジェクト（Objects）] を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス（Original Destination Address）] および [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトを作成できます。

ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクト マネージャで、[元の宛先ポート（Original Destination Port）] と [変換済み宛先ポート（Translated Destination Port）] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[手動NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：Where you want to add the rule. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

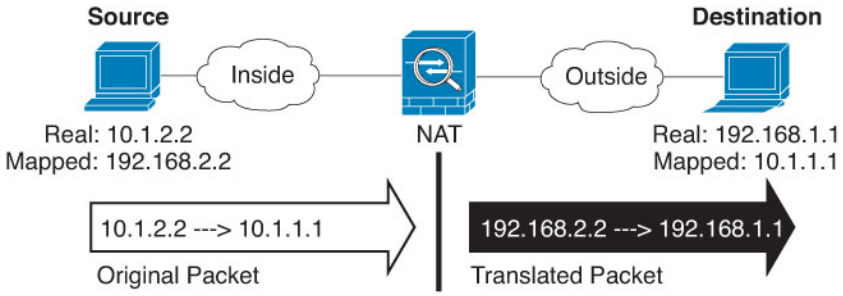
ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが

適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [インターフェイス（Interface）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）] のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）] フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

ステップ 8 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え （762 ページ）」を参照してください。
- [インターフェイス PAT へのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。

ステップ 9 [OK] をクリックします。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図は、ダイナミック PAT の一般的なシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピングアドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 *39* : ダイナミック *PAT*

変換が継続している間、アクセス ルールで許可されていれば、宛先ネットワーク上のリモート ホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。

（注） インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイス、特に「any」インターフェイスに同じプールを使用すると、プールがすぐに枯渇し、新しい変換に使用できるポートがなくなります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。ただし、インターフェイス上の IPv6 アドレスに対しインターフェイス PAT を使用することはできません。

同じブリッジ グループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT（NAT66）は使用できません。この制限は、ブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、インスペクション対象プロトコルに対する NAT サポート （686 ページ）を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバーで DoS 攻撃として解釈される可能性があります。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

始める前に

[オブジェクト（Objects）] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス（Original Address）]：ネットワーク オブジェクト（グループではなく）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）]：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
  - [単一の PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [元のアドレス（Original Address）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：次のいずれかになります。

- （インターフェイス PAT）宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。
- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。

ステップ 5 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [インターフェイスPATへのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 6 [OK] をクリックします。

ダイナミック手動 PAT の設定

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

始める前に

[オブジェクト（Objects）] を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元アドレス（Translated Source Address）：PAT アドレスを指定するオプションは次のとおりです。

- [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
- [単一の PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス（Original Destination Address）] と [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトも作成できます。

ダイナミック PAT の場合、宛先でポート変換を実行することもできます。オブジェクトマネージャで、[元の宛先ポート（Original Destination Port）] と [変換済み宛先ポート（Translated Destination Port）] に使用できるポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

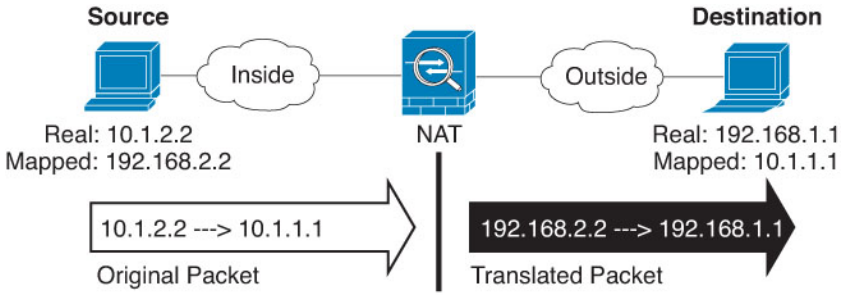
- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[手動NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：Where you want to add the rule. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバーインターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [インターフェイス（Interface）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：次のいずれかになります。
  - （インターフェイス PAT）宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）] フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

ステップ 8 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [インターフェイスPATへのフォールスルー（Fallthrough to Interface PAT）]（宛先インターフェイス）：その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 9 [OK] をクリックします。

スタティック NAT

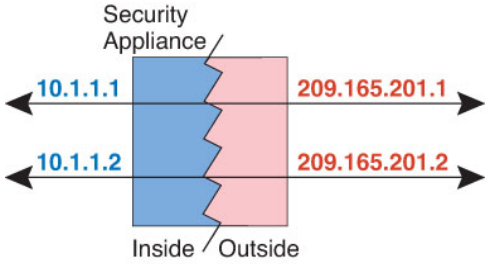
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じであるため、スタティック NAT では、双方向の接続（ホストへの接続とホストから接続の両方）を開始できます（接続を許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブであるため、実際のホストとリモート ホストの両方が接続を開始できます。

図 *40* : スタティック *NAT*



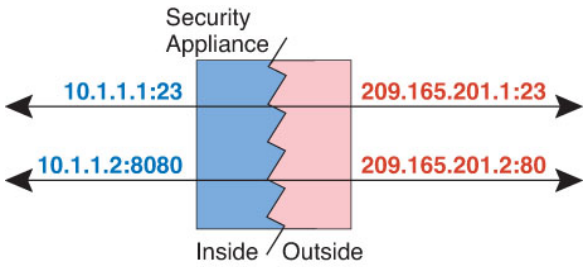
ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルおよびポートとマッピングされたプロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IP アドレスは別の値にマッピングされています。この変換は常にアクティブであるため、変換されたホストとリモート ホストの両方が接続を開始できます。

図 *41* : ポート変換を設定したスタティック *NAT* の一般的なシナリオ



ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルール対象外の別のポートで宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。さらに、手動 NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックが宛先 IP アドレスと一致する場合、宛先ポートに関係なくドロップされます。したがって、宛先 IP アドレスに対して許可される他のすべてのトラフィックに追加ルールを追加する必要があります。たとえば、ポートを指定せずに IP アドレスにスタティック NAT ルールを設定し、ポート変換ルールの後ろにそれを配置できます。

（注） セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、NAT が自動的にセカンダリ ポートを変換します。

次に、ポート変換を設定したスタティック NAT のその他の使用例の一部を示します。

アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する 3 つの個別のサーバ（FTP、HTTP、SMTP など）がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバーの正しい IP アドレスにマッピングできます。サーバーは標準のポート（それぞれ 21、80、および 25）を使用しているため、ポートを変更する必要はありません。

標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT を使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

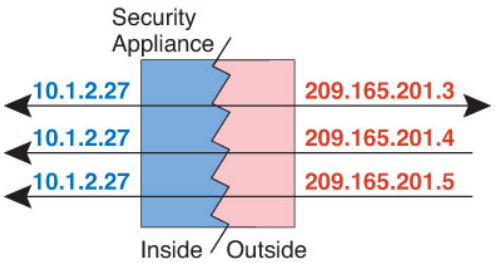
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

1 対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし、場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティック NAT を設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピング アドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピング アドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

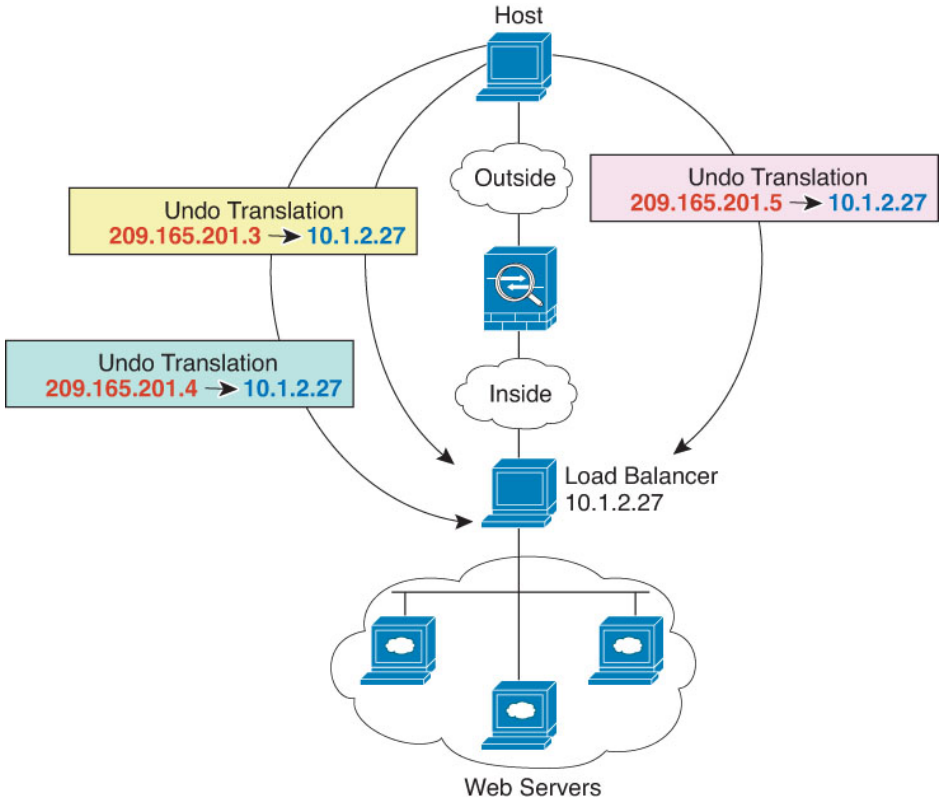
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *42 :* 一対多のスタティック *NAT*



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *43 : 1* 対多のスタティック *NAT* の例



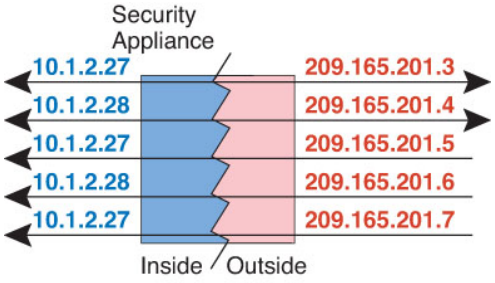
他のマッピング シナリオ（非推奨）

NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は 1 対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して 1 対多の設定を作成することをお勧めします。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次のマッピング アドレスが最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1 対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 *44 :* 少対多のスタティック *NAT*

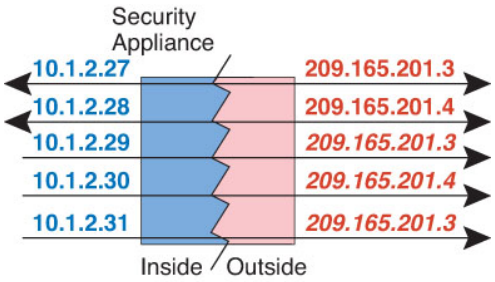


多対少または多対1コンフィギュレーションでは、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピング プールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注） 多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じIPアドレスに変換されると、アドレスの競合がある（5つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *45 :* 多対少のスタティック *NAT*



このようにスタティックルールを使用するのではなく、双方向の開始を必要とするトラフィックに1対1のルールを作成し、残りのアドレスにダイナミックルールを作成することをお勧めします。

スタティック自動 NAT の設定

スタティック自動 NAT ルールを使用して、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト（Objects）] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス（Original Address）]：ネットワーク オブジェクト（グループではなく）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（destination interface）]：宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

ステップ 1 **[ポリシー（Policies）] > [NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[スタティック（Static）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] は

マッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

- [元のアドレス（Original Address）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- （オプション）[元のポート（Original Port）]、[Translated Port（変換済みポート）]：TCP または UDP ポートを変換する必要がある場合、元のポートと変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコル用でなければなりません。そのオブジェクトがまだ存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

ステップ 5 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え（762 ページ）」を参照してください。このオプションはポート変換を行う場合は使用できません。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の

場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ 6 [OK] をクリックします。

スタティック手動 NAT の設定

自動 NAT がニーズを満たさない場合、スタティック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト（Objects）] を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [宛先インターフェイス（destination interface）]：宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス（Original Destination Address）] および [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。Object Manager では、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

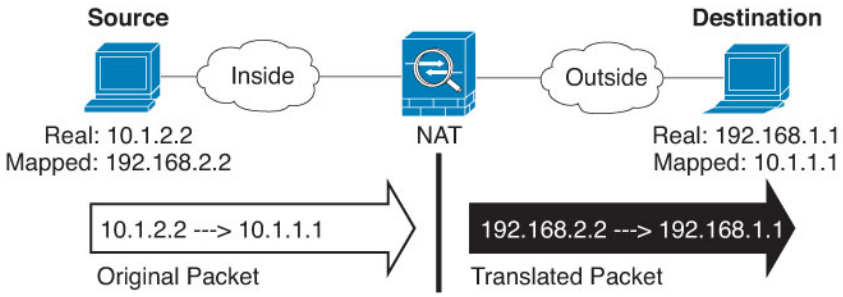
- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[手動NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：Where you want to add the rule. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）]：[スタティック（Static）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [インターフェイス（Interface）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- [元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え（762 ページ）」を参照してください。 このオプションはポート変換を行う場合は使用できません。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ 9 [OK] をクリックします。

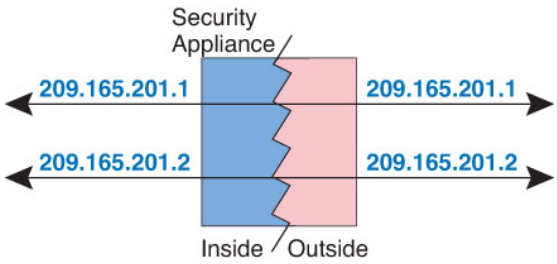
アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、NAT を各ネットワークに適するものの、1 つのネットワークを NAT から除外するとい

う広範なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換できます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 *46 : アイデンティティ NAT*



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

スタティック アイデンティティ自動 NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

[オブジェクト（Objects）] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス（Original Address）] : ネットワーク オブジェクト（グループではなく）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）] : 元の送信元オブジェクトとコンテンツがまったく同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

手順

ステップ 1 **[ポリシー（Policies）] > [NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[スタティック（Static）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [元のアドレス（Original Address）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

アイデンティティ NAT には、[元のポート（Original Port）] オプションと [変換済みポート（Translated Port）] オプションを設定しないでください。

ステップ 5 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [宛先インターフェイスのルート ルックアップの実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 6 [OK] をクリックします。

アイデンティティ手動 NAT の設定

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

[オブジェクト（Objects）] を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義しているときにオブジェクトを作成することもできます。またオブジェクトは次の要件も満たす必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス（Original Destination Address）] および [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトを作成できます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。Object Manager では、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT には同じオブジェクトを使用できます。

手順

ステップ 1 **[ポリシー（Policies）] > [NAT]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（）をクリックします。

（不要になったルールを削除するには、ルールの [ごみ箱（trash can）] アイコンをクリックします）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。

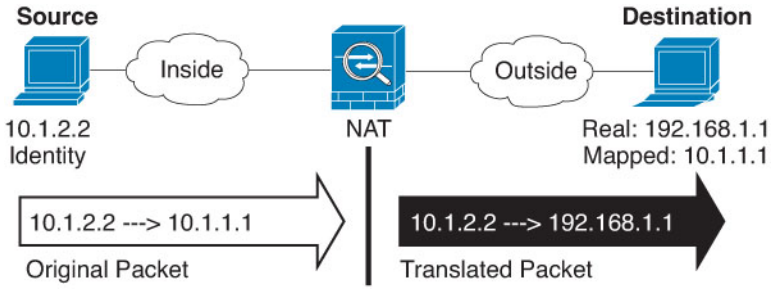
- [ルールの作成対象（Create Rule For）]：[手動NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：Where you want to add the rule. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）]：[スタティック（Static）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケット アドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



- [元の送信元アドレス（Original Source Address）]：変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（任意）宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

  [インターフェイス（Interface）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）] のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- [元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細オプション（Advanced Options）] リンクをクリックし、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [宛先インターフェイスのルートルックアップの実行（Perform route lookup for Destination Interface）]：元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代

わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 9 [OK] をクリックします。

Threat Defense の NAT ルールのプロパティ

ネットワークアドレス変換（NAT）ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、NAT ルールを使用してプライベート アドレスをパブリックにルーティングできるアドレスに変換します。1 つのアドレスから別のアドレスに変換するか、ポートアドレス変換（PAT）を使用して多数のアドレスを 1 つに変換し、ポート番号を使用して送信元アドレスを識別できます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

[役職（Title）]

ルールの名前を入力します。名前にスペースを含めることはできません。

[ルールの作成対象（Create Rule For）]

変換ルールを [自動NAT（Auto NAT）] にするか、[手動NAT（Manual NAT）] にするか。自動 NAT は手動 NAT よりシンプルですが、手動 NAT を使用すると、宛先アドレスに基づいて送信元アドレスの個別の変換を作成できます。

[ステータス（Status）]

ルールをアクティブにするか無効にするか。

[配置（Placement）]（手動 NAT のみ）

Where you want to add the rule. ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。

[タイプ（Type）]

変換ルールを [ダイナミック（Dynamic）] にするか、[スタティック（Static）] にするかを指定します。ダイナミック変換では、アドレス プールからマッピング アドレスが自動的に選択されるか、または、PAT の実装時にはアドレス/ポートの組み合わせが自動的に選択されます。マッピングアドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

次に、残りの NAT ルール プロパティを説明します。

自動 NAT のパケット変換プロパティ

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスと変換済みマッピング アドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

[送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]

（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

[元のアドレス（Original Address）]（常に必須）

変換している送信元アドレスを含むネットワーク オブジェクト。グループではなくネットワーク オブジェクトにする必要があり、ホスト、範囲、またはサブネットを含めることができます。

[変換済みアドレス（Translated Address）]（通常は必須）

変換先のマッピングアドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミックNAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにできますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかを実行します。
  - （インターフェイス PAT）宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- [スタティックNAT（Static NAT）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インター

フェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。

- [アイデンティティ NAT（Identity NAT）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

[元のポート（Original Port）]、[変換済みポート（Translated Port）]（スタティック NAT のみ）。

TCP または UDP ポートを変換する必要がある場合、元のポートおよび変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコル向けにする必要があります。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

手動 NAT のパケット変換プロパティ

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスと変換済みマッピング アドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

[送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]

（ブリッジ グループ メンバー インターフェイスに必須）この NAT ルールが適用されるインターフェイス。[送信元（Source）] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先（Destination）] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバー インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

[元の送信元アドレス（Original Source Address）]（常に必須）

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることが可能で、ホスト、範囲、またはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールに [すべて（Any）] を指定します。

[変換済み送信元アドレス（Translated Source Address）]（通常は必須）

変換先のマッピング アドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミック NAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにできますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかを実行します。
  - （インターフェイス PAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバー

インターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。

- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。

- [スタティックNAT（Static NAT）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイスNAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。

- [アイデンティティ NAT（Identity NAT）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

[元の宛先アドレス（Original Destination Address）]

宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス（Interface）] を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにできます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスにポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

[変換済み宛先アドレス（Translated Destination Address）]

変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

変換後の宛先として完全修飾ドメイン名を指定するネットワークオブジェクトを使用できます。詳細については、FQDN 宛先のガイドライン （688 ページ）を参照してください。

[元の送信元ポート（Original Source Port）]、[変換済み送信ポート（Translated Source Port）]、[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポート オブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上できます。サービスを設定するときは、次のルールに注意してください。

- （ダイナミック NAT または PAT）[元の送信元ポート（Original Source Port）] および [変換済み送信元ポート（Translated Source Port）] では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じオブジェクトを使用できます。

詳細 NAT プロパティ

NAT を設定するとき、[詳細（Advanced）] オプションで特別なサービスを提供するプロパティを設定できます。これらのプロパティはすべてオプションであり、該当サービスが必要な場合だけに設定します。

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 AAAA）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、「NAT を使用した DNS クエリと応答の書き換え（762 ページ）」を参照してください。このオプションは、スタティック NAT ルールでポート変換を行っているときは利用できません。

[インターフェイス PAT（宛先インターフェイス）へのフォールスルー（Fallthrough to Interface PAT (Destination Interface)）]（ダイナミック NAT のみ）

その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。このオプションは、IPv6 ネットワークでは使用できません。

宛先インターフェイスでプロキシ ARP なし（スタティック NAT のみ）

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

宛先インターフェイスでルート ルックアップを実行します（スタティック ID NAT のみ。ルーテッド モードのみ）

元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

IPv6 ネットワークの変換

IPv6 専用ネットワークと IPv4 専用ネットワークの間でトラフィックを通過させる必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークから内部アドレスを隠す必要がある場合があります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4（およびその反対）に変換します。2 つのポリシーを定義する必要があります。1 つは IPv6 から IPv4 への変換用、もう 1 つは IPv4 から IPv6 への変換用です。これは、1 つの 手動 NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

（注） NAT46 がサポートするのは、スタティック マッピングのみです。

- NAT66：IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

（注） NAT64 および NAT 46 は、標準的なルーテッド インターフェイスでのみ使用できます。NAT66 は、ルーテッド インターフェイスとブリッジ グループ メンバー インターフェイスの両方で使用できます。

NAT64/46：IPv6 アドレスの IPv4 への変換

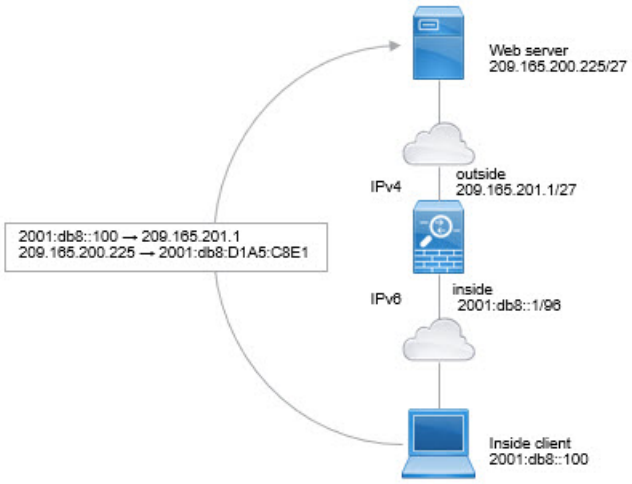
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2 つのアドレス プール（IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレス プールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレス プール）を定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは通常は小さく、一般的に IPv6 クライアント アドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比べると、多数の IPv6 クライアント アドレスがある場合でも、比較的簡単に対応できます。
- NAT 46 ルールの IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティック マッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。これは、1 つの 手動 NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

NAT64/46 の例：内部 IPv6 ネットワークと外部 IPv4 インターネット

次に、内部 IPv6 専用ネットワークがある場合に、インターネットに送信されるトラフィックを IPv4 に変換する簡単な例を示します。この例の想定では DNS 変換が不要なため、1 つの 手動 NAT ルールで NAT64 と NAT46 の両方の変換を実行できます。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。

手順

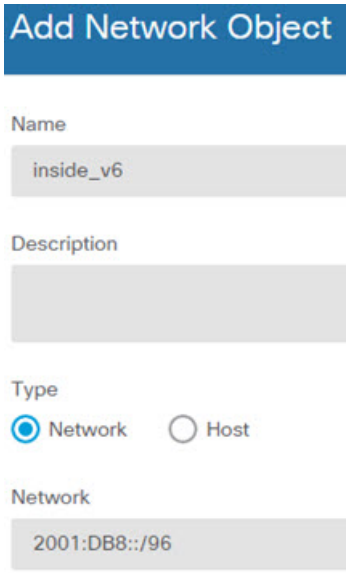
ステップ 1 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス（2001:db8::/96）を入力します。



d) **[OK]** をクリックします。

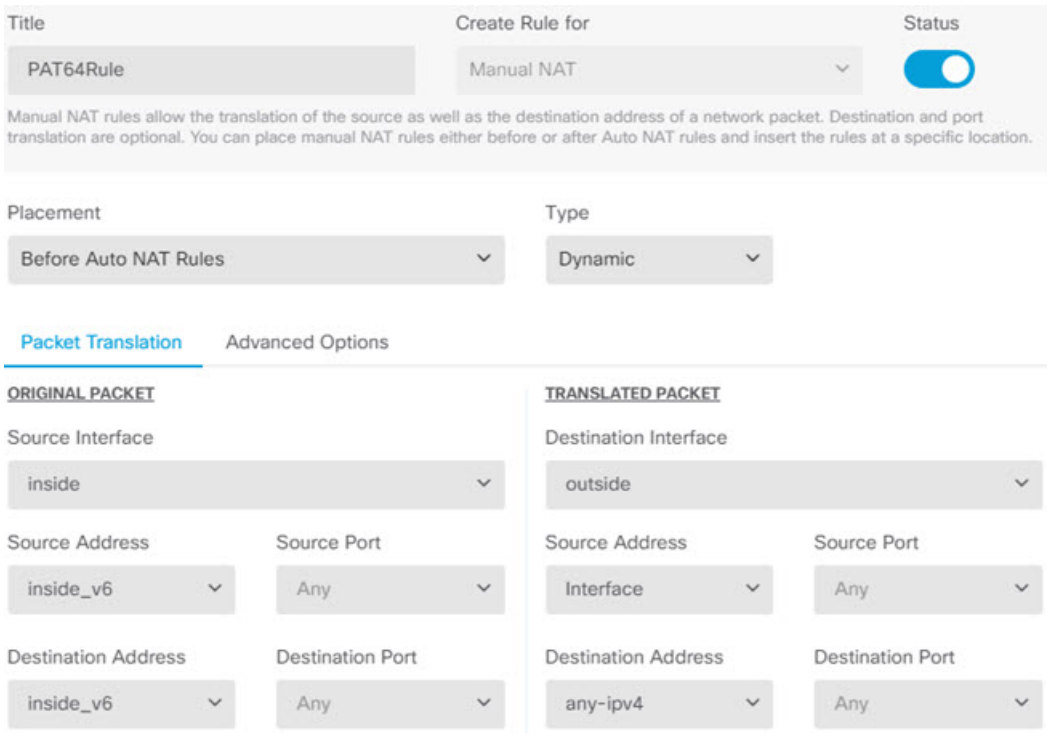
ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための手動 NAT ルールを作成します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = PAT64Rule（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [手動 NAT（Manual NAT）]。
- [配置（Placement）] = [自動NATルールの前（Before Auto NAT Rules）]
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のパケット発信元アドレス（Original Packet Source Address）] = inside_v6 ネットワークオブジェクト
- [変換済みパケット発信元アドレス（Translated Packet Source Address）]：[インターフェイス（Interface）]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。
- [元のパケット宛先アドレス（Original Packet Destination Address）] = inside_v6 ネットワークオブジェクト
- [変換済みパケット宛先アドレス（Translated Packet Destination Address）] = any-ipv4 ネットワークオブジェクト

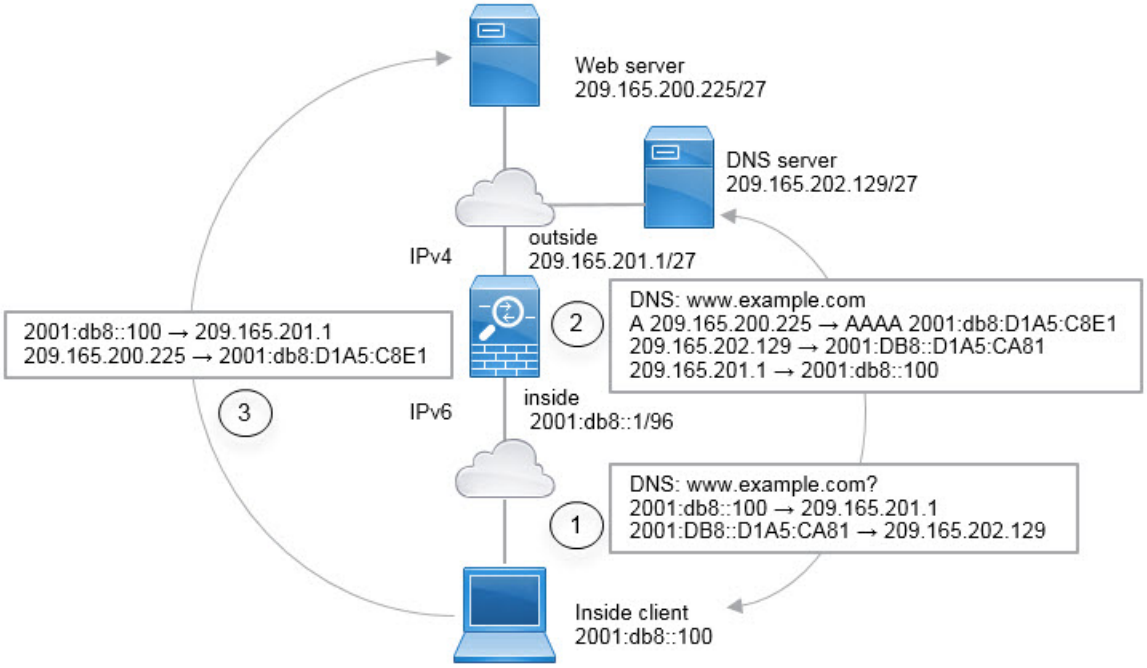


d) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。逆に、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。

NAT64/46 の例：外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザーが必要とするいくつかの IPv4 専用サービスが外部のインターネット上に存在する一般的な例です。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバーからの応答を A（IPv4）レコードから AAAA（IPv6）レコードに変換でき、アドレスが IPv4 から IPv6 に変換されます。

次は、内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとしている場合の Web 要求の一般的なシーケンスです。

1. クライアントのコンピュータが 2001:DB8::D1A5:CA81 にある DNS サーバーに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先が次のように変換されます。
   - 2001:DB8::100 を 209.165.201.1 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
   - 2001:DB8::D1A5:CA81 を 209.165.202.129 に変換（NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 に相当します）。
2. DNS サーバーが、www.example.com が 209.165.200.225 であることを示す A レコードに応答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
   - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
   - 209.165.201.1 を 2001:db8::100 に変換

3. これで、IPv6 クライアントが Web サーバーの IP アドレスを取得し、www.example.com（2001:db8:D1A5:C8E1）に HTTP 要求を送信できます。（D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します）。HTTP 要求の送信元と宛先が変換されます。
   - 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
   - 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換（NAT46 ルール）。

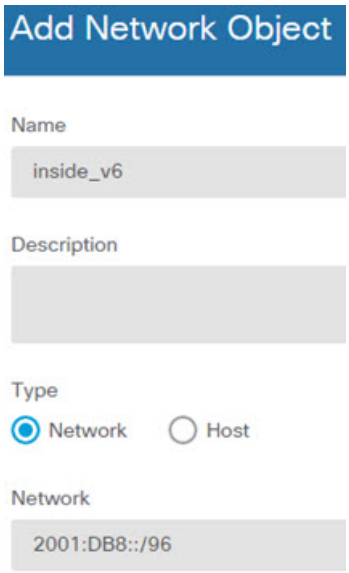
次の手順では、この例の設定方法について説明します。

手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワーク オブジェクトを作成します。

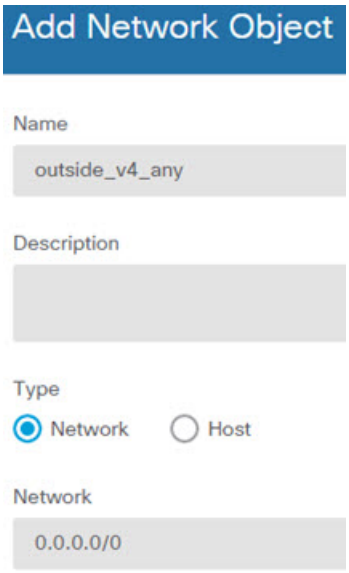
a) [オブジェクト（Objects）] を選択します。
b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス（2001:db8::/96）を入力します。



d) **[OK]** をクリックします。
e) [+] をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前（outside_v4_any など）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス（0.0.0.0/0）を入力します。



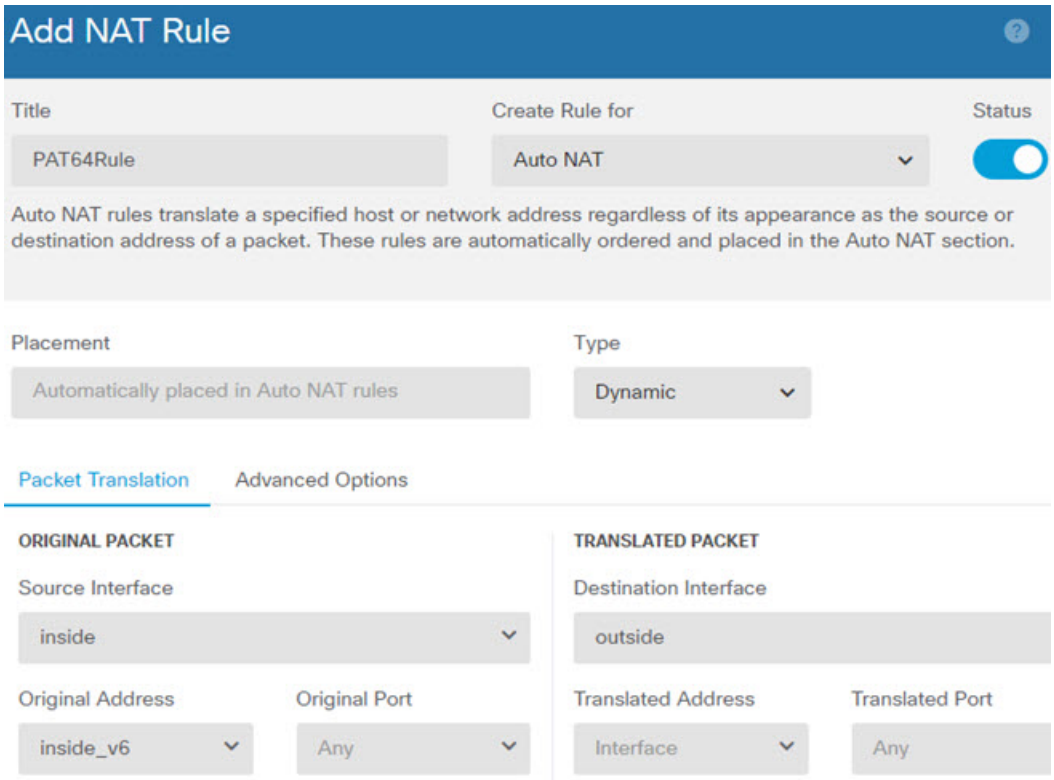
ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = PAT64Rule（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト（inside_v6 network object）
- [変換済みアドレス（Translated Address）] = [インターフェイス（Interface）]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。



d) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

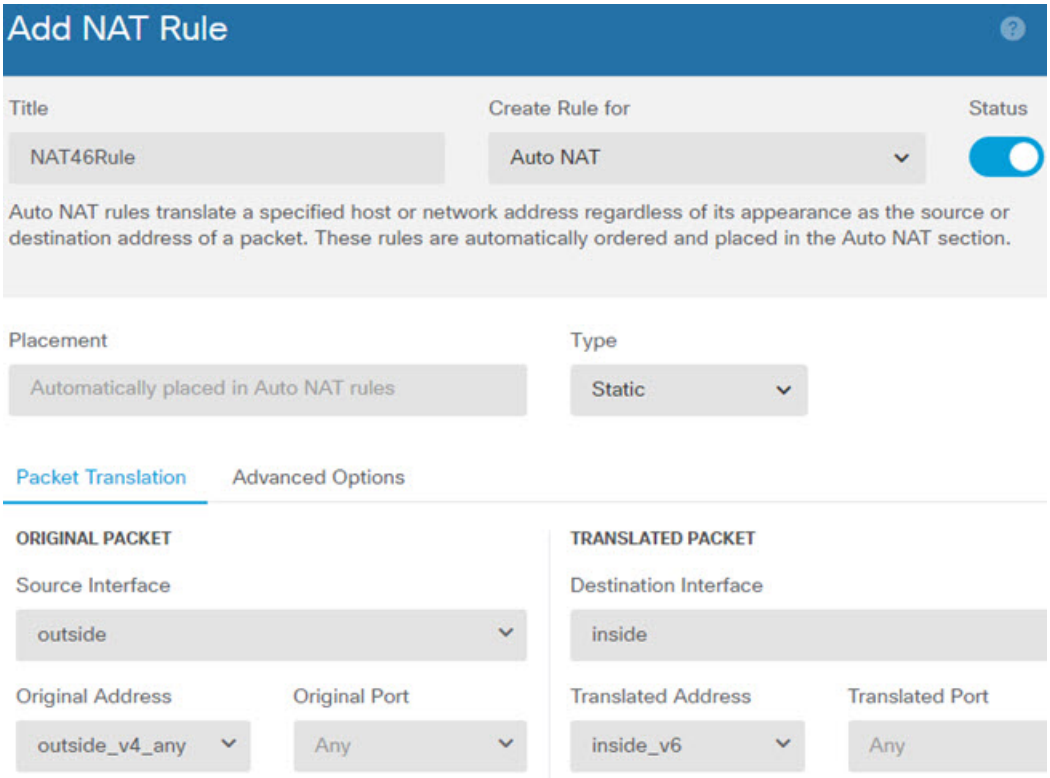
ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）] = NAT46Rule（またはユーザーが選択する別の名前）。
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = [外部（outside）]
- [宛先インターフェイス（Destination Interface）] = [内部（inside）]
- [元のアドレス（Original Address）] = outside_v4_any ネットワーク オブジェクト（outside_v4_any network object）。
- [変換済みアドレス（Translated Address）] = inside_v6 ネットワーク オブジェクト（inside_v6 network object）

- [詳細オプション（Advanced Options）] タブで、[このルールと一致するDNS応答を変換（Translate DNS replies that match this rule）] を選択します。



c) [OK] をクリックします。

このルールを使用すると、内部インターフェイスに届く外部ネットワークのすべての IPv4 アドレスが、組み込みの IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答が A（IPv4）レコードから AAAA（IPv6）レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

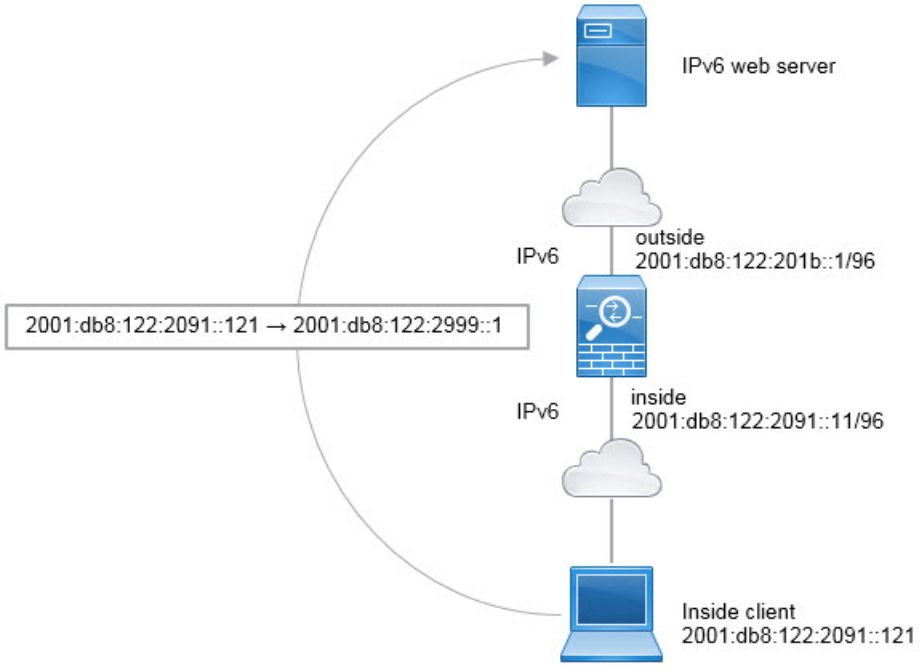
NAT66：IPv6 アドレスの異なる IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。これらのルールは、自動 NATを使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、手動 NAT のみを使用してスタティック NAT ルールを単方向にできます。

NAT66 の例：ネットワーク間のスタティック変換

自動 NATを使用して、IPv6 アドレスプール間のスタティック変換を設定できます。次の例では、2001:db8:122:2091::/96 ネットワークの内部アドレスを 2001:db8:122:2999::/96 ネットワークの外部アドレスに変換する方法について説明します。



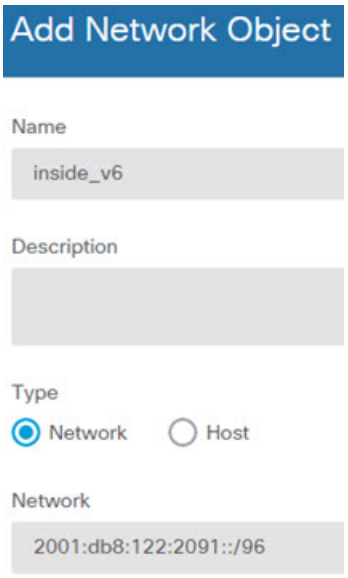
（注） この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッド インターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

ステップ 1 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。
b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 内部 IPv6 ネットワークを定義します。

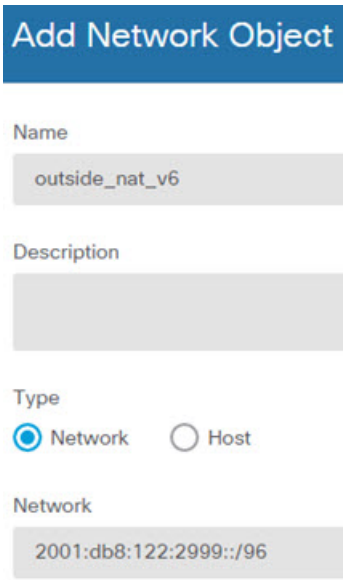
ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス（2001:db8:122:2091::/96）を入力します。



d) **[OK]** をクリックします。

e) [+] をクリックして、外部 IPv6 PAT ネットワークを定義します。

ネットワーク オブジェクトに名前（outside_nat_v6 など）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス（2001:db8:122:2999::/96）を入力します。



ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

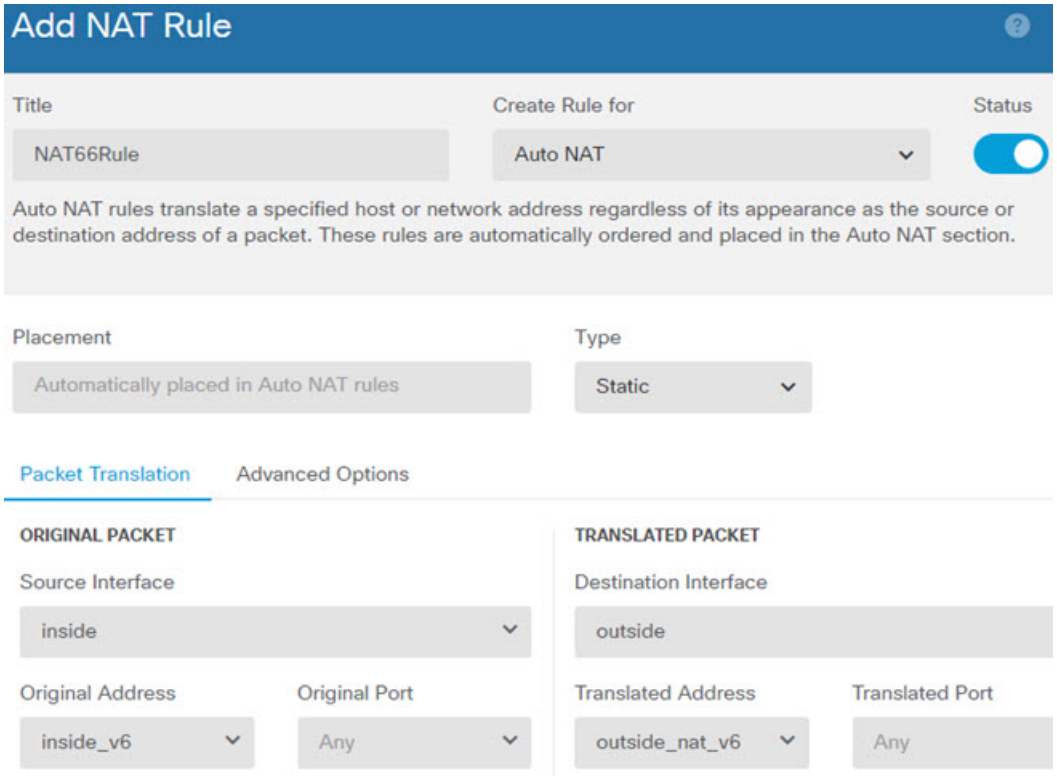
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = NAT66Rule（またはユーザーが選択する別の名前）

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト（inside_v6 network object）
- [変換済みアドレス（Translated Address）] = outside_nat_v6 ネットワーク オブジェクト（outside_nat_v6 network object）。



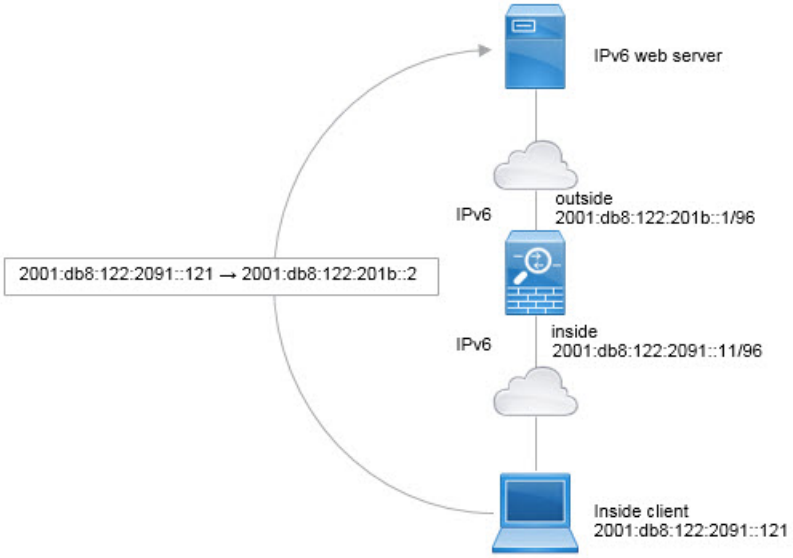
d) [OK] をクリックします。

このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスにスタティック NAT66 変換されます。

NAT66 の例：シンプルな IPv6 インターフェイス PAT

NAT66 を実装するための簡単なアプローチは、外部インターフェイスの IPv6 アドレス上の異なるポートに内部アドレスを動的に割り当てる方法です。

ただし、Device Manager を使用して、インターフェイスの IPv6 アドレスを使用するインターフェイス PAT は設定できません。代わりに、同じネットワーク上の 1 つの空きアドレスをダイナミック PAT プールとして使用します。



（注） この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッド インターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

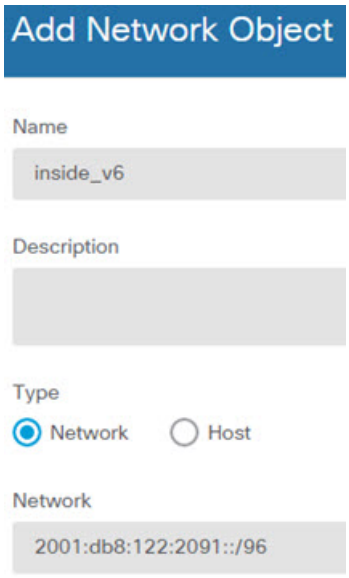
ステップ 1 内部 IPv6 ネットワークと IPv6 PAT アドレスを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス（2001:db8:122:2091::/96）を入力します。



d) **[OK]** をクリックします。

e) [+] をクリックして、外部 IPv6 PAT アドレスを定義します。

ネットワーク オブジェクトに名前（inside_v6 など）を付け、[ホスト（Host）] を選択して、ホスト アドレス（2001:db8:122:201b::2）を入力します。

ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

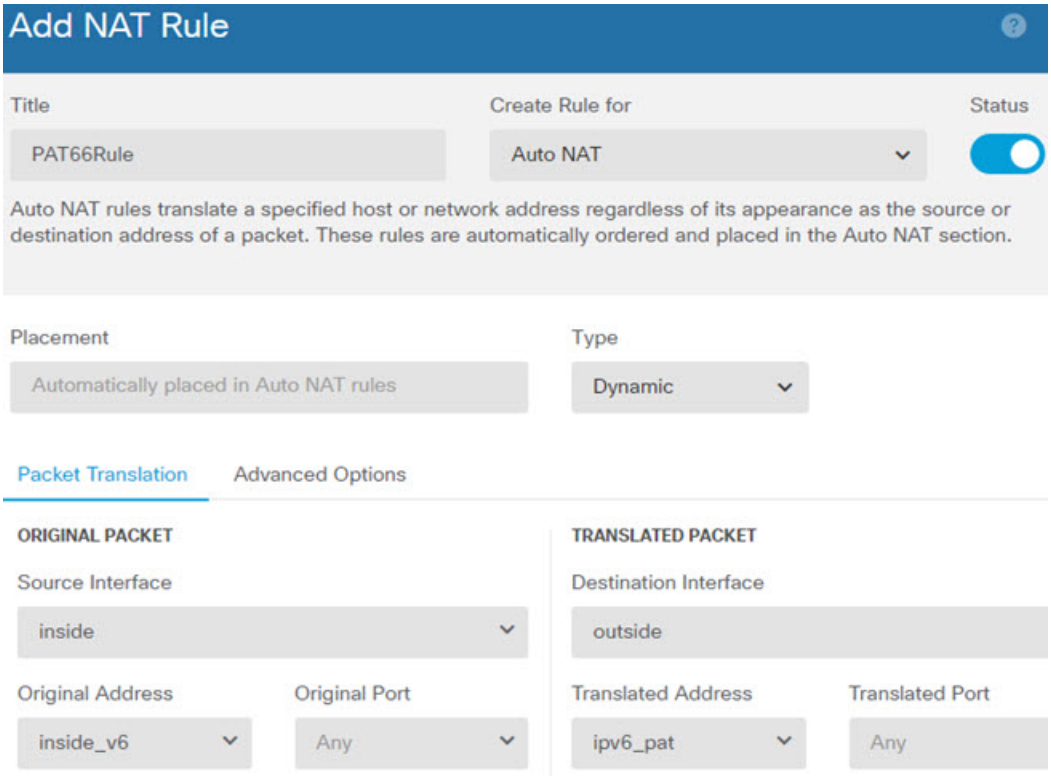
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = PAT66Rule（またはユーザーが選択する別の名前）。

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト（inside_v6 network object）
- [変換済みアドレス（Translated Address）] = ipv6_pat ネットワーク オブジェクト（ipv6_pat network object。



d) [OK] をクリックします。

このルールを使用すると、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:201b::2 のポートにダイナミック PAT66 変換されます。

NAT のモニタリング

NAT接続をモニターしてトラブルシューティングを実行するには、CLIコンソールを開くかデバイス CLI にログインして次のコマンドを使用します。

- **show nat** NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換を消去することで、クライアントの次回の接続時に、システムは新しいルールに基づいてクライアントの新しい変換を作成します。（このコマンドは CLI コンソールでは使用できません。）

NAT の例

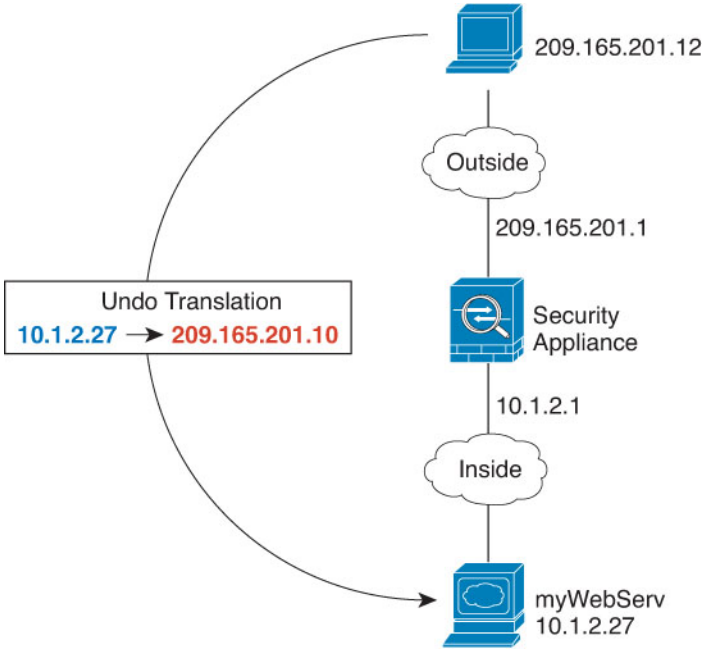
以下の各トピックでは、Threat Defense デバイスでの NAT の設定例を紹介します。

内部 Web サーバーへのアクセスの提供（スタティック自動 NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバーへのトラフィックをホストが開始できるようにするために必要です。

（注） この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッド インターフェイスであることを前提としています。内部インターフェイスが BVI の場合、Web サーバーが接続されている特定のブリッジ グループ メンバー インターフェイス（inside1_3 など）を選択します。

図 *47 :* 内部 *Web* サーバーのスタティック *NAT*



手順

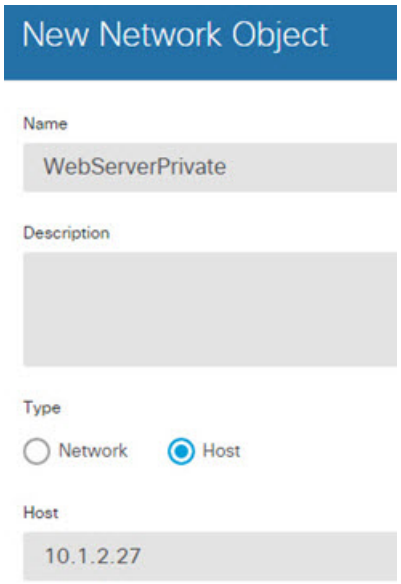
ステップ 1 サーバーのプライベート ホスト アドレスとパブリック ホスト アドレスを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) Web サーバのプライベート アドレスを定義します。

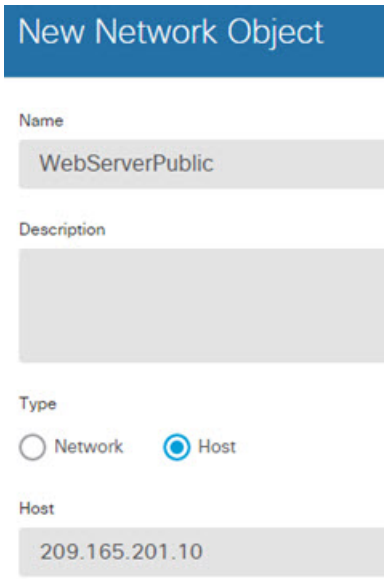
ネットワーク オブジェクトに名前（WebServerPrivate など）を付け、[ホスト（Host）] を選択して、実際のホスト IP アドレス（10.1.2.27）を入力します。



d) **[OK]** をクリックします。

e) [+] をクリックして、パブリック アドレスを定義します。

ネットワーク オブジェクトに名前（WebServerPublic など）を付け、[ホスト（Host）] を選択して、ホスト アドレス（209.165.201.10）を入力します。



f) **[OK]** をクリックします。

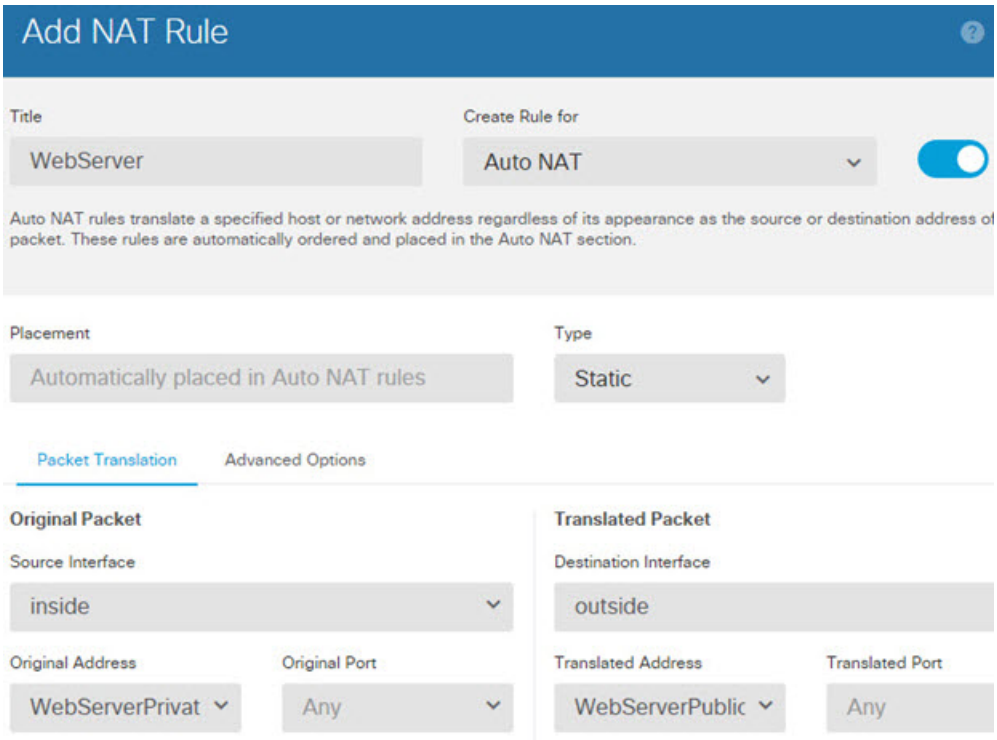
ステップ 2 オブジェクトのスタティック NAT を設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = WebServer（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）] = WebServerPrivate ネットワーク オブジェクト（WebServerPrivate network object）
- [変換済みアドレス（Translated Address）] = WebServerPublic ネットワーク オブジェクト（WebServerPublic network object）



d) [OK] をクリックします。

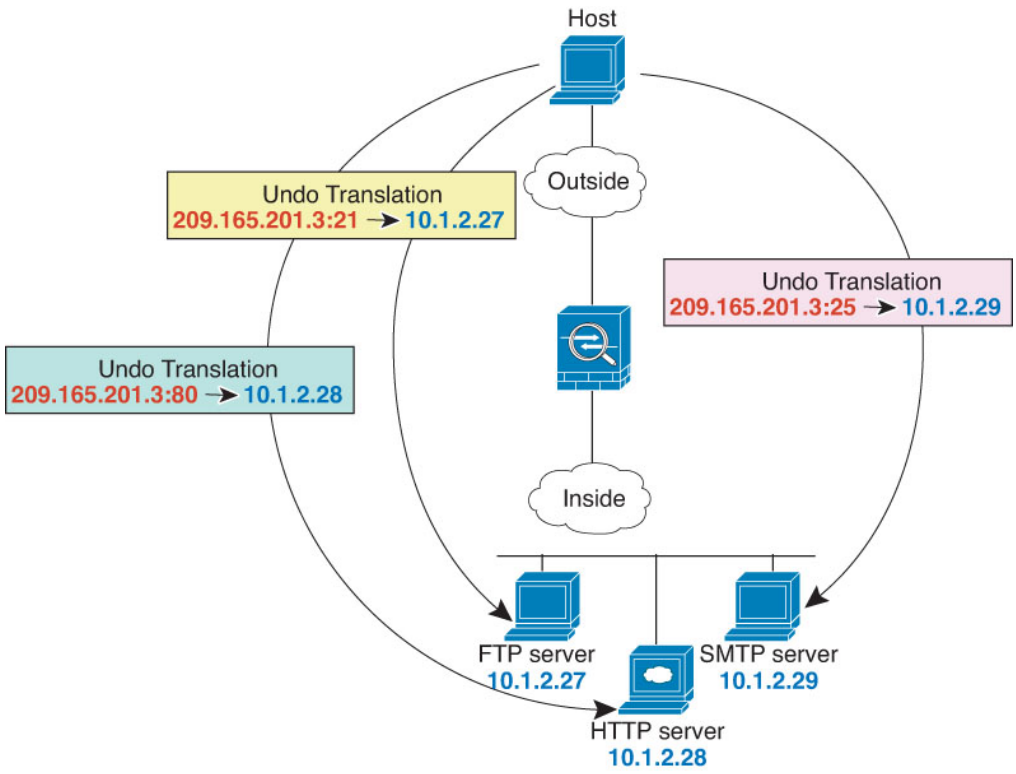
FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック自動 NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザーが FTP、HTTP、およびSMTPにアクセスするための単一のアドレスを提供します。これらのサーバーは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定

したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用できます。

（注） この例では、内部インターフェイスはスイッチに接続された標準ルーテッドインターフェイスで、スイッチにサーバーが接続されていると仮定します。内部インターフェイスがブリッジグループインターフェイス（BVI）であり、サーバーが別のブリッジグループメンバーインターフェイスに接続されている場合、各サーバーが対応するルールで接続する特定のメンバーインターフェイスを選択します。たとえば、ルールは「inside」ではなく、送信元インターフェイスの「inside1_2」、「inside1_3」、および「inside1_4」 の可能性があります。

図 *48*：ポート変換を設定したスタティック *NAT*



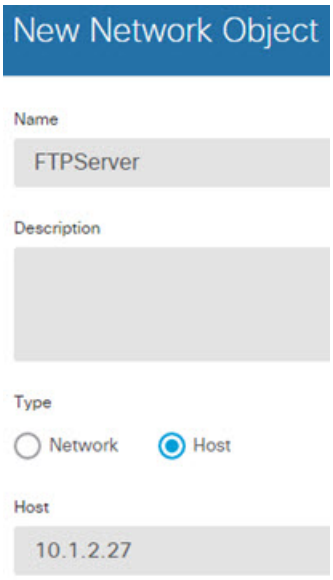
手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) ネットワーク オブジェクトに名前を付け（たとえば FTPserver）、[ホスト（Host）] を選択し、FTP サーバーの実際の IP アドレス（10.1.2.27）を入力します。

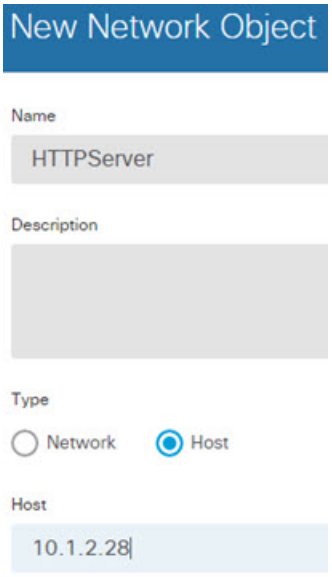


d) **[OK]** をクリックします。

ステップ 2 HTTP サーバのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえばHTTPserver）、[ホスト（Host）] を選択し、ホストアドレス（10.1.2.28）を入力します。

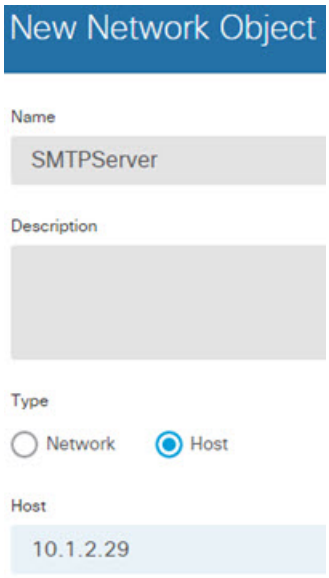


c) **[OK]** をクリックします。

ステップ 3 SMTP サーバのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえばSMTPserver）、[ホスト（Host）] を選択し、ホストアドレス（10.1.2.29）を入力します。

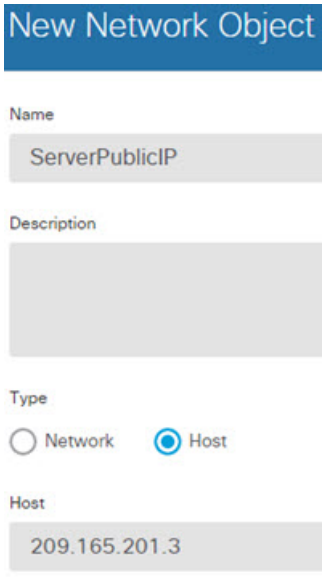


c) **[OK]** をクリックします。

ステップ 4 3 つのサーバに使用されるパブリック IP アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（たとえば ServerPublicIP）、[ホスト（Host）] を選択し、ホストアドレス（209.165.201.3）を入力します。



c) **[OK]** をクリックします。

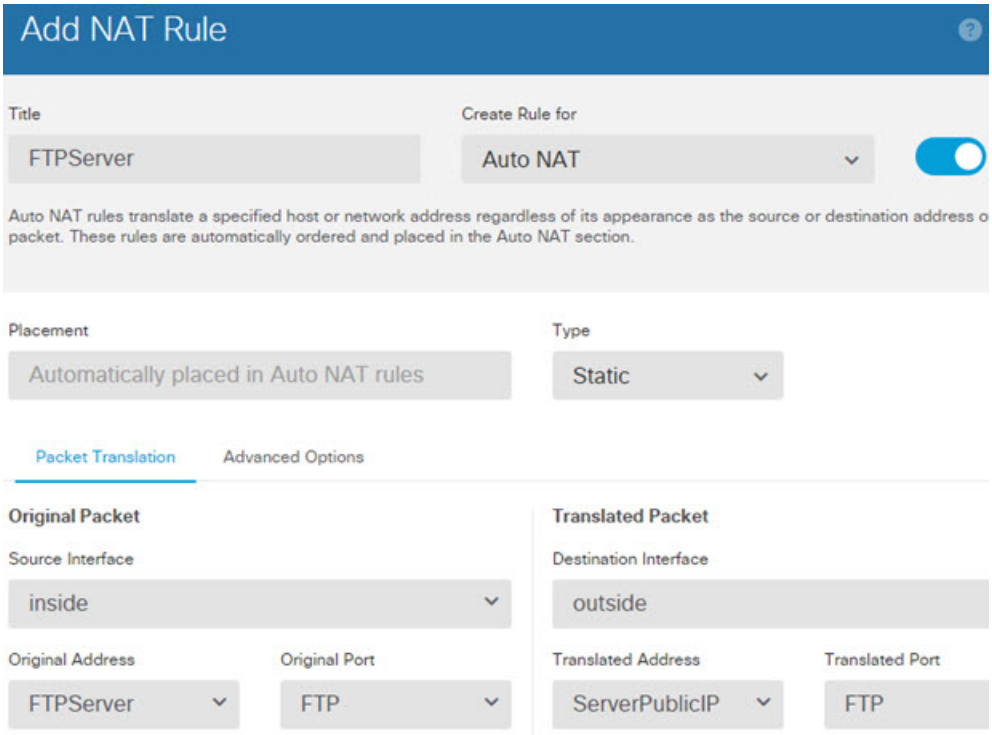
ステップ 5 FTP サーバーのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = FTPServer（または任意の別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）] = FTPServer ネットワーク オブジェクト（FTPserver network object）
- [変換済みアドレス（Translated Address）] = ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）。
- [元のポート（Original Port）] = FTP ポート オブジェクト（FTP port object）。
- [変換済みポート（Translated Port）] = FTP ポート オブジェクト（FTP port object）。



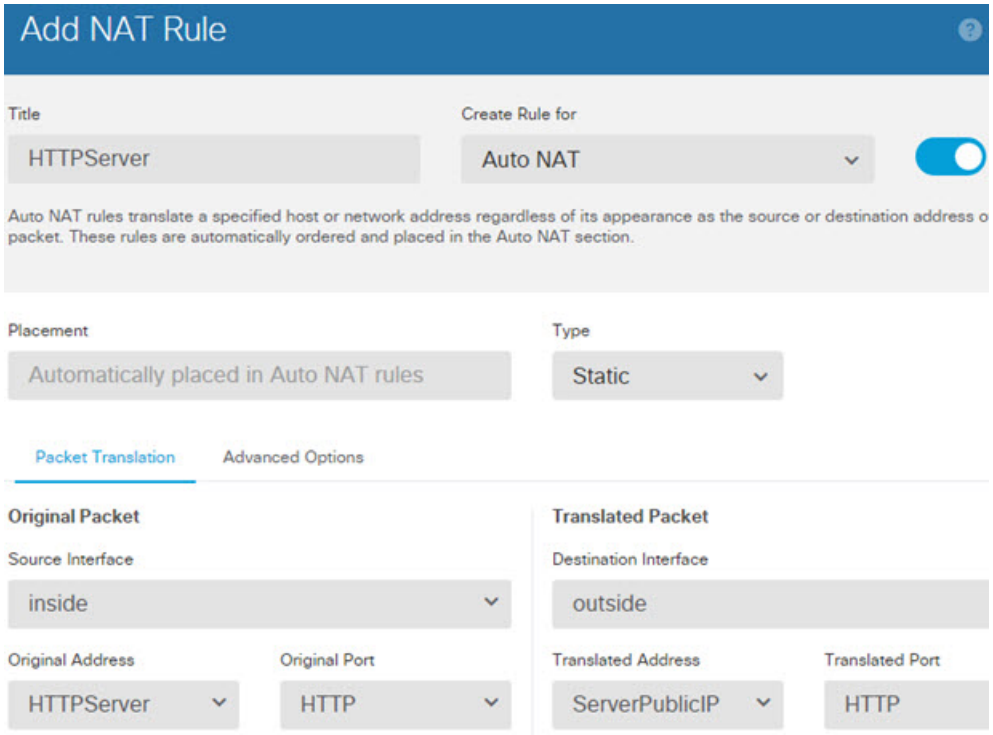
d) [OK] をクリックします。

ステップ 6 HTTP サーバーのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）] = HTTPServer（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）] = HTTPserver ネットワーク オブジェクト（HTTPserver network object）。
- [変換済みアドレス（Translated Address）] = ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）。
- [元のポート（Original Port）] = HTTP ポート オブジェクト（FTP port object）。
- [変換済みポート（Translated Port）] = HTTP ポート オブジェクト（HTTP port object）。



c) [OK] をクリックします。

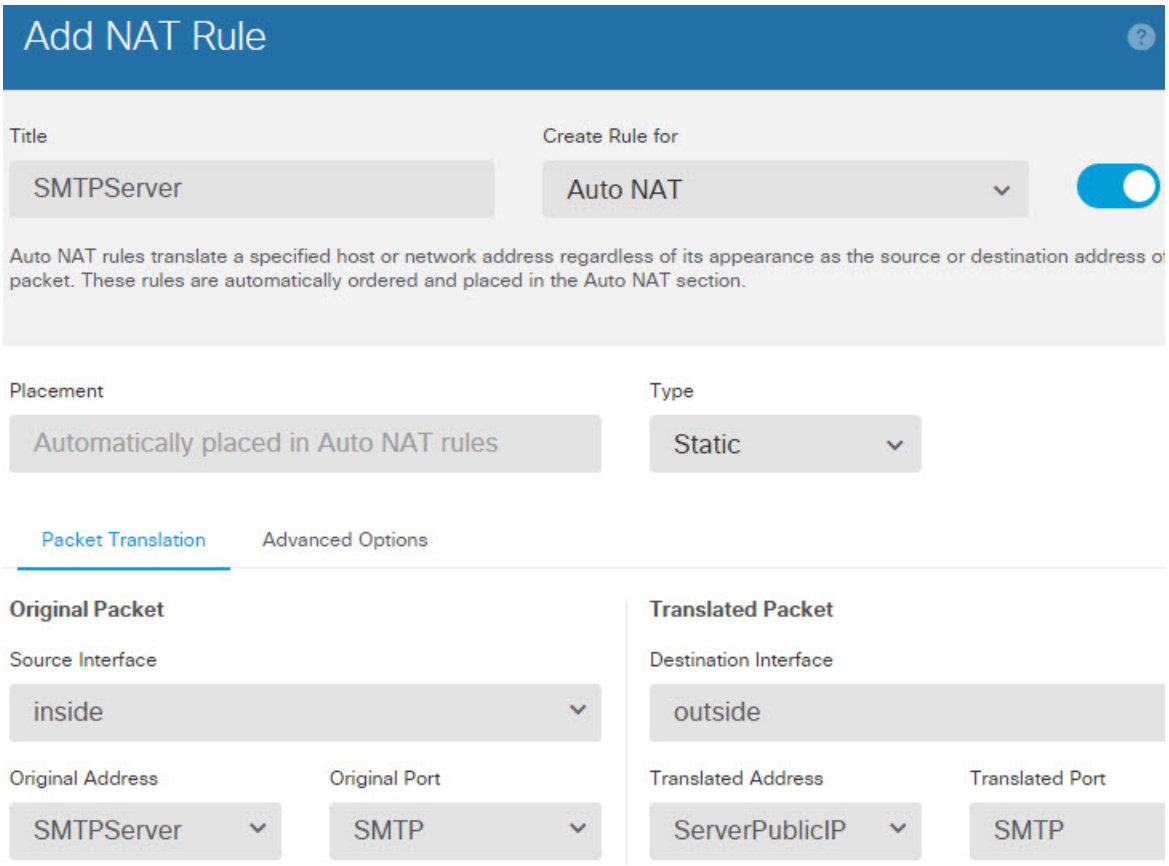
ステップ 7 SMTP サーバーのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）] = SMTPServer（または任意の別の名前）。

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）] = SMTPserver ネットワーク オブジェクト（SMTPserver network object）。
- [変換済みアドレス（Translated Address）] = ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）。
- [元のポート（Original Port）] = SMTP ポート オブジェクト（SMTP port object）。
- [変換済みポート（Translated Port）] = SMTP ポート オブジェクト（SMTP port object）。



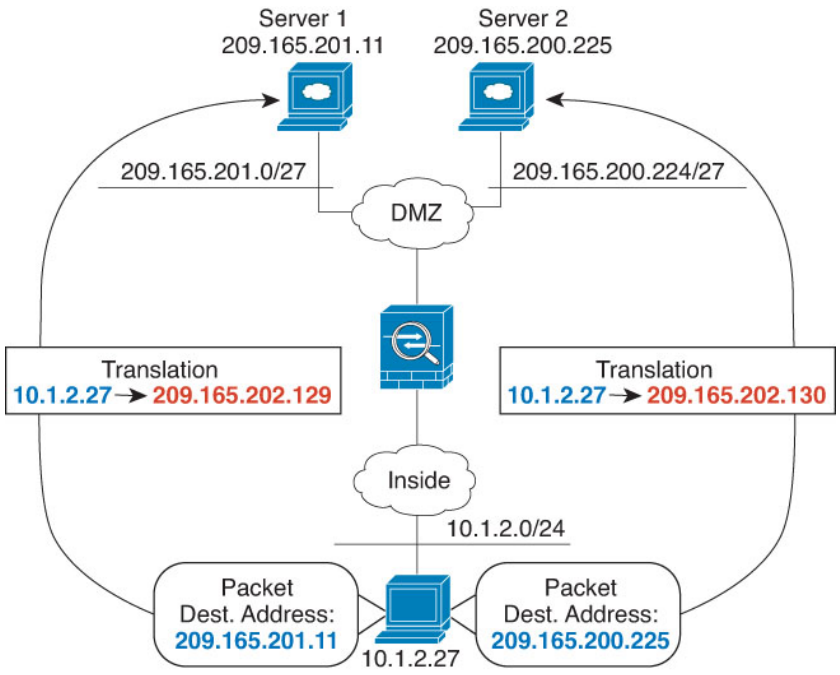
c) [OK] をクリックします。

宛先に応じて異なる変換（ダイナミック手動 PAT）

次の図に、2 台の異なるサーバーにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

（注） この例では、内部インターフェイスはスイッチに接続された標準ルーテッドインターフェイスで、スイッチにサーバーが接続されていると仮定します。内部インターフェイスがブリッジグループインターフェイス（BVI）であり、サーバーが別のブリッジグループ メンバーインターフェイスに接続されている場合、各サーバーが対応するルールで接続する特定のメンバーインターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの inside1_2 および inside1_3 を持つ場合があります。

図 *49 :* 異なる宛先アドレスを使用する手動 *NAT*



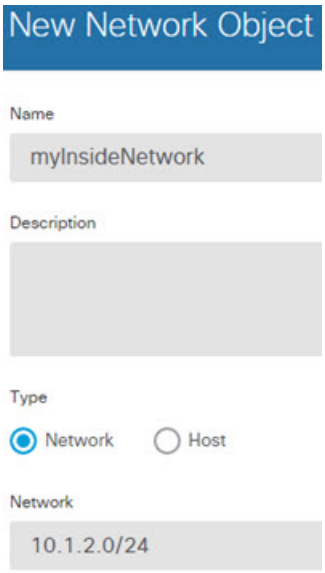
手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、[ネットワーク（Network）] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

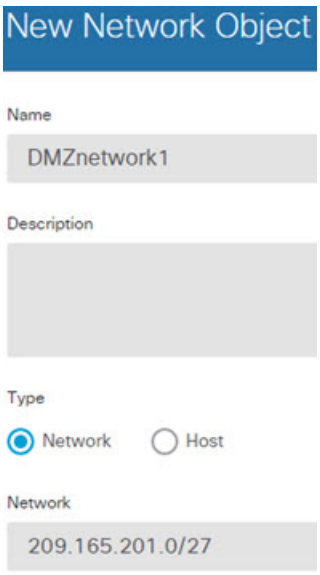


d) **[OK]** をクリックします。

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork1 など）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 209.165.201.0/27 を入力します（255.255.255.224 のサブネット マスク）。

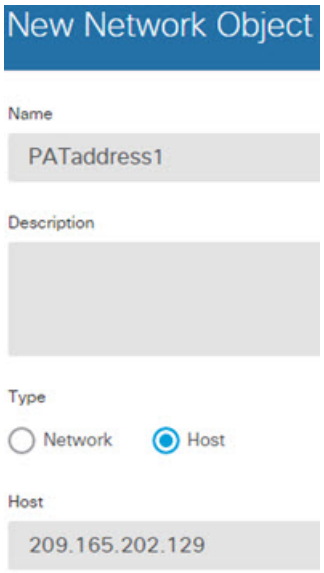


c) **[OK]** をクリックします。

ステップ 3 DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.202.129 を入力します。

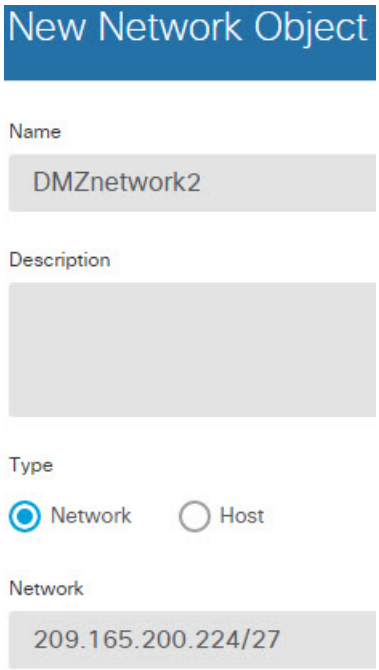


c) **[OK]** をクリックします。

ステップ 4 DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork2 など）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 209.165.200.224/27 を入力します（255.255.255.224 のサブネット マスク）。

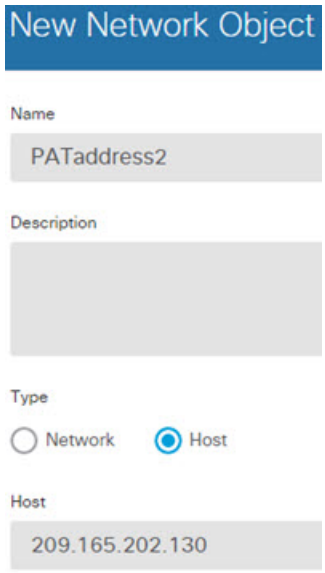


c) **[OK]** をクリックします。

ステップ 5 DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.202.130 を入力します。



c) **[OK]** をクリックします。

ステップ 6 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

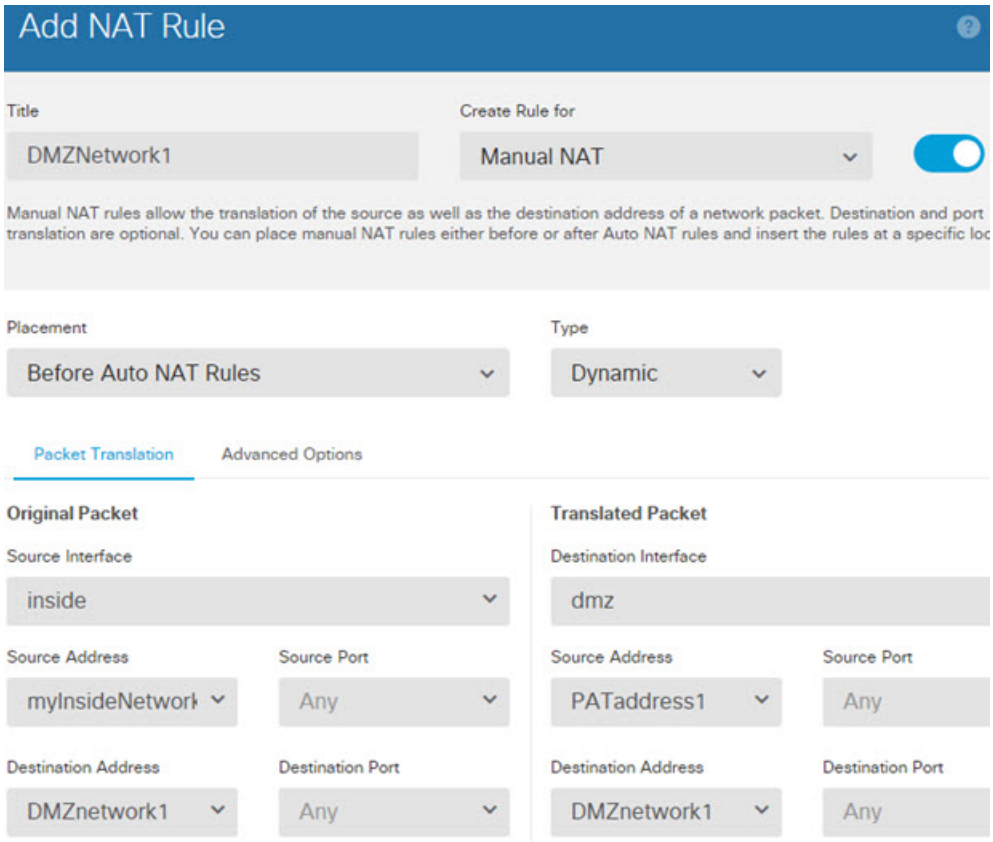
b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = DMZNetwork1（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = 手動 NAT（Manual NAT）。
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = dmz。
- [元の発信元アドレス（Original Source Address）] = myInsideNetwork のネットワーク オブジェクト（myInsideNetwork network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress1 のネットワーク オブジェクト（PATaddress1 network object）。
- [元の宛先アドレス（Original Destination Address）] = DMZnetwork1 のネットワーク オブジェクト（DMZnetwork1 network object）。

- [変換済みの宛先アドレス（Translated Destination Address）] = DMZnetwork1 のネットワーク オブジェクト（DMZnetwork1 network object）。

（注） 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート（Port）] フィールドはすべて空白のままにします。



d) [OK] をクリックします。

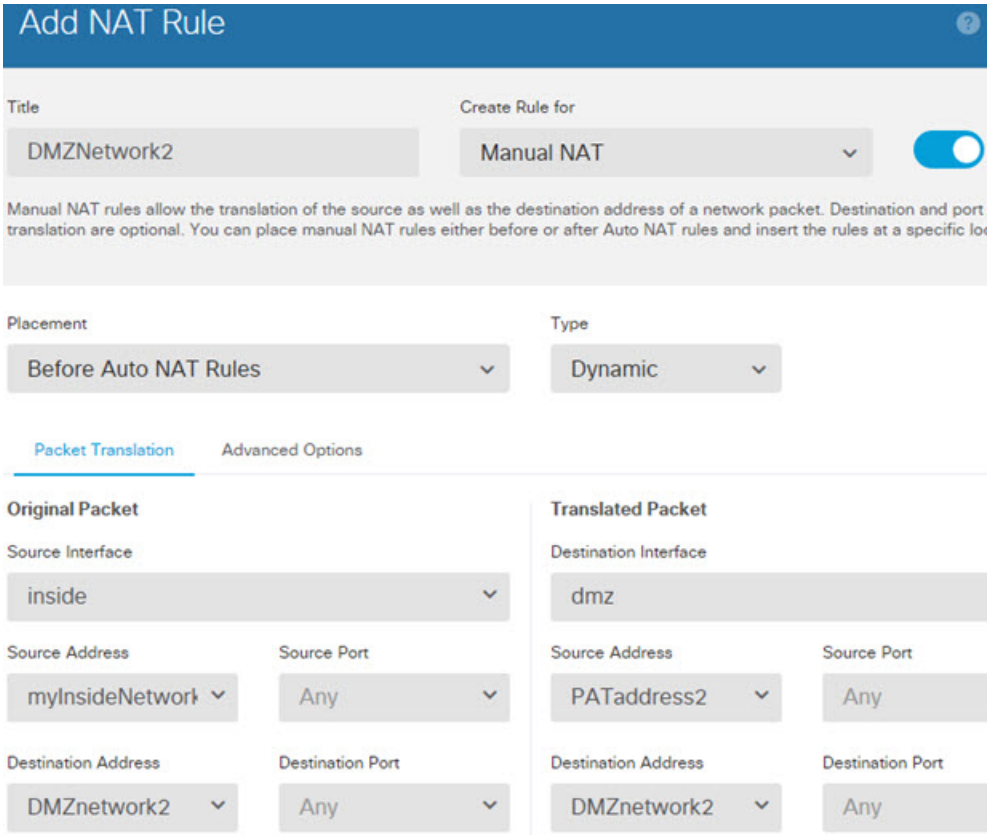
ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- タイトル（Title） = DMZNetwork2（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = 手動 NAT（Manual NAT）。
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = dmz。

- [元の発信元アドレス（Original Source Address）] = myInsideNetwork のネットワーク オブジェクト（myInsideNetwork network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress2 のネットワーク オブジェクト（PATaddress2 network object）。
- [元の宛先アドレス（Original Destination Address）] = DMZnetwork2 のネットワーク オブジェクト（DMZnetwork2 network object）。
- [変換済みの宛先アドレス（Translated Destination Address）] = DMZnetwork2 のネットワーク オブジェクト（DMZnetwork2 network object）。



c) [OK] をクリックします。

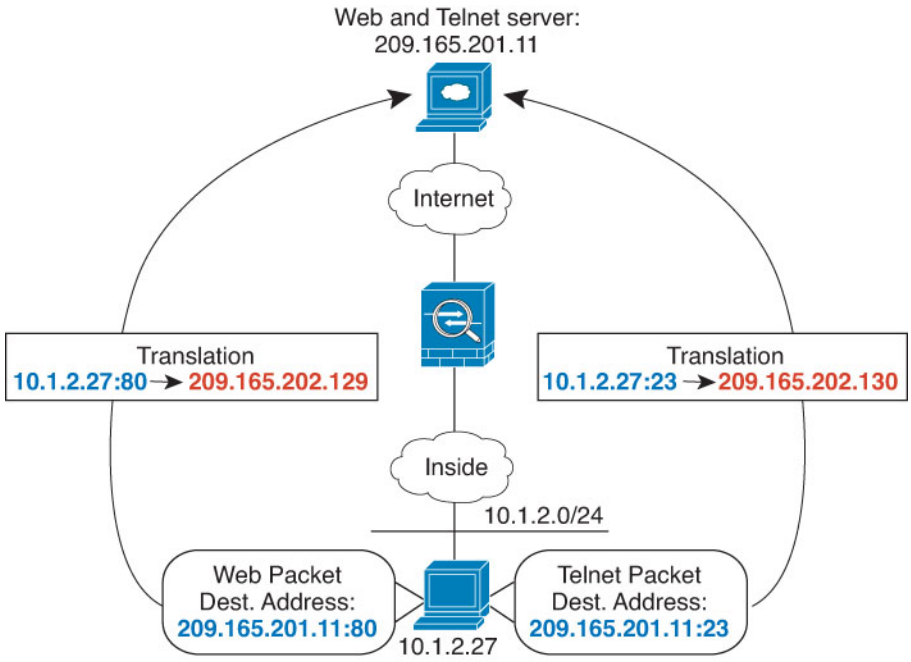
宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバーにアクセスすると、実際のアドレスは 209.165.202.129:

ポートに変換されます。ホストが Web サービスを求めて同じサーバーにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

（注） この例では、内部インターフェイスがスイッチに接続され、サーバーがスイッチに接続されている標準ルーテッドインターフェイスであると仮定します。内部インターフェイスがブリッジ グループ インターフェイス（BVI）であり、サーバーがブリッジ グループ メンバー インターフェイスに接続されている場合、サーバーが接続されている特定のメンバーインターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの inside1_2 を持つ場合があります。

図 *50* : 異なる宛先ポートを使用する手動 *NAT*



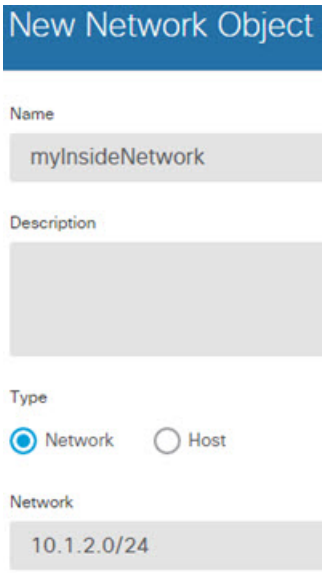
手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、[ネットワーク（Network）] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

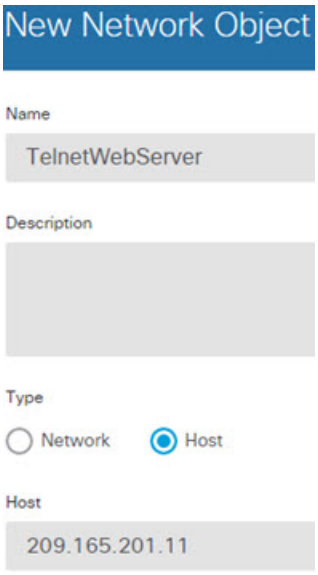


d) **[OK]** をクリックします。

ステップ 2 Telnet/Web サーバのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（TelnetWebServer など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.201.11 を入力します。

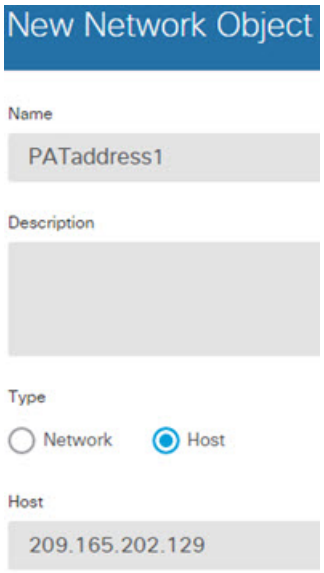


c) **[OK]** をクリックします。

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.202.129 を入力します。

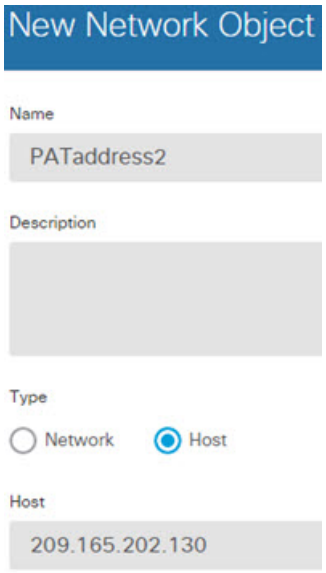


c) **[OK]** をクリックします。

ステップ 4 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) [+] をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.202.130 を入力します。



c) **[OK]** をクリックします。

ステップ 5 Telnet アクセスのダイナミック手動 PAT を設定します。

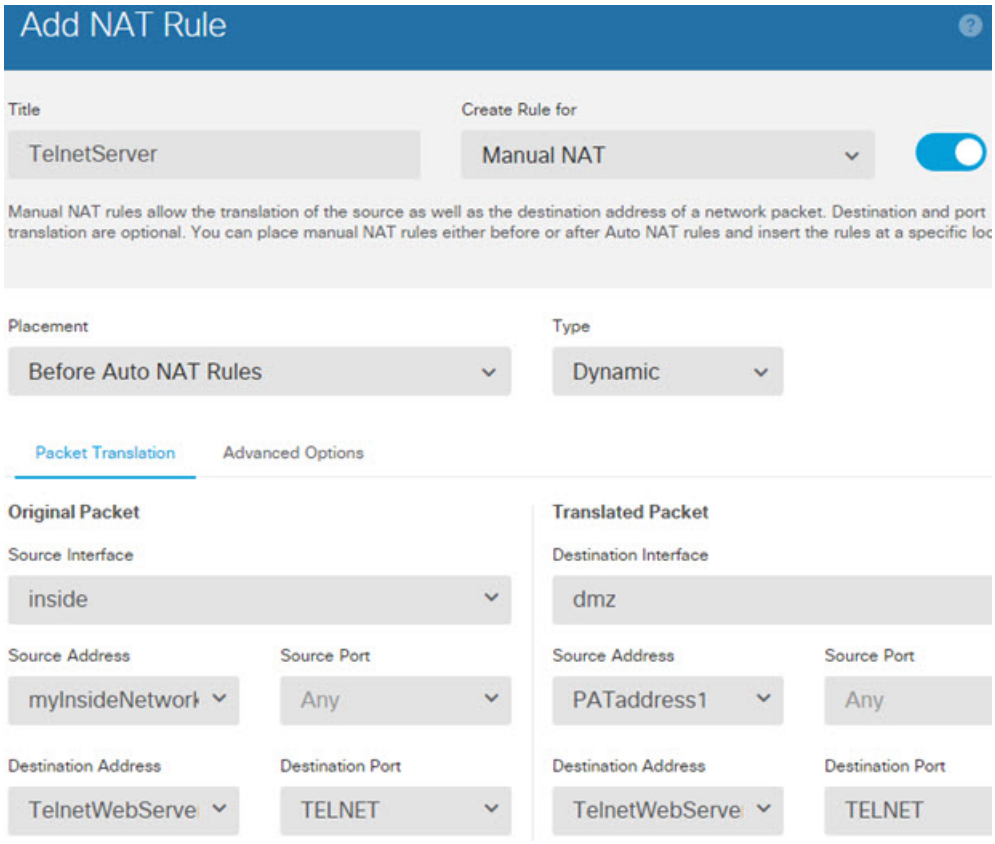
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = TelnetServer（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = 手動 NAT（Manual NAT）。
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = dmz。
- [元の発信元アドレス（Original Source Address）] = myInsideNetwork のネットワーク オブジェクト（myInsideNetwork network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress1 のネットワーク オブジェクト（PATaddress1 network object）。
- [元の宛先アドレス（Original Destination Address）] = TelnetWebServer のネットワーク オブジェクト（TelnetWebServer network object）。
- [変換済みの宛先アドレス（Translated Destination Address）] = TelnetWebServer のネットワーク オブジェクト（TelnetWebServer network object）。
- [元の宛先ポート（Original Destination Port）] = TELNET ポート オブジェクト（TELNET port object）。
- [変換済みの宛先ポート（Translated Destination Port）] = TELNET ポート オブジェクト（TELNET port object）。

（注） 宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。



d) [OK] をクリックします。

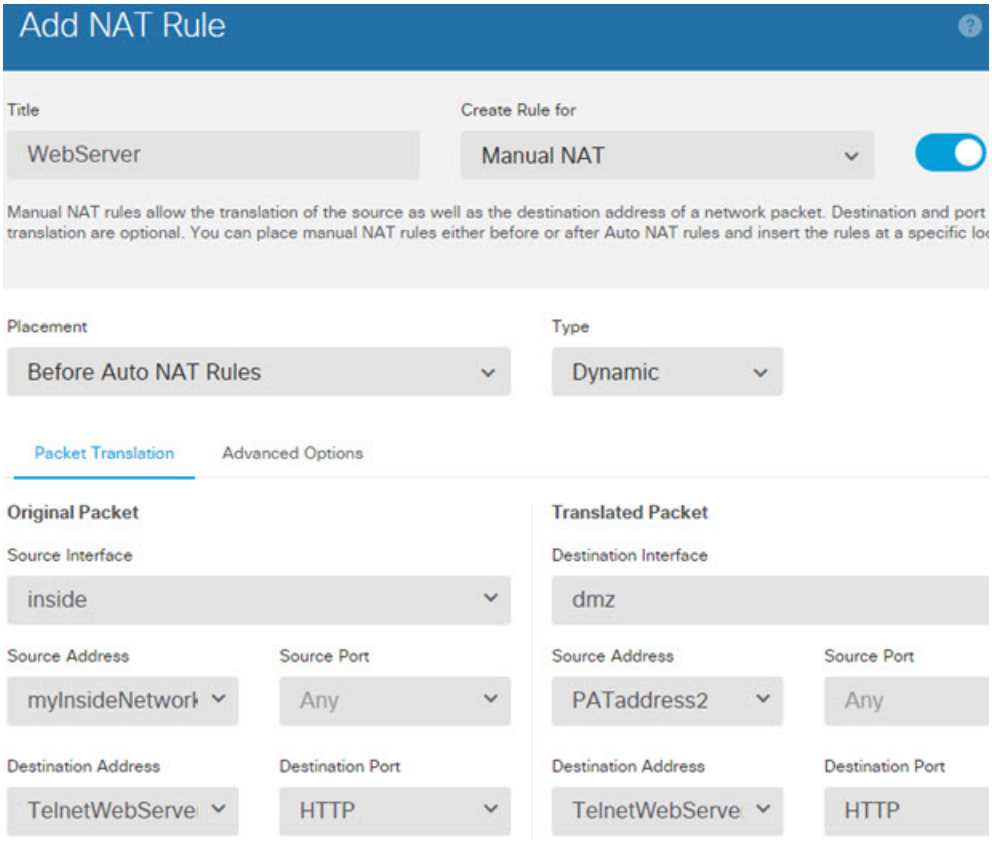
ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）] = WebServer（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = 手動 NAT（Manual NAT）。
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = dmz。
- [元の発信元アドレス（Original Source Address）] = myInsideNetwork のネットワーク オブジェクト（myInsideNetwork network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress2 のネットワーク オブジェクト（PATaddress2 network object）。
- [元の宛先アドレス（Original Destination Address）] = TelnetWebServer のネットワーク オブジェクト（TelnetWebServer network object）。

- [変換済みの宛先アドレス（Translated Destination Address）] = TelnetWebServer のネットワーク オブジェクト（TelnetWebServer network object）。
- [元の宛先ポート（Original Destination Port）] = HTTP ポート オブジェクト（HTTP port object）。
- [変換済みの宛先ポート（Translated Destination Port）] = HTTP ポート オブジェクト（HTTP port object）。



c) [OK] をクリックします。

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT 設定と一致するアドレスに置き換えて、DNS 応答を修正するように Threat Defense デバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーション ルールを設定するときに設定できます。DNS 修正は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A

レコードはマップされた値から実際の値へ書き換えられます。逆に、任意のインターフェイスからマッピン インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。この機能は、NAT44、NAT66、 NAT46、および NAT64 と連動します。

以下に、NAT ルールで DNS の書き換えを設定する必要が生じる主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード（IPv4 用）と AAAA レコード（IPv6 用）を変換するために DNS の書き換えが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS の書き換えの制限事項

次に DNS の書き換えの制限事項を示します。

- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS の書き換えは PAT には適用されません。
- 手動 NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- 実際には、DNS の書き換えは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、書き換えが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ（オペレーション コード 5）は書き換えられません。

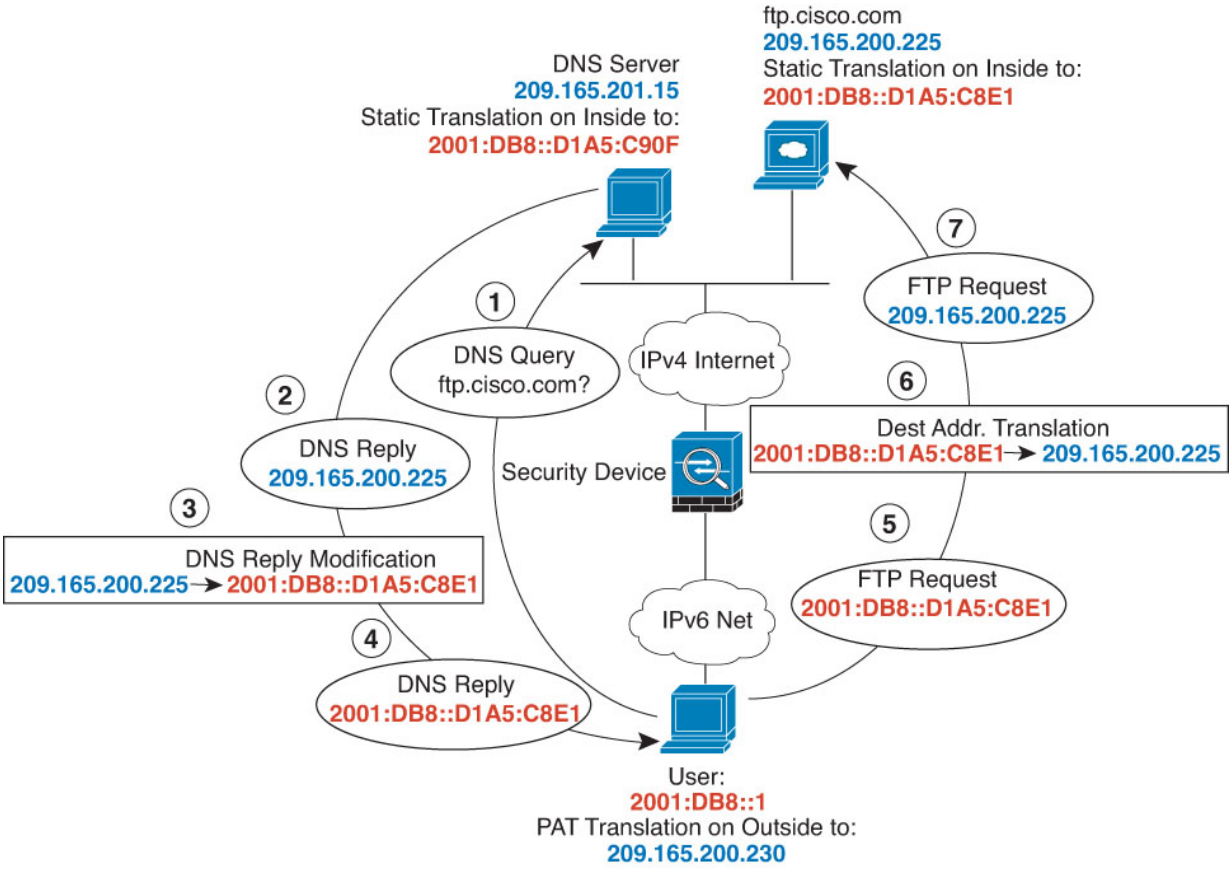
次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

DNS 64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザーが ftp.cisco.com のアドレスを DNS サーバーに要求すると、DNS サーバーは実際のアドレス（209.165.200.225）を応答します。

内部ユーザーに ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1：D1A5:C8E1 は IPv6 の 209.165.200.225 に相当）を使用させるには、スタティック変換用の DNS 応答修正を設

定する必要があります。この例には、DNS サーバーのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



（注） この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

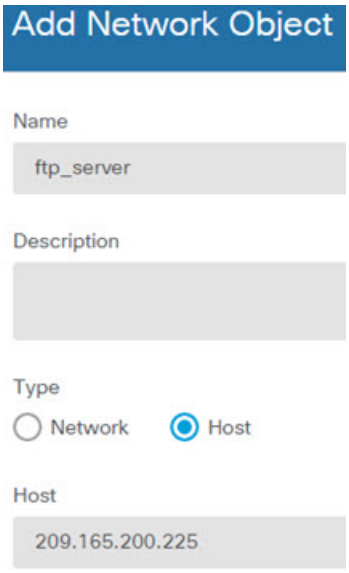
ステップ 1 FTP サーバー、DNS サーバー、内部ネットワーク、および PAT プールのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) 実際の FTP サーバ アドレスを定義します。

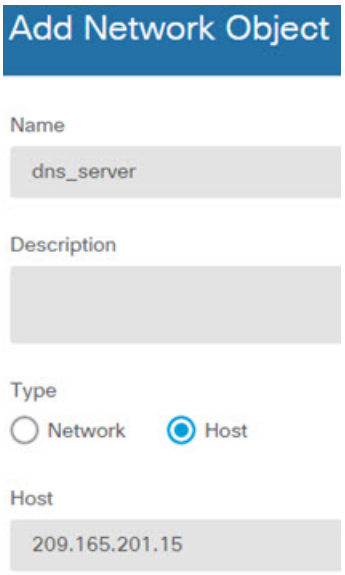
ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）] を選択して、実際のホストの IP アドレス 209.165.200.225 を入力します。



d) **[OK]** をクリックします。

e) [+] をクリックして DNS サーバーの実際のアドレスを定義します。

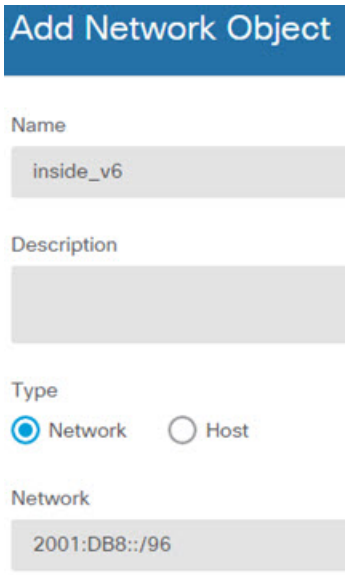
ネットワーク オブジェクトに名前を付け（dns_server など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.201.15 を入力します。



f) **[OK]** をクリックします。

g) [+] をクリックして内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前を付け（inside_v6 など）、[ネットワーク（Network）] を選択して、ネットワーク アドレス 2001:DB8::/96 を入力します。



h) **[OK]** をクリックします。

i) [+] をクリックして内部 IPv6 ネットワークの IPv4 PAT アドレスを定義します。

ネットワーク オブジェクトに名前を付け（ipv4_pat など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.200.230 を入力します。

j) **[OK]** をクリックします。

ステップ 2 FTP サーバーのための、DNS 修正を設定したスタティック NAT ルールを設定します。

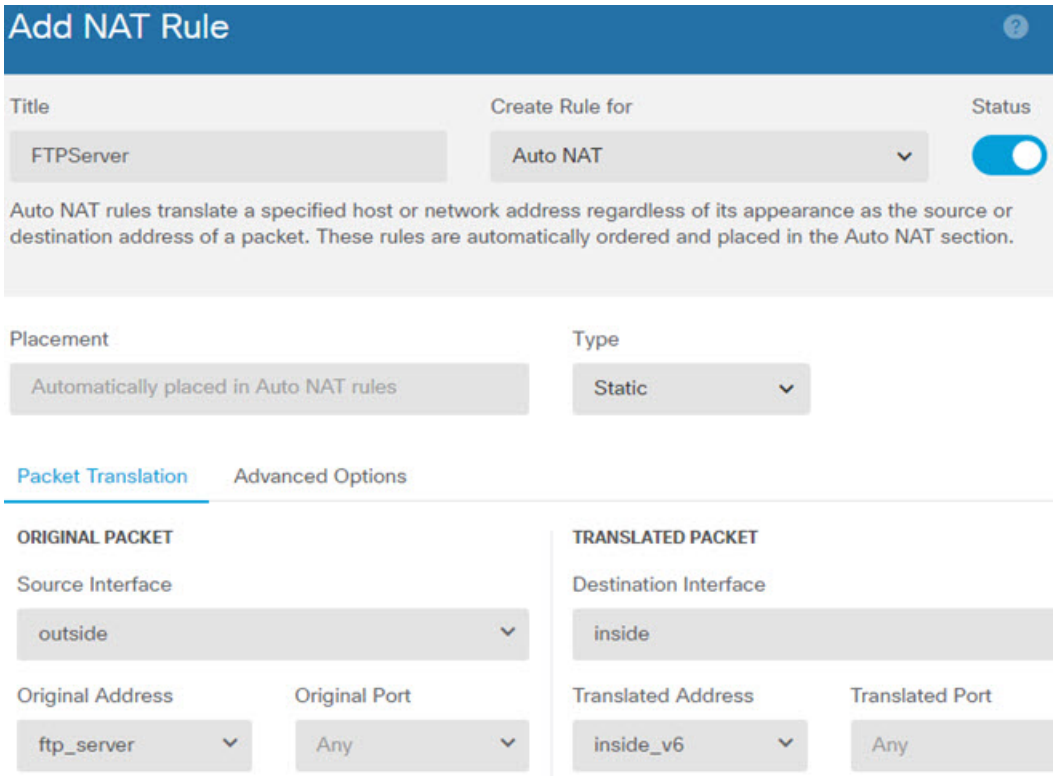
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = FTPServer（または任意の別の名前）

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = [外部（outside）]
- [宛先インターフェイス（Destination Interface）] = [内部（inside）]
- [元のアドレス（Original Address）] = ftp_server のネットワーク オブジェクト（ftp_server network object）。
- [変換済みアドレス（Translated Address）] = inside_v6 ネットワーク オブジェクト（inside_v6 network object）IPv4 アドレスを IPv6 アドレスに変換する場合、IPv4 組み込みアドレス方式が使用されているため、209.165.200.225 は IPv6 で対応する D1A5:C8E1 に変換され、ネットワーク プレフィックスが追加されて完全なアドレス 2001:DB8::D1A5:C8E1 となります。
- [詳細オプション（Advanced Options）] タブで、[このルールに一致するDNS応答を変換する（Translate DNS replies that match this rule）] を選択します。



d) [OK] をクリックします。

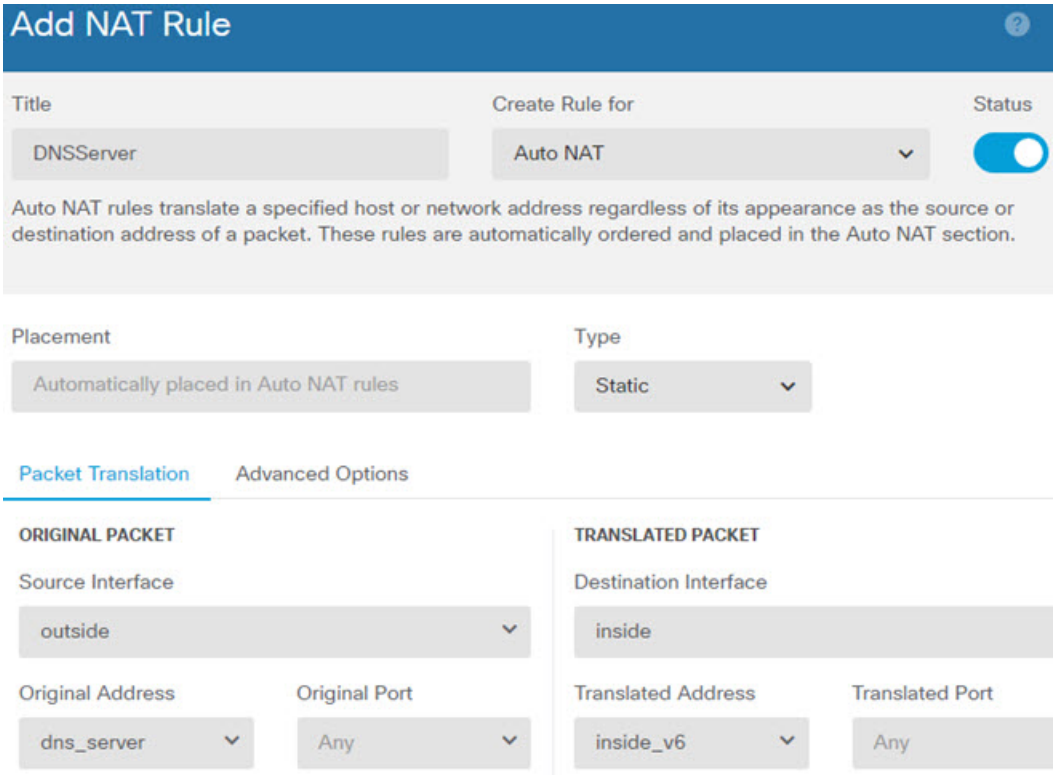
ステップ 3 DNS サーバーのためのスタティック NAT ルールを設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = DNSServer（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = [外部（outside）]
- [宛先インターフェイス（Destination Interface）] = [内部（inside）]
- [元のアドレス（Original Address）] = dns_server のネットワーク オブジェクト（dns_server network object.）。
- [変換済みアドレス（Translated Address）] = inside_v6 ネットワーク オブジェクト（inside_v6 network object）IPv4 アドレスを IPv6 アドレスに変換する場合、IPv4 組み込みアドレス方式が使用されているため、209.165.201.15 は IPv6 で対応する D1A5:C90F に変換され、ネットワーク プレフィックスが追加されて完全なアドレス 2001:DB8::D1A5:C90F となります。

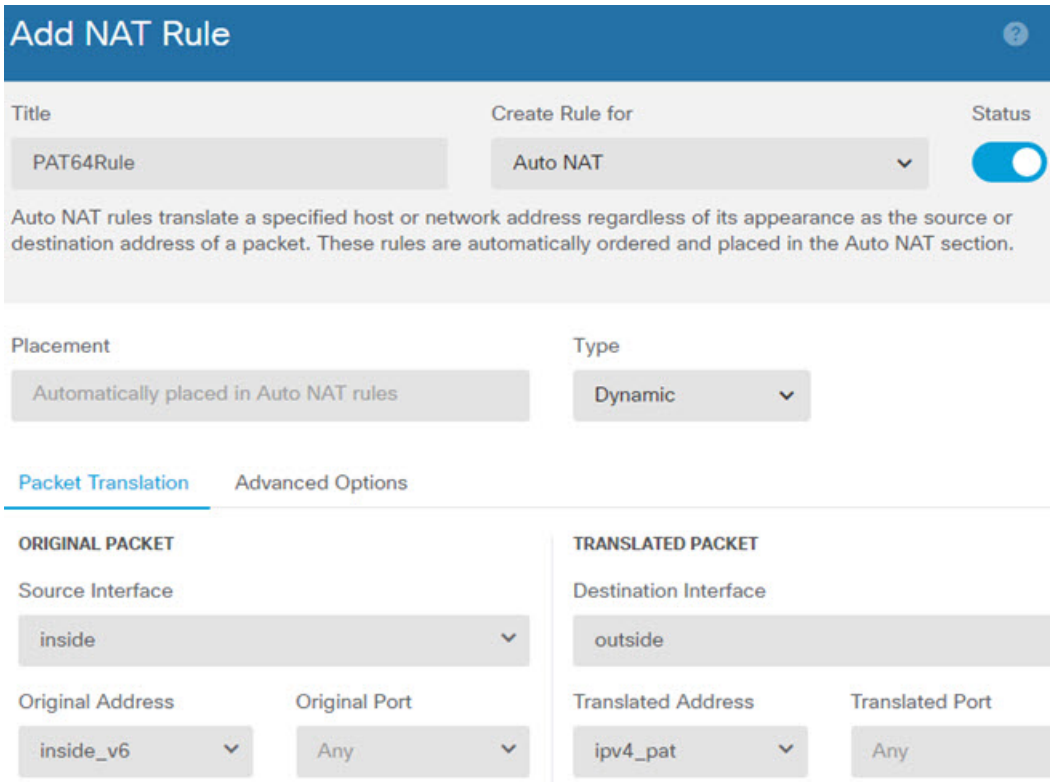


d) [OK] をクリックします。

ステップ 4 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。
b) [+] ボタンをクリックします。
c) 次のプロパティを設定します。

- [タイトル（Title）] = PAT64Rule（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）]：inside_v6 ネットワーク オブジェクト（inside_v6 network object）
- [変換済みのアドレス（Translated Address）] = ipv4_pat のネットワーク オブジェクト（ipv4_pat network object）。



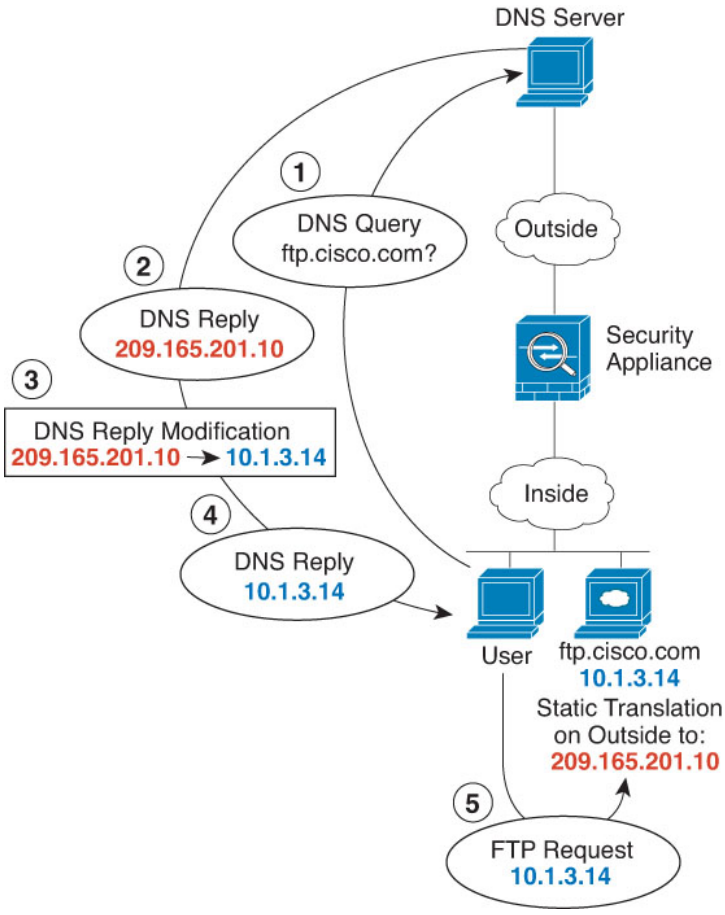
d) [OK] をクリックします。

DNS 応答修正：外部の DNS サーバー

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で確認できるマッピング アドレス（209.165.201.10）にスタティックに変換するように NAT を設定します。

この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザーは、マッピングアドレスではなく実際のアドレスを DNS サーバーから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバーはマッピングアドレス（209.165.201.10）を応答します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



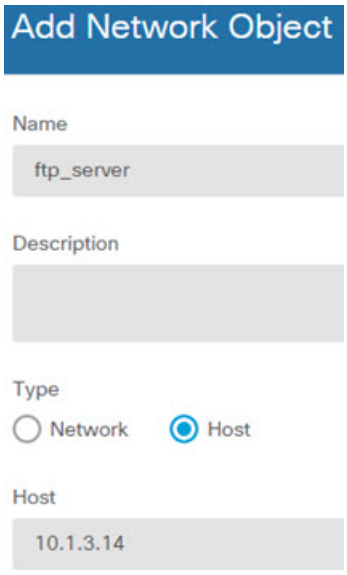
（注） この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッド インターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

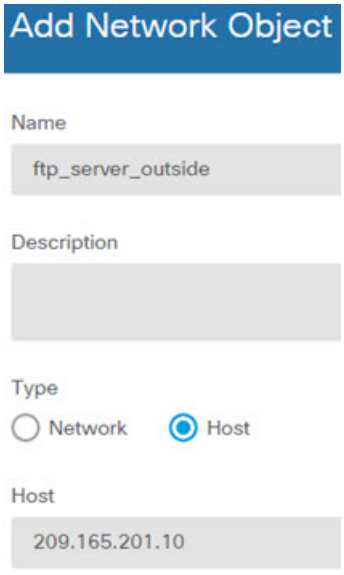
a) [オブジェクト（Objects）] を選択します。
b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 実際の FTP サーバ アドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）] を選択して、実際のホストの IP アドレス 10.1.3.14 を入力します。



d) **[OK]** をクリックします。
e) [+] をクリックして FTP サーバーの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server_outside など）、[ホスト（Host）] を選択して、ホスト アドレス 209.165.201.10 を入力します。



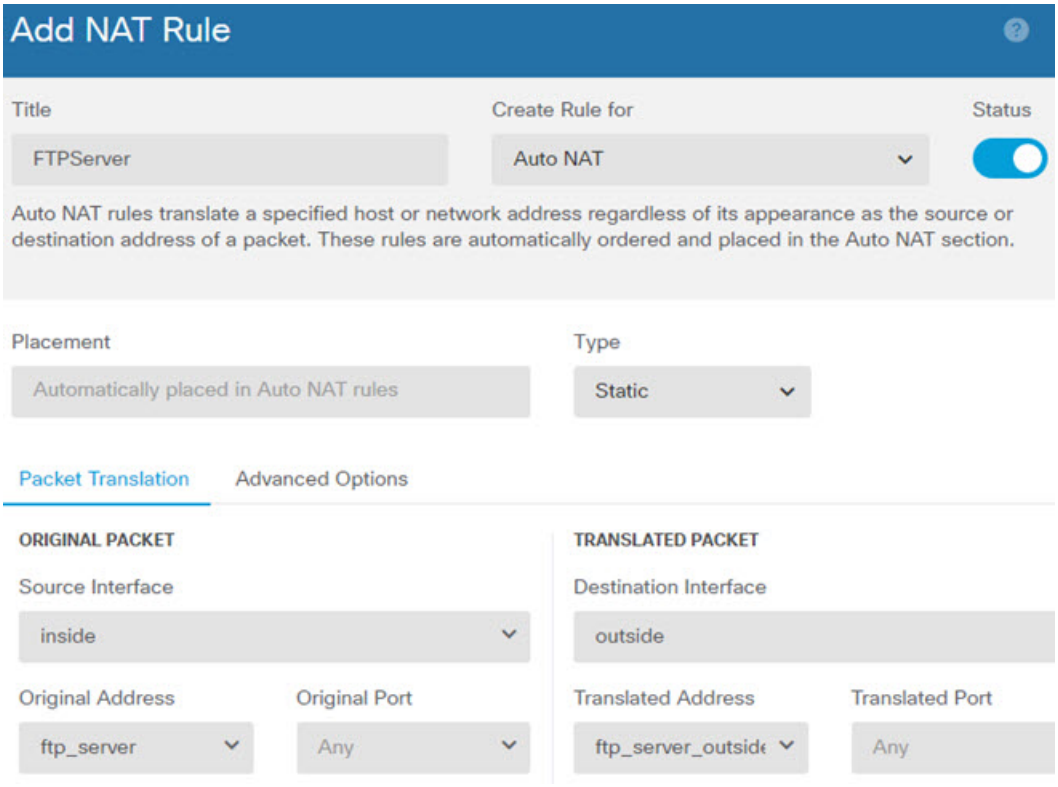
ステップ 2 FTP サーバーのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

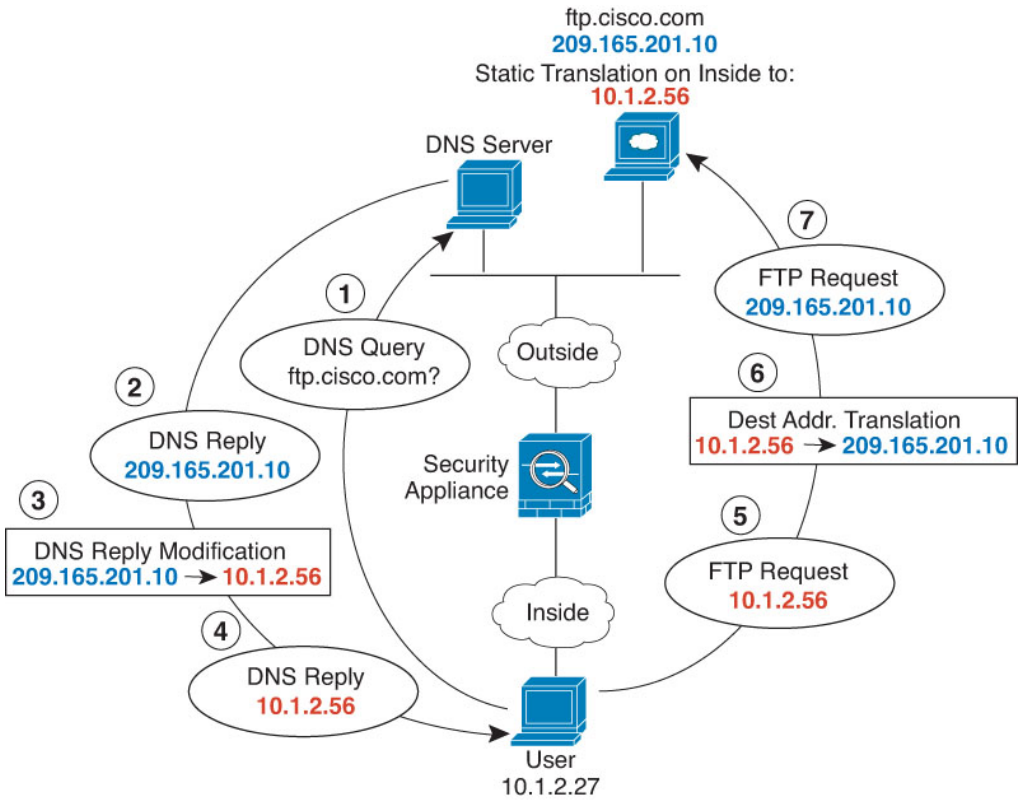
- [タイトル（Title）] = FTPServer（または任意の別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = 内部（inside）。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元のアドレス（Original Address）] = ftp_server のネットワーク オブジェクト（ftp_server network object）。
- [変換済みアドレス（Translated Address）] = ftp_server_outside のネットワーク オブジェクト（ftp_server_outside network object）。
- [詳細オプション（Advanced Options）] タブで、[このルールに一致するDNS応答を変換する（Translate DNS replies that match this rule）] を選択します。



d) [OK] をクリックします。

DNS 応答修正：ホスト ネットワーク上の DNS サーバー

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部ユーザーが ftp.cisco.com のアドレスを DNS サーバーに要求すると、DNS サーバーは実際のアドレス（209.165.20.10）を応答します。内部ユーザに ftp.cisco.com のマッピング アドレス（10.1.2.56）を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



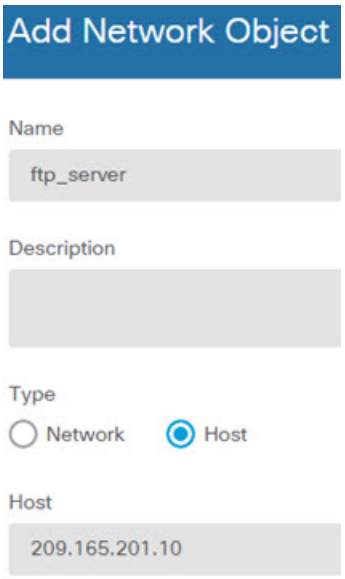
（注） この例は、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準のルーテッド インターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。
b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 実際の FTP サーバ アドレスを定義します。

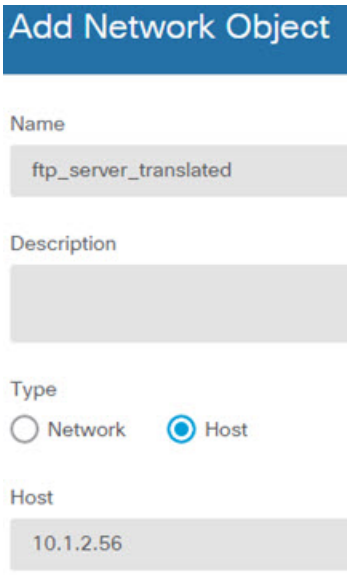
ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）] を選択して、実際のホストの IP アドレス 209.165.201.10 を入力します。



d) **[OK]** をクリックします。

e) [+] をクリックして FTP サーバーの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け（ftp_server_translated など）、[ホスト（Host）] を選択して、ホスト アドレス 10.1.2.56 を入力します。



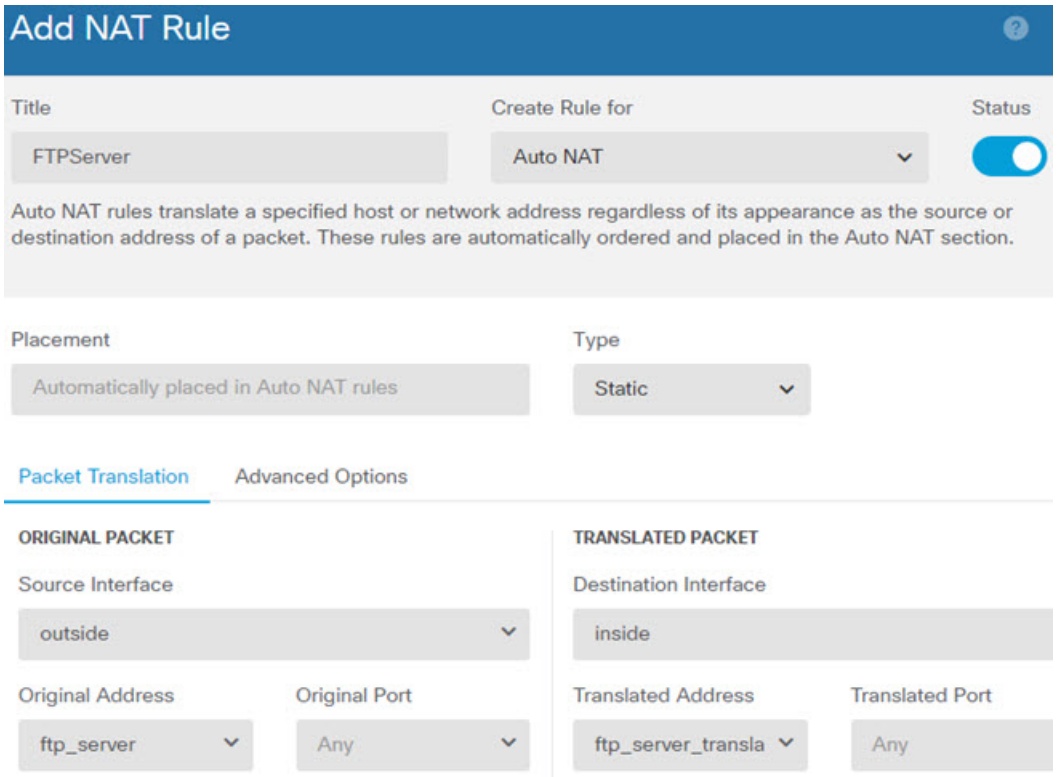
ステップ 2 FTP サーバーのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

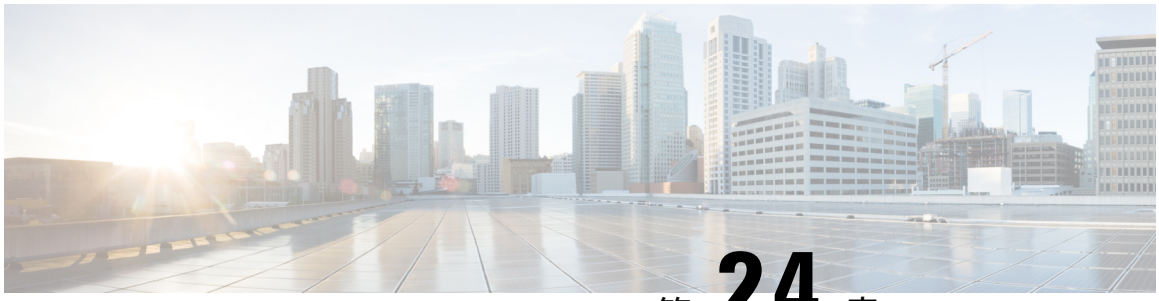
- [タイトル（Title）] = FTPServer（または任意の別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = [外部（outside）]
- [宛先インターフェイス（Destination Interface）] = [内部（inside）]
- [元のアドレス（Original Address）] = ftp_server のネットワーク オブジェクト（ftp_server network object）。
- [変換済みアドレス（Translated Address）] = ftp_server_translated のネットワーク オブジェクト。
- [詳細オプション（Advanced Options）] タブで、[このルールに一致するDNS応答を変換する（Translate DNS replies that match this rule）] を選択します。



d) [OK] をクリックします。

第 VI 部

バーチャル プライベート ネットワーク（VPN）



第 24 章

サイト間 VPN

バーチャル プライベート ネットワーク（VPN）は、パブリック ソース（インターネットやその他のネットワークなど）を使用して、リモート ピア間でセキュアなトンネルを確立するネットワーク接続です。VPN ではトンネルを使用して通常の IP パケット内のデータ パケットがカプセル化され、IP ベースのネットワークを介して転送されます。VPN ではプライバシーの確保と認証のために暗号化が使用され、データの整合性が確保されます。

VPN の基本

トンネリングによって、インターネットなどのパブリック TCP/IP ネットワークの使用が可能となり、リモートユーザとプライベート企業ネットワークとの間でセキュアな接続を作成できます。各セキュアな接続がトンネルと呼ばれます。

IPsec ベースの VPN テクノロジーでは、Internet Security Association and Key Management Protocol（ISAKMP または IKE）と IPsec トンネリングを使用して、トンネルを構築し管理します。ISAKMP と IPsec は、次を実現します。

- トンネル パラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。
- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル エンドポイントとして機能します。プライベート ネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリック ネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

サイト間 VPN 接続が確立された後、ローカル ゲートウェイの背後にあるホストは、セキュアなVPNトンネルを介してリモートゲートウェイの背後にあるホストと接続できます。接続は、2つのゲートウェイのIPアドレスとホスト名、それらの背後にあるサブネット、および2つのゲートウェイが互いを認証するために使用する方式で構成されます。

インターネット キー エクスチェンジ（IKE）

インターネット キー エクスチェンジ（IKE）は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション（SA）を自動的に確立するために使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ2で安全に通信できるようになります。フェーズ2のネゴシエーションでは、IKEによってIPsecなどの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE ポリシーは、2 つのピアが、ピア間の IKE ネゴシエーションの安全性を確保するために使用する一連のアルゴリズムです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、どのセキュリティ パラメータが後続の IKE ネゴシエーションを保護するかを規定します。IKE バージョン 1（IKEv1）の場合、IKE ポリシーには単一セットのアルゴリズムとモジュラスグループが含まれます。IKEv1 とは異なり、IKEv2 ポリシーでは、フェーズ 1 ネゴシエーション中にピアがその中から選択できるように、複数のアルゴリズムとモジュラス グループを選択できます。単一の IKE ポリシーを作成できますが、最も必要なオプションにより高い優先順位をつけるために異なるポリシーが必要となる場合もあります。サイト間 VPN の場合は、単一の IKE ポリシーを作成できます。

IKE ポリシーを定義するには、次を指定します。

- 固有の優先順位（1 ～ 65,543、1 が最高の優先順位）。
- データを保護し、プライバシーを確保するための IKE ネゴシエーションの暗号化方式。
- 送信者の ID を保証し、メッセージが伝送中に変更されないように確保するためのハッシュ メッセージ認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれる）。
- IKEv2 の場合、IKEv2 トンネル暗号化に必要なキーの材料とハッシュ操作を派生させるためのアルゴリズムとして使用される個別の擬似乱関数（PRF）。オプションは、ハッシュ アルゴリズムで使用されているものと同じです。
- 暗号化キー判別アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュ キーを派生させます。
- ピアの ID を保証するための認証方式。

• デバイスが暗号化キーを交換するまでに使用できる時間制限。

IKE ネゴシエーションが開始すると、ネゴシエーションを開始するピアはリモート ピアに有効なポリシーをすべて送信し、リモート ピアは優先順位順に自身のポリシーとの一致を検索します。ピアが、暗号化、ハッシュ（IKEv2 の場合は整合性と PRF）、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが同じでない場合は、リモート ピアから取得した短い方のライフタイムが適用されます。デフォルトでは、DES を使用するシンプルな IKE ポリシーが唯一有効なポリシーです。より高い優先順位のその他の IKE ポリシーによってより強力な暗号化標準をネゴシエートできますが、DES ポリシーでも正常なネゴシエーションが確保されます。

VPN 接続の安全性を確保する方法

VPN トンネルは通常、インターネットなどのパブリック ネットワークを経由するため、トラフィックを保護するために接続を暗号化する必要があります。IKE ポリシーと IPsec プロポーサルを使用して、暗号化とその他のセキュリティ技術を定義し、適用します。

デバイス ライセンスによって強力な暗号化を適用できる場合は、広範な暗号化とハッシュ アルゴリズム、および Diffie-Hellman グループがあり、その中から選択できます。ただし、一般に、トンネルに適用する暗号化が強力なほど、システム パフォーマンスは低下します。効率を損なうことなく十分な保護を提供するセキュリティとパフォーマンスのバランスを見出します。

シスコでは、どのオプションを選択するかについての特定のガイダンスは提供できません。比較的大規模な企業またはその他の組織内で運用している場合は、すでに、満たす必要がある標準が定義されている可能性があります。定義されていない場合は、時間を割いてオプションを調べてください。

以降のトピックでは、使用可能なオプションについて説明します。

使用する暗号化アルゴリズムの決定

IKE ポリシーまたは IPsec プロポーザルに使用する暗号化アルゴリズムを決定する際、選択肢は VPN のデバイスでサポートされるアルゴリズムに限られます。

IKEv2 では、複数の暗号化アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

IPsec プロポーザルでは、認証、暗号化、およびアンチリプレイ サービスを提供するカプセル化セキュリティ プロトコル（ESP）によってアルゴリズムが使用されます。ESP は、IP プロトコル タイプ 50 です。IKEv1 IPsec プロポーザルでは、アルゴリズム名の前に ESP というプレフィックスが付けられます。

デバイス ライセンスが強力な暗号化を適用できる場合、次の暗号化アルゴリズムを選択できます。強力な暗号化の対象ではない場合、DES のみ選択できます。

（注） 強力な暗号化の対象である場合、評価ライセンスをスマートライセンスにアップグレードする前に、暗号化アルゴリズムを確認および更新して暗号化を強化し、VPN設定が適切に機能するようにしてください。AESベースのアルゴリズムを選択します。強力な暗号化をサポートするアカウントを使用して登録されている場合、DES はサポートされません。登録後は、DES の使用対象をすべて削除するまで変更を展開できません。

- AES-GCM—（IKEv2 のみ）Galois/カウンタ モードの Advanced Encryption Standard は、機密性、データの発信元の認証を提供する操作のブロック暗号モードであり、AESよりも優れたセキュリティを提供します。AES-GCM には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。GCMはNSA Suite Bをサポートするために必要となるAESモードです。NSA Suite B は、暗号化強度に関する連邦標準規格を満たすためにデバイスがサポートすべき一連の暗号化アルゴリズムです。.
- AES（Advanced Encryption Standard）は DES よりも高度なセキュリティを提供する対称暗号化アルゴリズムであり、計算的には 3DES よりも効率的です。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。
- DES（データ暗号化標準）：56 ビット キーを使用して暗号化する対称秘密鍵ブロック アルゴリズムです。ライセンスアカウントが輸出規制の要件を満たしていない場合、これは唯一のオプションです。
- NULL、ESP-NULL：使用しないでください。NULL 暗号化アルゴリズムは、暗号化を使用しない認証を提供します。これは、ほとんどのプラットフォームでサポートされていません。

使用するハッシュ アルゴリズムの決定

IKEポリシーでは、ハッシュ アルゴリズムがメッセージ ダイジェストを作成します。これは、メッセージの整合性を保証するために使用されます。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数（PRF）に使用されます。

IPsecプロポーザルでは、ハッシュ アルゴリズムはカプセル化セキュリティ プロトコル（ESP）による認証のために使用されます。IKEv2 IPsec プロポーザルでは、これは整合性のハッシュと呼ばれます。IKEv1 IPsec プロポーザルでは、アルゴリズム名に ESP というプレフィックスだけでなく HMAC というサフィックスも付けられます（ハッシュ方式認証コードを意味する）。

IKEv2では、複数のハッシュ アルゴリズムを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

選択可能なハッシュ アルゴリズムは、次のとおりです。

- [SHA (Secure Hash Algorithm)]：標準の SHA（SHA1）は、160 ビットのダイジェストを生成します。

  IKEv2 の設定では、以下の SHA-2 オプションを指定して、より高度なセキュリティを実現できます。NSA Suite B 暗号化仕様を実装するには、次のいずれかを選択します。

  - SHA256：256 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA384：384 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。
  - SHA512：512 ビットのダイジェストを生成するセキュア ハッシュ アルゴリズム SHA 2 を指定します。

- NULL またはなし（NULL、ESP-NONE）：（IPsec プロポーザルのみ）NULL ハッシュ アルゴリズム。通常はテスト目的のみに使用されます。しかし、暗号化オプションとしていずれかの AES-GCM オプションを選択した場合は、NULL 整合性アルゴリズムを選択する必要があります。NULL 以外のオプションを選択した場合、これらの暗号化標準に対しては、整合性ハッシュは無視されます。

使用する Diffie-Hellman 係数グループの決定

次の Diffie-Hellman キー導出アルゴリズムを使用して、IPsec Security Association（SA：セキュリティアソシエーション）キーを生成することができます。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

AES 暗号化を選択する場合は、AES で必要な大きいキー サイズをサポートするために、Diffie-Hellman（DH：デフィーヘルマン）グループ 5 以降を使用する必要があります。IKEv1 ポリシーは、以下に示すすべてのグループをサポートしているわけではありません。

NSA Suite-B の暗号化の仕様を実装するには、IKEv2 を使用して楕円曲線 Diffie-Hellman（ECDH）オプション：19、20、21 のいずれか 1 つを選択します。楕円曲線オプションと、2048 ビット係数を使用するグループは、Logjam のような攻撃にさらされる可能性が低くなります。

IKEv2 では、複数のグループを設定できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。IKEv1 では、単一のオプションのみ選択できます。

- 14：Diffie-Hellman グループ 14（2048 ビット Modular Exponential（MODP）グループ）。192 ビットのキーでは十分な保護レベルです。
- 15：Diffie-Hellman グループ 15（3072 ビット MODP グループ）。
- 16：Diffie-Hellman グループ 16（4096 ビット MODP グループ）。
- 19：Diffie-Hellman グループ 19（国立標準技術研究所（NIST）256 ビット楕円曲線モジュロプライム（ECP）グループ）。
- 20：Diffie-Hellman グループ 20（NIST 384 ビット ECP グループ）。

- 21：Diffie-Hellman グループ 21（NIST 521 ビット ECP グループ）。
- 31：Diffie-Hellman グループ 31（Curve25519 256 ビット EC グループ）。

使用する認証方式の決定

次の方法を使用して、サイト間 VPN 接続でピアを認証できます。

事前共有キー

事前共有キーは、接続内の各ピアで設定された秘密鍵文字列です。これらのキーは、IKE が認証フェーズで使用します。IKEv1 の場合は、各ピアで同じ事前共有キーを設定する必要があります。IKEv2 の場合は、各ピアに一意のキーを設定できます。

事前共有キーは、証明書に比べて拡張性がありません。多数のサイト間 VPN 接続を設定する必要がある場合は、事前共有キー方式ではなく証明書方式を使用します。

証明書

デジタル証明書は IKE キー管理メッセージの署名や暗号化に RSA キー ペアを使用します。サイト間 VPN 接続の両端を設定するときに、リモートピアがローカルピアを認証できるように、ローカルデバイスのアイデンティティ証明書を選択します。

証明書方式を使用するには、次の手順を実行する必要があります。

1. ローカルピアを認証局（CA）に登録し、デバイスアイデンティティ証明書を取得します。この証明書をデバイスにアップロードします。詳細については、「内部および内部 CA 証明書のアップロード （184 ページ）」を参照してください。

   リモートピアも担当している場合、そのピアも登録してください。ピアに同じ CA を使用すると便利ですが、必須ではありません。

   自己署名証明書を使用して VPN 接続を確立することはできません。認証局でデバイスを登録する必要があります。

   Windows 認証局（CA）を使用してサイト間 VPN エンドポイントの証明書を作成する場合は、アプリケーションポリシー拡張に IP セキュリティエンドシステムを指定する証明書を使用する必要があります。これは（Windows CA サーバー）の [拡張] タブにある証明書の [プロパティ（Properties）] ダイアログボックスで確認できます。この拡張のデフォルトは IP セキュリティ IKE 中間であり、Device Manager を使用して設定されたサイト間 VPN では機能しません。

2. ローカルピアのアイデンティティ証明書に署名するために使用された、信頼できる CA 証明書をアップロードします。中間 CA を使用した場合は、ルート証明書と中間証明書を含む完全なチェーンをアップロードします。詳細については、「信頼できる CA 証明書のアップロード （188 ページ）」を参照してください。

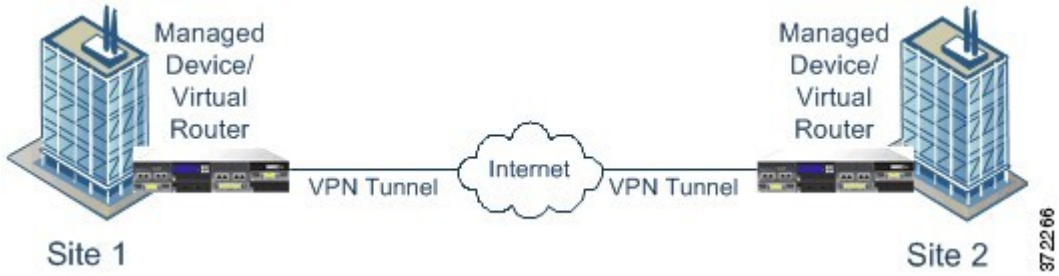
3. リモートピアが異なる CA で登録されていた場合、リモートピアのアイデンティティ証明書に署名するために使用した信頼できる CA 証明書もアップロードします。リモートピアを制御する組織から証明書を取得します。中間 CA を使用した場合は、ルート証明書と中間証明書を含む完全なチェーンをアップロードします。

4. サイト間VPN接続を設定したら、証明書方式を選択し、ローカルピアのアイデンティティ証明書を選択します。接続の両端が、接続のローカルエンドの証明書を指定します。リモート ピアの証明書は指定しません。

VPN トポロジ

Device Manager を使用して設定できるのは、ポイントツーポイント VPN 接続のみです。すべての接続はポイントツーポイントですが、デバイスが参加する各トンネルを定義することで、より大規模なハブアンドスポーク VPN、またはメッシュ VPN にリンクできます。

次の図は、一般的なポイントツーポイントの VPN トポロジを示しています。ポイントツーポイントの VPN トポロジでは、2 つのエンドポイントが相互に直接通信します。2 つのエンドポイントをピアデバイスとして設定し、いずれかのデバイスでセキュアな接続を開始することができます。



動的にアドレス指定されたピアによるサイト間 VPN 接続の確立

ピアの IP アドレスが不明な場合でも、ピアへのサイト間 VPN 接続を作成できます。これは、次のような場合に役立ちます。

- ピアが DHCP を使用してそのアドレスを取得した場合は、特定の静的 IP アドレスを持つリモートエンドポイントに依存することはできません。
- 不特定多数のリモートピアが、ハブアンドスポークトポロジのハブとして機能するデバイスとの接続を確立できるようにする場合。

動的にアドレス指定されたピアBへのセキュアな接続を確立する必要がある場合は、接続の終了 A にスタティック IP アドレスがあることを確認する必要があります。次に、A で接続を作成するときに、ピアのアドレスがダイナミックであることを指定します。ただし、ピアBで接続を設定する際は、リモートピアアドレスとして A の IP アドレスを入力します。

システムがサイト間 VPN 接続を確立する場合、ピアがダイナミックアドレスを持つすべての接続は応答のみとなります。つまり、リモートピアは接続を開始するものである必要があります。リモートピアが接続を確立しようとすると、デバイスは事前共有キーまたは証明書（接続で定義されているいずれかの方式）を使用して接続を検証します。

VPN 接続はリモートピアが接続を開始した後にのみ確立されるため、VPN トンネルのトラフィックを許可するアクセス制御ルールに一致するすべての発信トラフィックは、接続が確立

されるまでドロップされます。これにより、適切な暗号化と VPN 保護のないデータがネットワークから流出しないようになります。

仮想トンネルインターフェイスとルートベースの VPN

従来は、VPN トンネルを介して暗号化される特定のローカルネットワークとリモートネットワークを定義することにより、サイト間 VPN 接続を設定していました。これらは、VPN 接続プロファイルの一部である暗号マップで定義されます。このタイプのサイト間 VPN は、ポリシーベースと呼ばれます。

また、ルートベースのサイト間 VPN を設定することもできます。この場合は、仮想トンネルインターフェイス（VTI）を作成します。これは、特定の物理インターフェイス（通常、外部インターフェイス）に関連付けられた仮想インターフェイスです。その後、ルーティングテーブルと静的ルートおよび動的ルートを使用して、目的のトラフィックを VTI に転送します。VTI（出力）を介してルーティングされるトラフィックは、VTI 用に設定した VPN トンネルを介して暗号化されます。

そのため、ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウド サービス プロバイダーや大企業の VPN 管理が簡素化されます。

さらに、VTIのアクセス制御ルールを作成して、トンネルで許可されるトラフィックのタイプを微調整できます。たとえば、侵入検査や、URL およびアプリケーション フィルタリングを適用できます。

ルートベースの VPN を設定するためのプロセスの概要

概要として、ルートベースのサイト間 VPN をセットアップするプロセスには、次の手順が含まれます。

手順

ステップ 1 ローカルエンドポイントの IKEv1/2 ポリシーと IPsec プロポーザルを作成します。

ステップ 2 リモートピアに面する物理インターフェイスに関連付けられた仮想トンネルインターフェイス（VTI）を作成します。

ステップ 3 VTI、IKE ポリシー、および IPsec プロポーザルを使用するサイト間 VPN 接続プロファイルを作成します。

ステップ 4 リモートピア（およびリモート VTI）に同じ IKE および IPsec プロポーザルを作成し、このローカル VTI をリモートエンドポイントとして指定（リモートピアの観点から）するサイト間 VPN 接続プロファイルを作成します。

ステップ 5 トンネルを介して適切なトラフィックを送信するために、両方のピアでルートとアクセス制御ルールを作成します。

両方向のトラフィックフローを可能にするために、各エンドポイントのルートとアクセス制御が相互にミラーリングされていることを確認してください。

静的ルートには、次のような一般的特性があります。

- [インターフェイス（Interface）]：仮想トンネルインターフェイス（VTI）の名前。
- [ネットワーク（Networks）]：リモートエンドポイントによって保護されるリモートネットワークを定義するネットワークオブジェクト。
- [ゲートウェイ（Gateway）]：VPN トンネルのリモートエンドポイントの IP アドレスを定義するネットワークオブジェクト。

仮想トンネルインターフェイスとルートベースの VPN に関するガイドライン

IPv6 のガイドライン

仮想トンネルインターフェイスは IPv4 アドレスのみをサポートしています。VTI で IPv6 アドレスを設定することはできません。

追加のガイドライン

- 最大 1024 個の VTI を作成できます。
- VTI ルートベース VPN では、リバース ルート インジェクション（静的または動的）を設定できません（リバース ルート インジェクションは Threat Defense API のみを使用して設定可能）。
- VTI をローカルインターフェイスとして選択する場合は、動的ピアアドレスを設定できません。
- VTI をローカルインターフェイスとして選択する場合は、リモートバックアップピアを設定できません。
- カスタム仮想ルータに割り当てられている送信元インターフェイスに VTI を作成することはできません。仮想ルータを使用する場合、グローバル仮想ルータのインターフェイスのみで、VTI を設定できます。
- IKE および IPsec のセキュリティ アソシエーションには、トンネル内のデータ トラフィックに関係なく、継続的にキーの再生成が行われます。これにより、VTI トンネルは常にアップした状態になります。
- ルートベースの接続プロファイルで IKEv1 と IKEv2 の両方を設定することはできません。1 つのバージョンの IKE のみを設定する必要があります。
- 暗号マップに設定されるピアアドレスと VTI のトンネル宛先が異なる場合は、同じ物理インターフェイスで異なる VTI およびポリシーベース（暗号マップ）設定を指定できます。
- VTI を介してサポートされるのは BGP ルーティングプロトコルだけです。

- システムが IOS IKEv2 VTI クライアントを終端している場合は、IOS VTI クライアントによって開始されたセッションのモード CFG 属性をシステムが取得できないため、IOS での設定交換要求を無効にします。
- ルートベースのサイト間 VPN は双方向として設定されます。つまり、VPN トンネルのどちらのエンドポイントでも接続を開始できます。接続プロファイルを作成したら、このエンドポイントを唯一のイニシエータ（INITIATE_ONLY）に変更するか排他的にレスポンダ（RESPOND_ONLY）に変更することができます。必ず、補完的な接続タイプを使用するようにリモートエンドポイントを変更してください。この変更を行うには、API エクスプローラに移動し、GET /devices/default/s2sconnectionprofiles を使用して接続プロファイルを見つける必要があります。その後、本文の内容をコピーして PUT /devices/default/s2sconnectionprofiles/{objId} メソッドに貼り付け、[connectionType] を更新して目的のタイプを指定して、メソッドを実行します。

IPsec フローのオフロード

IPsec フローのオフロードを使用するように、サポートするデバイスモデルを設定できます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。

オフロード操作は、特に、入力の事前復号および復号処理と出力の事前暗号化および暗号化処理に関連しています。システムソフトウェアは、セキュリティポリシーを適用するための内部フローを処理します。

IPsec フローのオフロードはデフォルトで有効になっており、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 3100

IPsec フローのオフロードに関する制約事項

次の IPsec フローはオフロードされません。

- IKEv1 トンネル。IKEv2 トンネルのみがオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- ボリュームベースのキー再生成が設定されているフロー。
- 圧縮が設定されているフロー。
- トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
- AH 形式。ESP/NAT-T 形式のみがサポートされます。
- ポストフラグメンテーションが設定されているフロー。
- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。

• ファイアウォールフィルタが有効になっているフロー。

IPsec フローのオフロードの設定

IPsec フローのオフロードは、この機能をサポートするハードウェア プラットフォームではデフォルトで有効になっています。設定を変更するには、FlexConfig を使用して **flow-offload-ipsec** コマンドを実装します。このコマンドの詳細については、ASA コマンドリファレンスを参照してください。

サイト間 VPN の管理

バーチャル プライベート ネットワーク（VPN）は、パブリック ソース（インターネットやその他のネットワークなど）を使用して、リモート ピア間でセキュアなトンネルを確立するネットワーク接続です。VPN ではトンネルを使用して通常の IP パケット内のデータ パケットがカプセル化され、IP ベースのネットワークを介して転送されます。VPN ではプライバシーの確保と認証のために暗号化が使用され、データの整合性が確保されます。

ピア デバイスへの VPN 接続を作成できます。接続はすべてポイントツーポイントですが、関連する接続をすべて設定することで、大規模なハブアンドスポークやメッシュ VPN にデバイスを接続できます。

始める前に

次の事実によって、再作成できるサイト間 VPN 接続のタイプと数が制御されます。

- VPN 接続では、暗号化を使用してネットワークのプライバシーが保護されます。使用できる暗号化アルゴリズムは、基本ライセンスで強力な暗号化が許可されているどうかによって異なります。これは、Cisco Smart License Manager に登録するときにデバイス上で輸出管理機能を許可するオプションを選択しているかどうかによって制御されます。評価ライセンスを使用している場合、または輸出管理機能を有効にしていない場合は、強力な暗号化を使用できません。
- 最大 20 の一意の IPsec プロファイルを作成できます。一意性は、IKEv1/v2 プロポーザルと証明書、接続タイプ、DH グループ、および SA ライフタイムの組み合わせによって決定されます。既存のプロファイルを再利用できます。そのため、すべてのサイト間 VPN 接続に同じ設定を使用すると、1 つの一意の IPsec プロファイルを持つことになります。一意の IPsec プロファイルの数が上限の 20 に達すると、既存の接続プロファイルに使用したものと同じ属性の組み合わせを使用しないかぎり、新しいサイト間 VPN 接続を作成できません。

手順

ステップ 1 [デバイス（Device）] をクリックし、次に [サイト間VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。

これで、[サイト間VPN（Site-to-Site VPN）] ページが開き、設定済みのすべての接続が表示されます。

ステップ 2 次のいずれかを実行します。

- 新しいサイト間 VPN 接続を作成するには、[+] ボタンをクリックします。サイト間 VPN 接続の設定 （790 ページ）を参照してください。

  まだ接続が存在しない場合でも、[サイト間接続の作成（Create Site-to-Site Connection）] ボタンはクリックできます。

- 既存の接続を編集するには、その接続の編集（  ）アイコンをクリックします。サイト間 VPN 接続の設定 （790 ページ）を参照してください。

- 接続設定のサマリーをクリップボードにコピーするには、その接続の [コピー（copy）] アイコン（  ）をクリックします。その情報をドキュメントに貼り付け、リモート デバイスの管理者に送信して、接続の一端の設定をサポートできます。

- 不要になった接続を削除するには、その接続の [削除（delete）] アイコン（  ）をクリックします。

サイト間 VPN 接続の設定

リモート デバイス オーナーの協力と許可を得ている場合、ポイントツーポイント VPN 接続を作成し、デバイスを別のデバイスにリンクできます。すべての接続はポイントツーポイントですが、デバイスが参加する各トンネルを定義することで、より大きなハブアンドスポークまたはメッシュ VPN にリンクできます。

始める前に

ローカル ネットワーク/リモート ネットワークの組み合わせごとに、1 つの VPN 接続を作成できます。ただし、リモート ネットワークが各接続プロファイルで一意である場合は、ローカル ネットワークに対して複数の接続を作成できます。

リモートネットワークが重複している場合は、より制限の厳しい接続プロファイルを最初に作成するように注意してください。システムはトンネルを、表示される順序（アルファベット順）ではなく、接続プロファイルを作成した順序で作成します。

たとえば、リモートエンドポイント A へのアクセスには 192.16.0.0/16 から 10.91.0.0/16 までをトンネリングさせ、192.16.0.0/24 から 10.0.0.0/8 の残りへのトンネリングはリモートエンドポイント B を介して行う場合、B の接続プロファイルを作成する前に A の接続プロファイルを作成する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、次に [サイト間VPN（Site-to-Site VPN）] グループの [設定の表示（View Configuration）] をクリックします。

ステップ 2 次のいずれかを実行します。

- 新しいサイト間 VPN 接続を作成するには、[+] ボタンをクリックします。

  まだ接続が存在しない場合でも、[サイト間接続の作成（Create Site-to-Site Connection）] ボタンはクリックできます。

- 既存の接続を編集するには、その接続の編集（）アイコンをクリックします。

不要になった接続を削除するには、接続の [削除（delete）]アイコン（）をクリックします。

ステップ 3 ポイントツーポイント VPN 接続のエンドポイントを定義します。

- [接続プロファイル名（Connection Profile Name）]：この接続の名前で、スペースなしで最大 64 文字 までです。例、MainOffice。IP アドレスは名前として使用できません。
- [タイプ（Type）]：VPN トンネルを介して送信する必要があるトラフィックを識別する方法。次のいずれかを選択します。
  - [ルートベース（VTI）（Route Based (VTI)）]：ルーティングテーブル（主にスタティックルート）を使用して、トンネルに参加するローカルネットワークとリモートネットワークを定義します。このオプションを選択する場合は、仮想トンネルインターフェイス（VTI）をローカル VPN アクセスインターフェイスとして選択する必要があります。また、トンネルのリモートエンドには静的 IP アドレスを使用する必要があります。VPN 接続プロファイルを作成した後に、必ず、VTI の適切な静的ルートとアクセス制御ルールを設定してください。
  - [ポリシーベース（Policy Based）]：ローカルネットワークとリモートネットワークを、サイト間 VPN 接続プロファイルで直接指定します。これは、VPN トンネルによって保護する必要があるトラフィックを定義するための従来のアプローチです。
- [ローカルサイト（Local Site）]：これらのオプションではローカルエンドポイントを定義します。
  - [ローカルVPNのアクセスインターフェイス（Local VPN Access Interface）]：リモートピアが接続できるインターフェイスを選択します。これは通常、外部インターフェイスです。インターフェイスをブリッジグループのメンバーにはできません。ポリシーベースの接続のバックアップピアを設定する場合は、ピアが接続できるすべてのインターフェイスを選択してください。ルートベースの接続の場合、選択できるインターフェイスは 1 つだけです。
  - [ローカルネットワーク（Local Network）]：（ポリシーベースのみ）[+] をクリックし、VPN 接続に参加する必要があるローカルネットワークを識別するネットワークオブジェクトを選択します。これらのネットワーク上のユーザーは、この接続を介してリモート ネットワークに到達できます。

（注） これらのネットワークに IPv4 アドレスまたは IPv6 アドレスを使用できますが、接続の各側に一致するアドレス タイプがなければなりません。たとえば、ローカル IPv4 ネットワークの VPN 接続には、少なくとも 1 つのリモート IPv4 ネットワークが必要です。1 つの接続の両側で、IPv4 と IPv6 を組み合わせることができます。エンドポイントの保護されたネットワークは重複することはできません。

- [リモートサイト（Remote Site）]：これらのオプションでリモート エンドポイントを定義します。
  - [スタティック（Static）]/[ダイナミック（Dynamic）]：リモートピアの IP アドレスが静的または動的（DHCP などを使用して）のどちらで定義されるか。[スタティック（Static）] を選択した場合、リモートピアの IP アドレスも入力します。[ダイナミック（Dynamic）] を選択した場合、リモートピアのみがこの VPN 接続を開始できるようになります。

    ルートベースの VPN の場合は、選択できるのは [スタティック（Static）] のみです。
  - [リモートIPアドレス（Remote IP Address）]（スタティック アドレス指定のみ）：VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスを入力します。
  - [リモートバックアップピア（Remote Backup Peers）]：（オプション、ポリシーベースの接続のみ）[ピアの追加（Add Peer）] をクリックして、リモートエンドポイントのバックアップを追加します。プライマリエンドポイントが使用できなくなると、システムはバックアップピアの 1 つで VPN 接続を再確立しようとします。複数のバックアップを追加できます。

    各バックアップピアを設定するときに、そのピアで使用する事前共有キーと証明書を設定できます。プライマリリモートピアの設定に使用したのと同じ手法を使用します。接続プロファイルに設定されている同じ値を使用するには、これらの設定を空白のままにします。

    最初のバックアップピアを設定後、[別のピアを追加（Add Another Peer）] をクリックして別のピアを追加するか、ピアを削除するか、または [編集（Edit）] をクリックしてピアの設定を変更できます。

    バックアップピアがプライマリピアとは異なるインターフェイスを介して到達可能な場合は、[ローカルVPNアクセスインターフェイス（Local VPN Access Interface）] で必要なインターフェイスを選択していることを確認します。
  - [リモートネットワーク（Remote Network）]：（ポリシーベースのみ）[+] をクリックし、VPN接続に参加する必要があるリモートネットワークを識別するネットワークオブジェクトを選択します。これらのネットワーク上のユーザーは、この接続を介してローカル ネットワークに到達できます。

ステップ 4 [Next] をクリックします。

ステップ 5 VPN のプライバシー設定を定義します。

（注） ライセンスにより、どの暗号化プロトコルを選択できるかが決まります。最も基本的なオプション以外のものを選択するには、輸出規制を満たすなど、強力な暗号化が必要です。

- [IKEバージョン2（IKE Version 2）]、[IKEバージョン1（IKE Version 1）]：インターネットキーエクスチェンジ（IKE）ネゴシエーション時に使用する IKE バージョンを選択します。ポリシーベースの接続の場合は、いずれかまたは両方を選択できます。ルートベースの場合、選択できるのは一方のみです。デバイスがもう 1 つのピアとの接続のネゴシエーションを試行する場合は、ユーザーが許可したバージョン、およびもう 1 つのピアが受け入れるバージョンのどちらでも使用されます。両方のバージョンを許可すると、最初に選択したバージョンとのネゴシエーションが正常に行われなかった場合、デバイスはもう 1 つのバージョンに自動的にフォールバックします。IKEv2 が設定されている場合、常に最初に試行されます。ネゴシエーションで使用するには、両方のピアが IKEv2 をサポートする必要があります。

- [IKEポリシー（IKE Policy）]：インターネットキーエクスチェンジ（IKE）は、IPsec ピアの認証、IPsec 暗号化キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動的な確立に使用されるキー管理プロトコルです。これはグローバルポリシーで、有効にしたオブジェクトはすべての VPN に適用されます。[編集（Edit）] をクリックし、IKE バージョンごとに現在グローバルに有効なポリシーを確認し、新しいポリシーを有効化し、作成します。詳細については、グローバル IKE ポリシーの設定（797 ページ）を参照してください。

- [Ipsecプロポーザル（IPsec Proposal）]：IPsec プロポーザルは、IPsec トンネルのトラフィックを保護するセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。[編集（Edit）] をクリックし、IKE バージョンごとのプロポーザルを選択します。ユーザーに許可するすべてのプロポーザルを選択します。[デフォルトの設定（Set Default）] をクリックし、システム デフォルトを選択します。これはエクスポート コンプライアンスに応じて異なります。一致が合意されるまで、最も強いプロポーザルから最も弱いプロポーザルまで、ピアとのネゴシエートが行われます。詳細については、「IPsec プロポーザルの設定（802 ページ）」を参照してください。

- [認証タイプ（Authentication Type）]：VPN 接続でピアを認証する方法（[事前共有手動キー（Preshared Manual Key）] または [証明書（Certificate）] のいずれか）。また、選択内容に基づいて次のフィールドに入力する必要があります。IKEv1 の場合、接続用に設定された IKEv1 ポリシーオブジェクトで選択された認証方式と選択内容が一致する必要があります。オプションの詳細については、使用する認証方式の決定（784 ページ）を参照してください。

  - （IKEv2）[ローカル事前共有キー（Local Preshared Key）]、[リモートピア事前共有キー（Remote Peer Preshared Key）]：VPN 接続のためにこのデバイスとリモート デバイスで定義されたキー。これらのキーは IKEv2 では異なることがあります。このキーには 1 ～ 127 の英数字を指定できます。

  - （IKEv1）[事前共有キー（Preshared Key）]：ローカル デバイスとリモート デバイスの両方で定義されたキー。このキーには 1 ～ 127 の英数字を指定できます。

- [証明書（Certificate）]：ローカル ピアのデバイス アイデンティティ証明書。これは、認証局（CA）から取得した証明書である必要があります。自己署名証明書は使用できません。証明書をアップロードしていない場合は、[新しいオブジェクトの作成（Create New Object）] リンクをクリックします。また、アイデンティティ証明書の署名に使用されたルート証明書および中間 CA 証明書をアップロードする必要があります。アップロードされた証明書の [検証の使用（Validation Usage）] が [IPsecクライアント（IPsec Client）] を含むように設定されていることを確認します。まだアップロードしていない場合は、このウィザードを完了した後に実行できます。

- [IPsec設定（IPsec Settings）]：セキュリティ アソシエーションのライフタイム。ライフタイムに達すると、システムはセキュリティ アソシエーションを再ネゴシエートします。システムは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。ライフタイムには、「指定時刻」ライフタイムと「トラフィック量」ライフタイムの2つがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。

  - [ライフタイム期間（Lifetime Duration）]：セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。

  - [ライフタイムサイズ（Lifetime Size）]：所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。範囲は 10 ー 2147483647 KB、または空白です。グローバル デフォルトは 4,608,000 キロバイトです。サイズベースの制限を削除し、期間を唯一の制限として使用するには、フィールドを空白のままにします。

- [NAT免除（NAT Exempt）]：（ポリシーベースのみ）ローカル VPN アクセスインターフェイスで VPN トラフィックを NAT ポリシーから免除するかどうか。NAT ルールをローカル ネットワークに適用しない場合、ローカル ネットワークをホストするインターフェイスを選択します。このオプションは、ローカル ネットワークが 1 つのルーテッド インターフェイス（ブリッジグループ メンバーではない）の背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッド インターフェイスまたは 1 つ以上のブリッジグループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、NAT からのサイト間 VPN トラフィックの除外 （809 ページ）を参照してください。

- [Perfect Forward Secrecy用Diffie-Helmanグループ（Diffie-Helman Group for Perfect Forward Secrecy）]：暗号化されたやり取りごとに一意のセッション キーを生成および使用するため、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。一意のセッション キーを使用することによって、やり取りを以降の復号から保護します。このことは、やり取り全体が記録され、攻撃者がエンドポイント デバイスで使用される事前共有キーまたは秘密キーを入手している場合であっても該当します。Perfect Forward Secrecy を有効にする場合、[モジュラスグループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムを選択します。IKEv1 と IKEv2 の両方を有効にすると、オプションは IKEv1 でサポートされているものに制限されます。オプショ

ンの説明については、使用する Diffie-Hellman 係数グループの決定 （783 ページ）を参照してください。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 サマリーを確認し、[終了（Finish）] をクリックします。

サマリー情報がクリップボードにコピーされます。この情報はドキュメントに貼り付けて、リモート ピアの設定、またはピアの設定責任者に送信するために使用できます。

サイト間VPN経由によるトラフィックの許可（796ページ）で説明したように、追加の手順でVPN トンネル内のトラフィックを許可する必要があります。

設定を展開後、デバイス CLI にログインし、**show ipsec sa** コマンドを使用してエンドポイントでセキュリティ アソシエーションが確立されることを確認します。「サイト間 VPN 接続の確認 （806 ページ）」を参照してください。

仮想トンネルインターフェイスの設定

ルートベースのサイト間VPN接続プロファイルでのみ仮想トンネルインターフェイス（VTI）を使用できます。VTIは物理インターフェイスに関連付けられており、これを介してリモートピアへのVPN接続が確立されます。仮想インターフェイスを使用すると、サイト間VPN接続が簡素化され、接続プロファイルでVPNのローカルネットワークとリモートネットワークを指定するのではなく、スタティックルートと動的ルートを使用してトラフィックを制御できます。

手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーのリンクをクリックして、[仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] をクリックします。

ステップ 2 次のいずれかを実行します。

- [+] または [仮想トンネルインターフェイスの作成（Create Virtual Tunnel Interface）] をクリックして新しいインターフェイスを作成します。
- 既存のインターフェイスの編集アイコン（  ）をクリックします。

インターフェイスが不要になった場合は、そのインターフェイスの削除アイコン（  ）をクリックします。インターフェイスを削除する前に、まず、そのインターフェイスを使用するサイト間接続プロファイルをすべて削除する必要があります。

ステップ 3 次のオプションを設定します。

- [名前（Name）]：インターフェイス名（最大 48 文字）。既存のインターフェイスの名前を変更すると、それを含むすべてのポリシーとオブジェクトでも名前が自動的に変更されます。名前に大文字を使用することはできません。

- [ステータス（Status）]：スライダをクリックして有効の位置にします（）。
- [Description]：（任意） 説明は 200 文字以内で、改行を入れずに 1 行で入力します。
- [トンネルID（Tunnel ID）]：0 ー 10413 の番号。この番号が「Tunnel」という語に付加されて、インターフェイスのハードウェア名が形成されます。まだ別の VTI に使用されていない番号を選択する必要があります。たとえば、インターフェイス Tunnel1 を作成するには 1 を入力します。
- [トンネルの送信元（Tunnel Source）]：この VTI に関連付けられるインターフェイスを選択します。トンネルの送信元は、仮想トンネルインターフェイスで定義されたサイト間 VPN がリモートエンドポイントに接続するためのインターフェイスです。外部インターフェイスなどのリモートエンドポイントに到達できるインターフェイスを選択します。送信元インターフェイスには、名前付きの物理インターフェイス、サブインターフェイス、または Etherchannel を指定できます。インターフェイスをブリッジ仮想インターフェイス（BVI）のメンバーにすることはできません。
- [IPアドレスとサブネットマスク（IP Address and Subnet Mask）]：IPv4 アドレスおよび関連サブネットマスク。たとえば、192.168.1.1/24 または /255.255.255.0 です。このアドレスは、トンネル送信元インターフェイスのアドレスと同じサブネット上にある必要はありません。ただし、送信元インターフェイスでリモートアクセス（RA）VPN を設定する場合、VTI IP アドレスは RA VPN に設定されたアドレスプール内にはありません。

ステップ 4 [OK] をクリックします。

サイト間 VPN 経由によるトラフィックの許可

サイト間 VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

- **sysopt connection permit-vpn** コマンドを設定します。これにより、VPN 接続と一致するトラフィックがアクセス コントロール ポリシーから免除されます。このコマンドのデフォルトは **no sysopt connection permit-vpn** で、VPN トラフィックをアクセス コントロール ポリシーでも許可する必要があることを意味します。

  これは、外部ユーザが保護されたリモート ネットワーク内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

  このコマンドを設定するのに適した方法は、リモート アクセス VPN 接続プロファイルを作成し、そこで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（Bypass Access Control policy for decrypted traffic）] オプションを選択することです。RA VPN を設定しない場合、または RA VPN を設定できない場合、FlexConfig を使用してコマンドを設定することができます。

（注） この方式は、仮想トンネルインターフェイス（VTI）で設定されたルートベースの VPN 接続には適用されません。ルートベースの VPN のアクセス制御ルールは常に設定する必要があります。

- リモート ネットワークからの接続を許可するアクセス制御ルールを作成します。この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

グローバル IKE ポリシーの設定

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

IKE ポリシー オブジェクトはこれらのネゴシエーションに対して IKE プロポーザルを定義します。有効にするオブジェクトは、ピアが VPN 接続をネゴシエートするときに使用するものであり、接続ごとに異なる IKE ポリシーを指定することはできません。各オブジェクトの相対的な優先順位は、これらの中でどのポリシーを最初に試すかを決定します。数が小さいほど、優先順位が高くなります。ネゴシエーションで両方のピアがサポートできるポリシーを見つけられなければ、接続は確立されません。

IKE グローバル ポリシーを定義するには、各 IKE バージョンを有効にするオブジェクトを選択します。事前定義されたオブジェクトが要件を満たさない場合、セキュリティ ポリシーを適用する新しいポリシーを作成します。

次に、オブジェクト ページでグローバル ポリシーを設定する方法について説明します。VPN 接続を編集しているときに IKE ポリシー設定の [編集（Edit）] をクリックすることで、ポリシーの有効化、無効化および作成が行えます。

（注） 最大 20 の IKE ポリシーを有効にできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [IKEポリシー（IKE Policies）] を選択します。

IKEv1 と IKEv2 のポリシーが別のリストに表示されます。

ステップ 2 各 IKE バージョンで許可する IKE ポリシーを有効にします。

a) オブジェクト テーブル上部の [IKEv1] または [IKEv2] を選択すると、そのバージョンのポリシーが表示されます。

b) 適切なオブジェクトを有効にし、要件を満たしていないオブジェクトを無効にするには、[状態（State）] トグルをクリックします。

セキュリティ要件の一部が既存のオブジェクトに反映されていない場合、要件に合う新しい要件を定義します。詳細については、次のトピックを参照してください。

- IKEv1 ポリシーの設定 （798 ページ）
- IKEv2 ポリシーの設定 （800 ページ）

c) 相対的な優先順位が要件を満たすことを確認します。

ポリシーの優先順位を変更する必要がある場合は編集します。ポリシーが事前定義されたシステム ポリシーである場合、優先順位を変更するための独自のバージョンのポリシーを作成する必要があります。

優先順位は相対的であり、絶対的ではありません。たとえば、優先順位 80 は 160 より優先されます。80 が最も優先順位の高い有効なオブジェクトである場合、これが最初に選択されるポリシーとなります。その後、優先順位が 25 のポリシーを有効にすると、それが最初に選択されるポリシーとなります。

d) 両方の IKE バージョンを使用する場合、このプロセスを他のバージョンでも繰り返します。

IKEv1 ポリシーの設定

インターネット キー エクスチェンジ（IKE）バージョン 1 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv1 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv1 ポリシーが存在します。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。IKEv1 設定の編集時に、オブジェクト リストに表示される [新しいIKEポリシーの作成（Create New IKE Policy）] リンクをクリックして、IKEv1 ポリシーを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IKEポリシー（IKE Policies）] を選択します。

ステップ 2 IKEv1 ポリシーを表示するには、オブジェクト テーブル上部の [IKEv1] を選択します。

ステップ 3 システム定義ポリシーのいずれかが要件を満たす場合には、[状態（State）] トグルをクリックして有効にします。

不要なポリシーを無効にする場合にも、[状態（State）] トグルを使用します。番号が小さい方が高い優先順位を持つ相対的な優先順位により、どのポリシーが最初に試行されるかが決定されます。

ステップ 4 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 5 IKEv1 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先度（1 ～ 65,535）。このプライオリティによって、共通のセキュリティアソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [状態（State）]：IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [認証（Authentication）]：2 つのピア間で使用される認証方式。詳細については、使用する認証方式の決定 （784 ページ）を参照してください。
  - [事前共有キー（Preshared Key）]：各デバイスで定義されている事前共有キーを使用します。事前共有キーを使用すると、秘密鍵を 2 つのピア間で共有し、認証フェーズ中に IKE で使用できます。ピアに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。
  - [証明書（Certificate）]：ピアのデバイス ID 証明書を使用して相互に識別します。認証局に各ピアを登録することによって、これらの証明書を取得する必要があります。

また、各ピアでアイデンティティ証明書の署名に使用された、信頼できる CA ルート証明書および中間 CA 証明書もアップロードする必要があります。ピアは、同じ CA または別の CA に登録できます。どちらのピアにも自己署名証明書を使用することはできません。

- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。オプションの説明については、使用する暗号化アルゴリズムの決定（781 ページ）を参照してください。
- [Diffie-Hellman グループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。オプションの説明については、使用する Diffie-Hellman 係数グループの決定（783 ページ）を参照してください。
- [ハッシュ（Hash）]：メッセージの整合性の確保に使用されるメッセージ ダイジェストを作成するためのハッシュ アルゴリズム。オプションの説明については、使用するハッシュ アルゴリズムの決定（782 ページ）を参照してください。
- [有効期間（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 6 [OK] をクリックして変更を保存します。

IKEv2 ポリシーの設定

インターネット キー エクスチェンジ（IKE）バージョン 2 ポリシー オブジェクトには、VPN 接続を定義する際に必要な IKEv2 ポリシーが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

複数の事前定義された IKEv2 ポリシーがあります。必要に適したポリシーがあれば、[状態（State）] トグルをクリックして有効にします。セキュリティ設定の他の組み合わせを実装する新しいポリシーも作成できます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。IKEv2 設定の編集時に、オブジェクト リストに表示される [新しい

IKEポリシーの作成（Create New IKE Policy）] リンクをクリックして、IKEv2 ポリシーを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IKEポリシー（IKE Policies）] を選択します。

ステップ 2 IKEv2 ポリシーを表示するには、オブジェクト テーブル上部の [IKEv2] を選択します。

ステップ 3 システム定義ポリシーのいずれかが要件を満たす場合には、[状態（State）] トグルをクリックして有効にします。

不要なポリシーを無効にする場合にも、[状態（State）] トグルを使用します。番号が小さい方が高い優先順位を持つ相対的な優先順位により、どのポリシーが最初に試行されるかが決定されます。

ステップ 4 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 5 IKEv2 プロパティを設定します。

- [優先順位（Priority）]：IKE ポリシーの相対的優先度（1 ～ 65,535）。このプライオリティによって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。リモート IPsec ピアが、最も高いプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、次に低いプライオリティで定義されているパラメータの使用を試行します。値が小さいほど、プライオリティが高くなります。
- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [状態（State）]：IKE ポリシーが有効か無効かを示します。トグルをクリックして状態を変更します。IKE ネゴシエーション中には、有効なポリシーのみが使用されます。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 セキュリティ アソシエーション（SA）の確立に使用される暗号化アルゴリズム。有効にするすべてのアルゴリズムを選択します。ただし、同じポリシーに混合モード（AES-GCM）と通常モードのオプションを含めることはできません（通常モードには整合性ハッシュの選択が必要ですが、混合モードは個別の整合性ハッシュの選択を無効化します）。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定 （781 ページ）を参照してください。
- [Diffie-Hellmanグループ（Diffie-Hellman Group）]：2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きい

ほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。許可するすべてのアルゴリズムを選択します。システムは、最も強いグループから始めて最も弱いグループに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （783 ページ）を参照してください。

- [整合性ハッシュ（Integrity Hash）]：メッセージの整合性の確保に使用されるメッセージダイジェストを作成するためのハッシュ アルゴリズムの整合性部分。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。整合性ハッシュは、AES-GCM 暗号化オプションでは使用されません。オプションの説明については、使用するハッシュ アルゴリズムの決定 （782 ページ）を参照してください。
- [擬似ランダム関数（PRF）ハッシュ（Pseudo Random Function（PRF）Hash）]：IKEv2 トンネル暗号化に必要なキー材料とハッシュ操作を得るためのアルゴリズムとして使用されるハッシュ アルゴリズムの擬似ランダム関数（PRF）部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用するハッシュ アルゴリズムの決定 （782 ページ）を参照してください。
- [有効期間（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（120 ～ 2147483647 までの秒数、または空白）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。デフォルトは 86400 です。無期限のライフタイムを指定するには、値を入力しません（フィールドを空白のままにします）。

ステップ 6 [OK] をクリックして変更を保存します。

IPsec プロポーザルの設定

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2 つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。IPsec Security Association（SA：セキュリティ アソシエーション）のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec プロポーザル オブジェクトがあります。

- IKEv1 IPsec プロポーザルを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。アルゴリズムには単一のオプションを選択できます。VPN で複数の組み合わせをサポートするには、複数の IKEv1 IPsec プロポーザル オブジェクトを作成して選択します。
- IKEv2 IPsec プロポーザルを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。システムは、設定をセキュア度が最も高いものから最も低いものに並べ替え、マッチが見つかるまでピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

カプセル化セキュリティ プロトコル（ESP）は、IKEv1 と IKEv2 IPsec プロポーザルの両方に使用されます。これは認証、暗号化、およびアンチリプレイ サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

（注） IPsec トンネルで暗号化と認証の両方を使用することを推奨します。

次に、各 IKE バージョンの IPsec プロポーザルの設定方法を説明します。

IKEv1 の IPsec プロポーザルの設定

IKEv1 IPsec プロポーザル オブジェクトを使用して、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

定義済みの複数の IKEv1 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv1 IPsec 設定を編集している間に、オブジェクト リストに表示される [新規IPsecプロポーザルの作成（Create New IPsec Proposal）] リンクをクリックして、IKEv1 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IPsecプロポーザル（IPsec Proposals）] を選択します。

ステップ 2 オブジェクト テーブルの上にある [IKEv1] を選択して、IKEv1 IPsec プロポーザルを表示します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 IKEv1 IPsec プロポーザルのプロパティを設定します。

- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [モード（Mode）]：IPsec トンネルが動作するモード。
  - [トンネル（Tunnel）]モード：IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネル モードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。
  - [トランスポート（Transport）]モード：IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。
- [ESP暗号化（ESP Encryption）]：このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。オプションの説明については、使用する暗号化アルゴリズムの決定 （781 ページ）を参照してください。
- [ESPハッシュ（ESP Hash）]：認証に使用するハッシュまたは整合性アルゴリズム。オプションの説明については、使用するハッシュ アルゴリズムの決定 （782 ページ）を参照してください。

ステップ 5 [OK] をクリックして変更を保存します。

IKEv2 の IPsec プロポーザルの設定

IKEv2 IPsec プロポーザル オブジェクトを使用して、IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルでは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。

定義済みの複数の IKEv2 IPsec プロポーザルがあります。その他のセキュリティ設定の組み合わせを実装する新しいプロポーザルを作成することもできます。システム定義オブジェクトは、編集または削除できません。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成および編集する方法について説明します。VPN 接続の IKEv2 IPsec 設定を編集している間に、オブジェクトリストに表示される [新規IPsecプロポーザルの作成（Create New IPsec Proposal）] リンクをクリックして、IKEv2 IPsec プロポーザル オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [IPsecプロポーザル（IPsec Proposals）] を選択します。

ステップ 2 オブジェクト テーブルの上にある [IKEv2] を選択して、IKEv2 IPsec プロポーザルを表示します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 IKEv2 IPsec プロポーザルのプロパティを設定します。

- [名前（Name）]：オブジェクトの名前（最大 128 文字）。
- [暗号化（Encryption）]：このプロポーザルのカプセル化セキュリティ プロトコル（ESP）暗号化アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用する暗号化アルゴリズムの決定 （781 ページ）を参照してください。
- [整合性ハッシュ（Integrity Hash）]：認証に使用するハッシュまたは整合性アルゴリズム。許可するすべてのアルゴリズムを選択します。システムは、最も強いアルゴリズムから始めて最も弱いアルゴリズムに至るまで、適合するものが確認できるまでピアとネゴシエートします。オプションの説明については、使用するハッシュ アルゴリズムの決定 （782 ページ）を参照してください。

  （注） 暗号化アルゴリズムとしていずれかの AES-GCM/GMAC オプションを選択する場合は、ヌル整合性アルゴリズムを選択する必要があります。これらの暗号化基準では、ヌル以外のオプションを選択している場合でも、整合性ハッシュは使用されません。

ステップ 5 [OK] をクリックして変更を保存します。

サイト間 VPN 接続の確認

サイト間 VPN 接続を設定し、設定をデバイスに展開した後で、システムがリモート デバイスとのセキュリティ アソシエーションを確立することを確認します。

接続を確立できない場合は、デバイス CLI から **ping interface** *interface_name remote_ip_address* コマンドを使用して、VPNインターフェイスを介したリモートデバイスへのパスが存在することを確認します。設定したインターフェイスを介した接続が存在しない場合は、**interface** *interface_name* キーワードをオフにしたまま、接続が別のインターフェイス経由になっていないかどうかを判別します。接続に対して間違ったインターフェイスが選択されている可能性があります。保護されたネットワークに面したインターフェイスではなく、リモートデバイスに面したインターフェイスを選択する必要があります。

ネットワーク パスが存在する場合は、両方のエンドポイントで設定およびサポートされている IKE バージョンとキーを確認し、必要に応じて VPN 接続を調整します。アクセス制御または NAT ルールが接続をブロックしていないことを確認します。

手順

ステップ 1 デバイス CLI にログインします（CLI（コマンドライン インターフェイス）へのログイン （9 ページ）を参照）。

ステップ 2 **show ipsec sa** コマンドを使用して、IPSec セキュリティ アソシエーションが確立されていることを確認します。

ご使用のデバイス（**local addr**）とリモート ピア（**current_peer**）の間に VPN 接続が確立されているはずです。その接続を介してトラフィックを送信すると、パケット（pkts）数が増加します。アクセス リストには、接続のローカル ネットワークおよびリモート ネットワークが表示されます。

たとえば、次の出力は、IKEv2 接続を示しています。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

次の出力は、IKEv1 接続を示しています。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 077D72C9
      current inbound spi : AC146DEC

    inbound esp sas:
      spi: 0xAC146DEC (2887020012)
         SA State: active
```

```
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
        slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
        sa timing: remaining key lifetime (kB/sec): (3914999/28567)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x000007FF
    outbound esp sas:
      spi: 0x077D72C9 (125661897)
        SA State: active
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
        slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
        sa timing: remaining key lifetime (kB/sec): (3914999/28567)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

ステップ 3 **show isakmp sa** コマンドを使用して、IKE セキュリティ アソシエーションを確認します。

sa キーワードを使用せずに（または代わりに **stats** キーワードを使用して）このコマンドを使用すると、IKE 統計情報が表示されます。

たとえば、次の出力は、IKEv2 セキュリティ アソシエーションを示しています。

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify:
PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

次の出力は、IKEv1 セキュリティ アソシエーションを示しています。

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

```
There are no IKEv2 SAs
```

サイト間 VPN のモニタリング

サイト間 VPN 接続をモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。

- **show ipsec sa** は VPN セッション（セキュリティ アソシエーション）を表示します。これらの統計は **clear ipsec sa counters** コマンドを使用してリセットできます。
- **show ipsec** *keyword* は IPsec 運用データおよび統計情報を表示します。**show ipsec ?** と入力し、使用可能なキーワードを確認します。
- **show isakmp** は ISAKMP 運用データおよび統計情報を表示します。

サイト間 VPN の例

以下に、サイト間 VPN を設定する例を示します。

NAT からのサイト間 VPN トラフィックの除外

インターフェイスでサイト間 VPN 接続が定義されていて、かつそのインターフェイス向けの NAT ルールを指定している場合、NAT ルールから VPN 上のトラフィックを任意で除外できます。この操作は、VPN 接続のリモート エンドが内部アドレスを処理できる場合に行うと便利です。

VPN 接続を作成するときに、[NATを除外（NAT Exempt）] オプションを選択すると、ルールが自動的に作成されます。ただし、これはローカルで保護されたネットワークが単一のルーテッド インターフェイス（ブリッジ グループ メンバーではない）を介して接続されている場合のみ動作します。その代わりに、接続内のローカル ネットワークが複数のルーテッド インターフェイス、または 1 つ以上のブリッジ グループ メンバーの背後に存在する場合、NAT 免除ルールを手動で設定する必要があります。

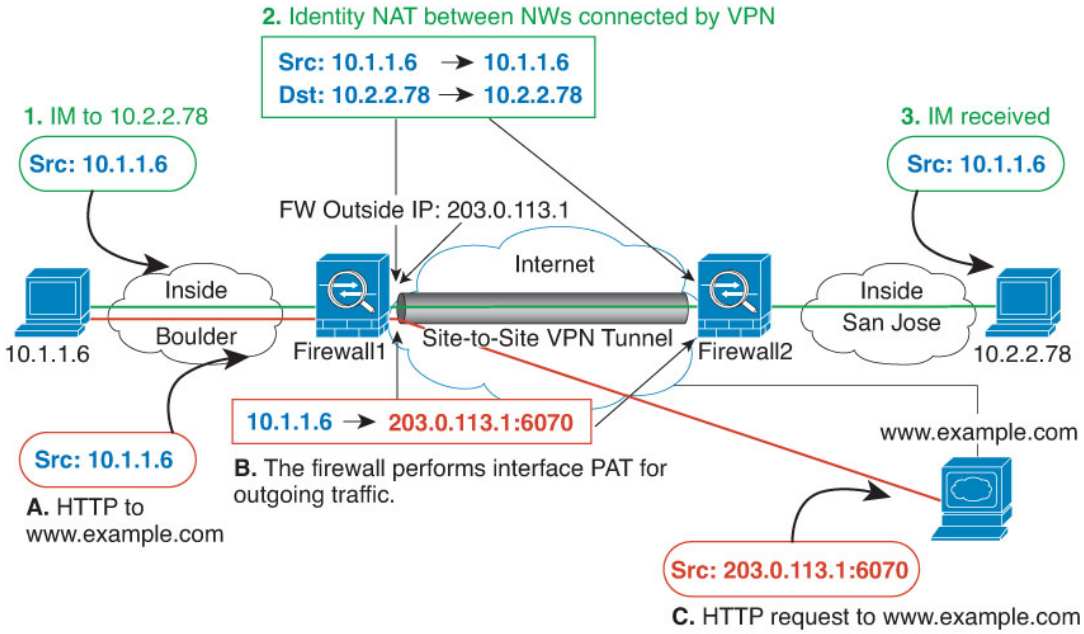
NAT ルールから VPN トラフィックを除外するには、宛先がリモート ネットワークのときにローカル トラフィックの手動アイデンティティ NAT ルールを作成します。次に、任意の宛先（インターネットなど）のトラフィックに NAT を適用します。ローカル ネットワークに複数のインターフェイスがある場合、各インターフェイスにルールを作成します。次の点も考慮してください。

- 接続内に複数のローカル ネットワークがある場合、ネットワークを定義するオブジェクトを保持するネットワーク オブジェクト グループを作成します。

- VPN に IPv4 ネットワークと IPv6 ネットワークの両方を含める場合、それぞれに個別のアイデンティティ NAT ルールを作成します。

次の例では、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 *51* : サイトツーサイト *VPN* のためのインターフェイス *PAT* およびアイデンティティ *NAT*



次の例は、Firewall1（ボールダー）の設定を示します。例では、内部インターフェイスがブリッジ グループであると仮定するため、各メンバー インターフェイスにルールを記述する必要があります。ルーティングされた内部インターフェイスが 1 つある場合も複数ある場合も、プロセスは同じです。

（注） この例では、IPv4 のみと仮定します。VPN に IPv6 ネットワークも含まれる場合、IPv6 にはパラレル ルールを作成します。IPv6 インターフェイス PAT は実装できないため、PAT を使用するには固有の IPv6 アドレスを持つホスト オブジェクトを作成する必要があることに注意してください。

手順

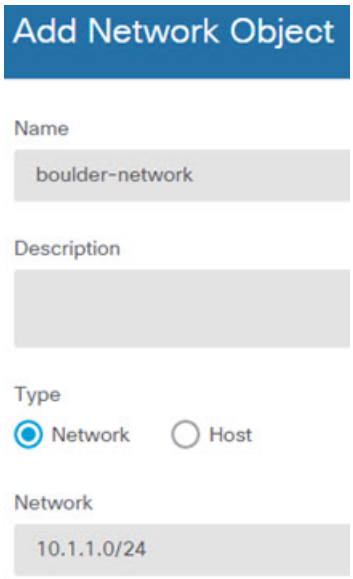
ステップ 1 さまざまなネットワークを定義するには、オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 目次から [ネットワーク（Network）] を選択し、[+] をクリックします。

c) ネットワーク内でボールダーを特定します。

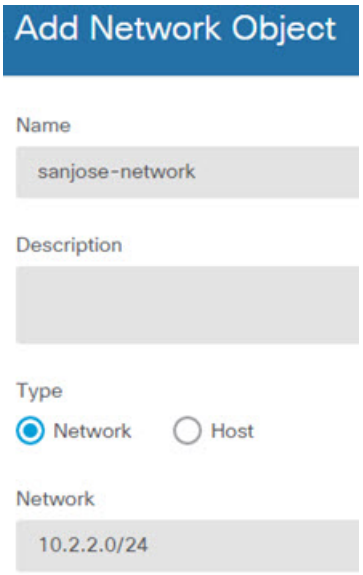
ネットワーク オブジェクトに名前を付け（boulder-network など）、[ネットワーク（Network）] を選択して、ネットワーク アドレス 10.1.1.0/24 を入力します。



d) [OK] をクリックします。

e) [+] をクリックしてサンノゼの内部ネットワークを定義します。

ネットワーク オブジェクトに名前を付け（sanjose-network など）、[ネットワーク（Network）] を選択して、ネットワーク アドレス 10.2.2.0/24 を入力します。



f) [OK] をクリックします。

ステップ 2 Firewall1（ボールダー）上で VPN 経由でサンノゼに向かう場合、ボールダー ネットワークの手動アイデンティティ NAT を設定します。

a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

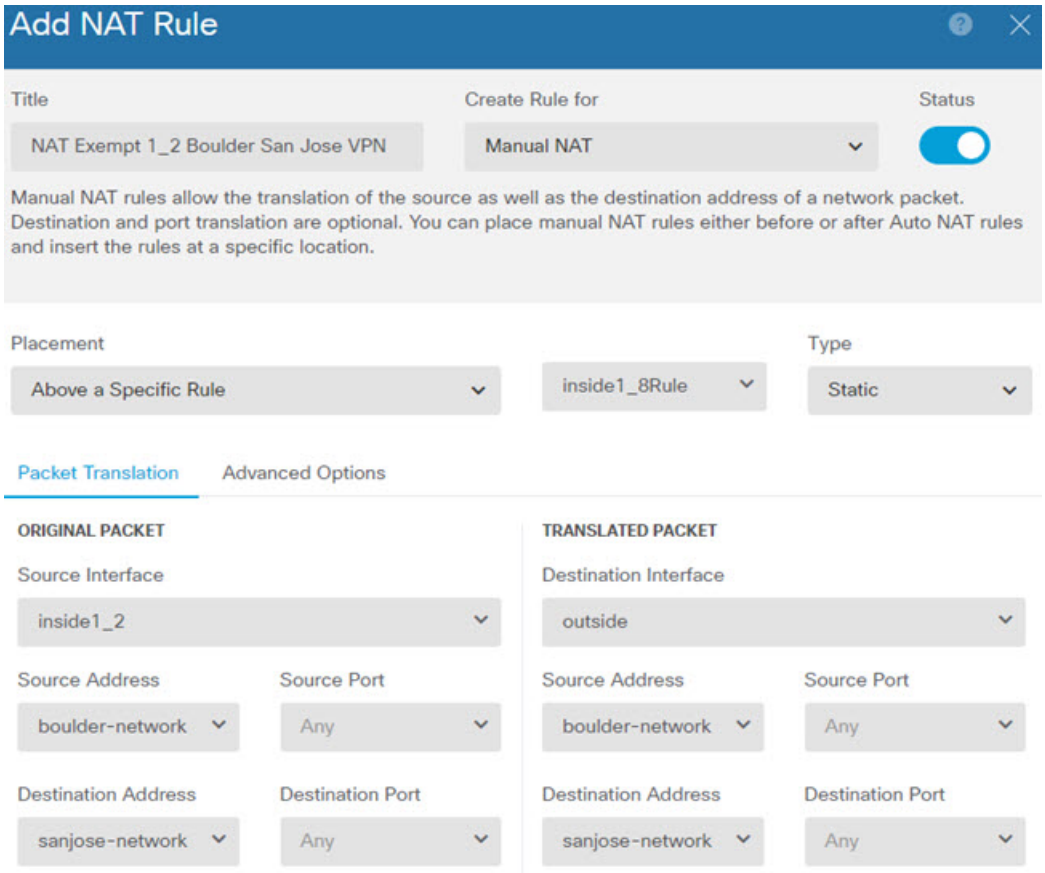
b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = NAT Exempt 1_2 Boulder San Jose VPN（または別の名前）。
- [ルールの作成対象（Create Rule For）] = 手動 NAT（Manual NAT）。
- [配置（Placement）] = [特定のルールの上（Above a Specific Rule）]。[自動NATの前に手動NAT（Manual NAT Before Auto NAT）] セクションの最初のルールを選択します。このルールが、宛先インターフェイスの一般的なインターフェイス PAT ルールの前に来ていることを確認してください。そうでないと、ルールが正しいトラフィックに適用されない場合があります。
- [タイプ（Type）] = [スタティック（Static）]
- [送信元インターフェイス（Source Interface）] = inside1_2。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元の発信元アドレス（Original Source Address）] = boulder-network のネットワーク オブジェクト（boulder-network network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = boulder-network のネットワーク オブジェクト（boulder-network network object）。
- [元の宛先アドレス（Original Destination Address）] = sanjose-network のネットワーク オブジェクト（sanjose-network network object）。

- [変換済みの宛先アドレス（Translated Destination Address）] = sanjose-network のネットワーク オブジェクト（sanjose-network network object）。

（注） 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート（Port）] フィールドはすべて空白のままにします。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。



d) [詳細（Advanced）] タブで [宛先インターフェイスでプロキシARPなし（Do not proxy ARP on Destination interface）] を選択します。

e) [OK] をクリックします。

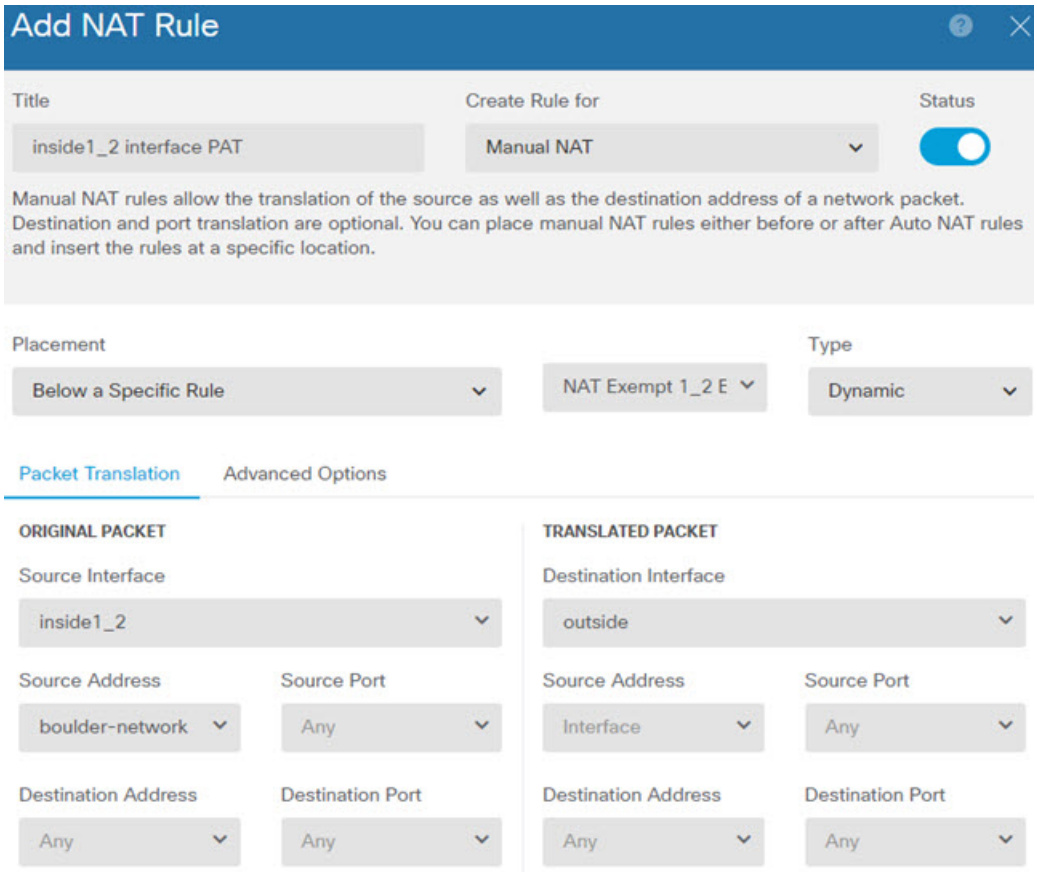
f) 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 3 Firewall1（ボールダー）上でボールダーの内部ネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

（注） これらは初期設定時にデフォルトで作成されるため、内部インターフェイスにはすでに IPv4 トラフィックをカバーするダイナミック インターフェイス PAT ルールがある可能性があります。ただし、この設定は説明を完結させるために示しています。この手順を完了する前に、内部インターフェイスとネットワークをカバーするルールがすでに存在していることを確認して、存在している場合はこの手順をスキップしてください。

a) [+] ボタンをクリックします。
b) 次のプロパティを設定します。

- [タイトル（Title）] = inside1_2 インターフェイス PAT（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = 手動 NAT（Manual NAT）。
- [配置（Placement）] = [特定のルールの下（Below a Specific Rule）]。[自動NATの前に手動NAT（Manual NAT Before Auto NAT）] セクションで、このインターフェイスのために先に作成したルールを選択します。このルールは任意の宛先アドレスに適用されるため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動NATの前にNAT ルール（NAT Rules Before Auto NAT）] セクションの最後に配置されますが、これでも問題ありません。
- [タイプ（Type）] = [ダイナミック（Dynamic）]
- [送信元インターフェイス（Source Interface）] = inside1_2。
- [宛先インターフェイス（Destination Interface）] = [外部（outside）]
- [元の発信元アドレス（Original Source Address）] = boulder-network のネットワーク オブジェクト（boulder-network network object）。
- [変換済み発信元アドレス（Translated Source Address）] = [インターフェイス（Interface）]。このオプションは、宛先インターフェイスを使用するインターフェイス PAT を設定します。
- [元の宛先アドレス（Original Destination Address）] = 任意（any）。
- [変換済みの宛先アドレス（Original Destination Address）] = 任意（any）。



c) [OK] をクリックします。

d) 他の内部インターフェイスごとに、同等のルールを作成するプロセスを繰り返します。

ステップ 4 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 5 Firewall2（サンノゼ）の管理を行っている場合、そのデバイスに同様のルールを設定できます。

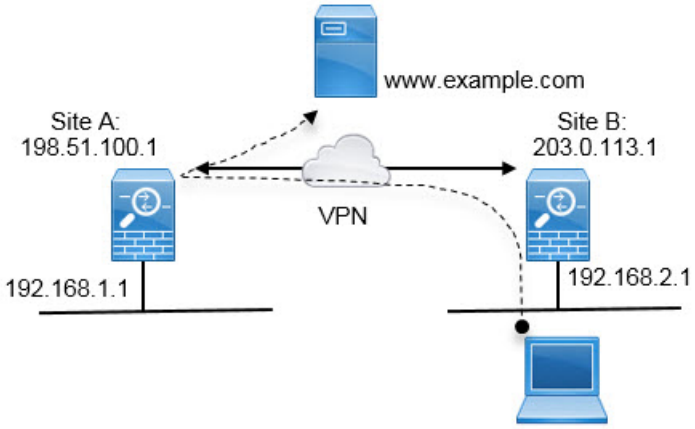
- 手動アイデンティティ NAT ルールは、宛先が boulder-network の場合は sanjose-network 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイス オブジェクトを作成します。

- 手動ダイナミック インターフェイス PAT ルールは、宛先が「任意」の場合は sanjose-network 向けになります。

外部インターフェイスで外部のサイト間VPNユーザーにインターネット アクセスを提供する方法（ヘア ピニング）

サイト間 VPN では、リモート ネットワーク上のユーザに自分のデバイスを介してインターネットにアクセスさせたい場合があります。ただし、インターネットに接続している同一インターフェイス（外部インターフェイス）上のデバイスにリモート ユーザーがアクセスしているため、インターネット トラフィックが外部インターフェイスの外側からそのまま返される必要があります。この手法はヘア ピニングと呼ばれる場合もあります。

次の図は例を示しています。198.51.100.1（メイン サイトのサイト A）と 203.0.113.1（リモート サイトのサイト B）間にサイト間 VPN トンネルが設定されています。リモート サイトの内部ネットワーク（192.168.2.0/24）からのユーザ トラフィックはすべて VPN を通過します。そのため、内部ネットワークのユーザがインターネット上のサーバ（www.example.com など）にアクセスする場合、接続は最初に VPN を通過し、その後 198.51.100.1 インターフェイスからインターネットにルートバックされます。



次の手順では、このサービスの設定方法について説明します。VPN トンネルの両方のエンドポイントを設定する必要があります。

始める前に

この手順では、VPN トラフィックをアクセス コントロール ポリシーの対象とする、VPN トラフィックを許可するためのデフォルト設定を使用していると仮定します。実行中のコンフィギュレーションでは、これは **no sysopt connection permit-vpn** コマンドで表されます。代わりに FlexConfig を介して **sysopt connection permit-vpn** を有効にした場合、または RA VPN 接続プロファイルで [復号されたトラフィックでアクセス制御ポリシーをバイパスする（Bypass Access Control policy for decrypted traffic）] オプションを選択することで、アクセス制御ルールを設定する手順は不要になります。

手順

ステップ 1 （サイト A、メイン サイト）リモート サイト B へのサイト間 VPN 接続を設定します。

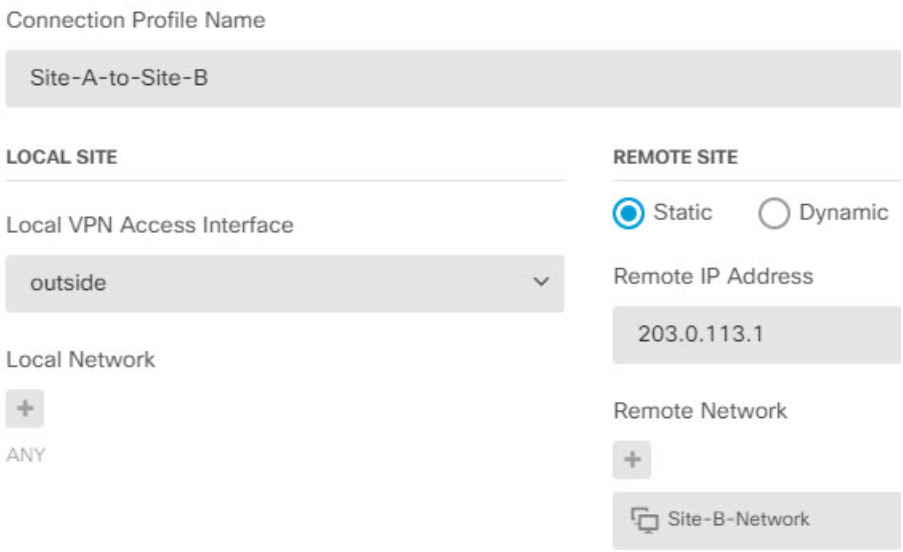
a) [デバイス（Device）] をクリックし、[サイト間VPN（Site-to-Site VPN）] グループで [設定の表示（View Configuration）] をクリックします。

b) [+] をクリックして新しい接続を追加します。

c) 次のようにエンドポイントを定義し、[次へ（Next）] をクリックします。

- [接続プロファイル名（Connection Profile Name）]：わかりやすい接続の名前を付けます。例、Connection Profile Name。
- [ローカルVPNアクセスインターフェイス（Local VPN Access Interface）]：外部インターフェイスを選択します。
- [ローカルネットワーク（Local Network）]：デフォルトの [任意（Any）] のままにします。
- [リモートIPアドレス（Remote IP Address）]：リモート ピアの外部インターフェイスの IP アドレスを入力します。この例では、203.0.113.1 です。
- [リモートネットワーク（Remote Network）]：[+] をクリックして、リモート ピアの保護ネットワークを定義するネットワーク オブジェクトを選択します。この例では 192.168.2.0/24 です。[ネットワークの新規作成（Create New Network）] をクリックしてすぐにオブジェクトを作成できます。

次に、最初の手順の状況を図で示します。

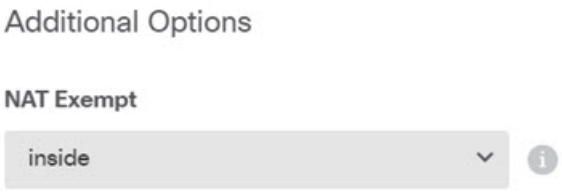


d) プライバシー ポリシーを定義し、[次へ（Next）] をクリックします。

- [IKEポリシー（IKE Policy）]：IKE の設定はヘア ピニングに影響を与えません。セキュリティのニーズに合わせて IKE バージョン、ポリシー、およびプロポーザルを選択し

ます。入力するローカルとリモートの事前共有キーはメモしてください。リモート ピアの設定時に必要になります。

- [NAT免除（NAT Exempt）]：[内部（inside）] インターフェイスを選択します。



- [Perfect Forward SecrecyのDiffie Helmanグループ（Diffie Helman Group for Perfect Forward Secrecy）]：この設定はヘア ピニングに影響しません。必要に応じて設定します。

e) [終了（Finish）] をクリックします。

接続の概要がクリップボードにコピーされます。接続の概要は、テキストファイルやその他のドキュメントに貼り付けて、リモート ピアの設定に役立てることができます。

ステップ 2 （サイト A、メイン サイト）外部インターフェイスから送信されたすべての接続を外部 IP アドレス（インターフェイス PAT）のポートに変換するよう NAT ルールを設定します。

デバイスの初期設定を完了すると、InsideOutsideNatRule という名前の NAT ルールが作成されます。このルールは、外部インターフェイス経由でデバイスを抜ける任意のインターフェイスから、インターフェイス PAT を IPv4 トラフィックに充当します。外部インターフェイスは「任意の」送信元インターフェイスに含まれるため、必要なルールは、編集または削除していない限り、すでに存在しています。

次の手順で、必要なルールを作成する方法を説明します。

a) **[ポリシー（Policies）]** > **[NAT]** をクリックします。

b) 次のいずれかを実行します。

- InsideOutsideNatRule を編集するには、[アクション（Action）] 列にマウス オーバーし、[編集（edit）] アイコン（）をクリックします。
- ルールを新規作成するには、[+] ボタンをクリックします。

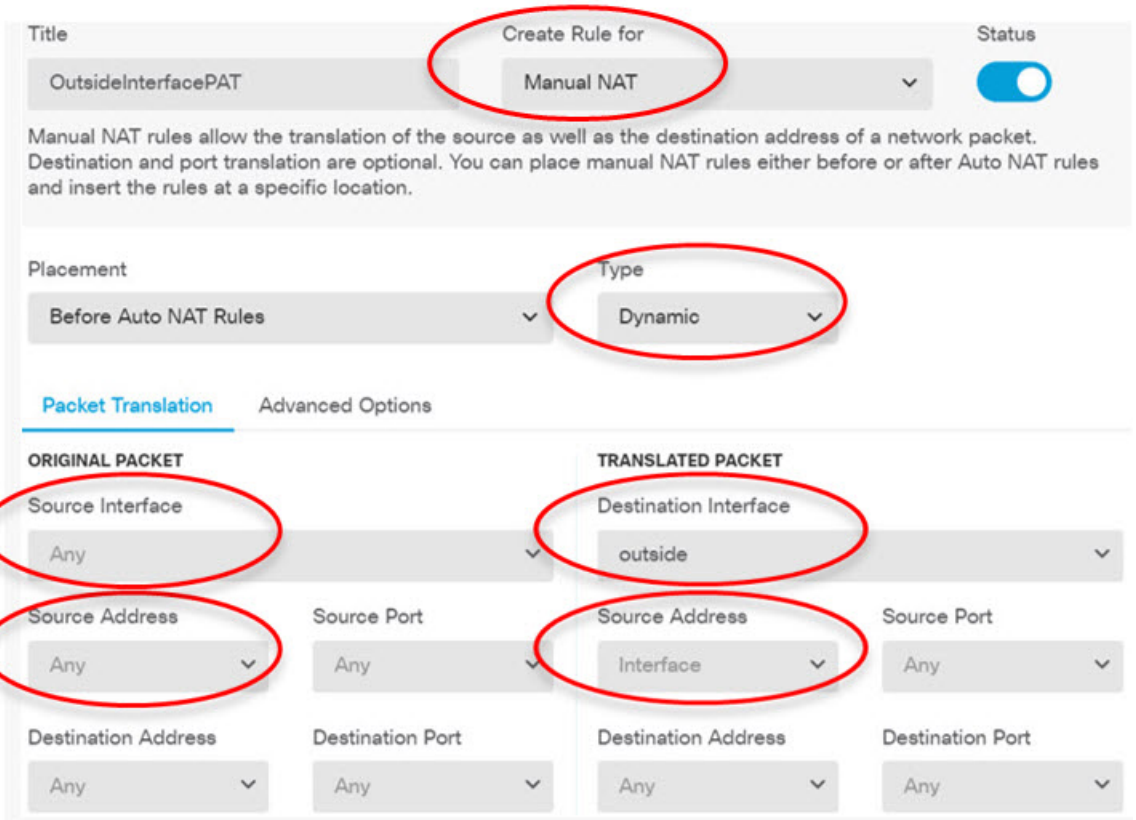
c) 次のプロパティを使用してルールを設定します。

- [タイトル（Title）]：新しいルールのわかりやすい名前をスペースを含めず入力します。たとえば、OutsideInterfacePAT と入力します。
- [ルールの作成先（Create Rule For）]：[手動NAT（Manual NAT）]。
- [配置（Placement）]：[自動NATルールの前（Before Auto NAT Rules）]（デフォルト）。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [元のパケット（Original Packet）]：[送信元アドレス（Source Address）] で [任意（Any）] または [any-ipv4] を選択します。[送信元インターフェイス（Source Interface）] で、[任

意（Any）]（デフォルト）を選択していることを確認します。[元のパケット（Original Packet）] の他のすべてのオプションは、デフォルトの [任意（Any）] のままにします。

- [変換後のパケット（Translated Packet）] : [宛先インターフェイス （Destination Interface）] で、[外部（outside）] を選択します。[変換後のアドレス（Translated Address）] で、[インターフェイス（Interface）] を選択します。[変換後のパケット（Translated Packet）] の他のすべてのオプションは、デフォルトの [任意（Any）] のままにします。

次の図は、発信元アドレスに [任意（Any）] を選択したシンプルな例を示しています。



d) [OK] をクリックします。

ステップ 3 （サイト A、メイン サイト）サイト B の保護ネットワークへのアクセスを許可するアクセス制御ルールを設定します。

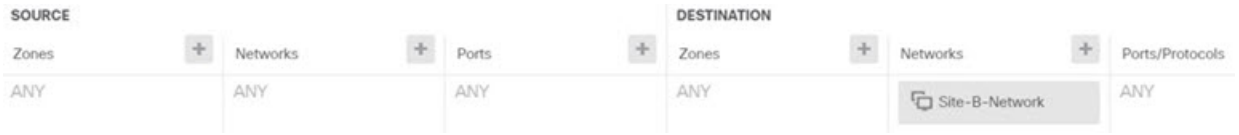
VPN 接続を作成するだけで、VPN 上のトラフィックが自動的に許可されるわけではありません。使用しているアクセス コントロール ポリシーがリモート ネットワークへのトラフィックを許可している必要があります。

次の手順では、リモート ネットワーク用の固有ルールの追加方法を示します。追加のルールが必要かどうかは、既存のルールによって異なります。

a) **[ポリシー（Policies）] > [アクセス制御（Access Control）]** をクリックします。

b) [+] をクリックして新しいルールを作成します。
c) 次のプロパティを使用してルールを設定します。

- [順序（Order）]：ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。デフォルトでは、ルールはポリシーの最後に追加されます。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。
- [タイトル（Title）]：スペースを含めずにわかりやすい名前を入力します。例、Site-B-Network。
- [アクション（Action）]：[許可（Allow）]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼（Trust）] を選択できます。
- [送信元または宛先（Source/Destination）] タブ：**[宛先（Destination）]** > **[ネットワーク（Network）]** で、リモート ネットワークの VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先（Source and Destination）] の他のすべてのオプションについては、デフォルトの [任意（Any）] のままにします。



- [アプリケーション（Application）]、[URL]、および [ユーザー（Users）] タブ：これらのタブではデフォルトの設定（何も選択しない）のままにします。
- [侵入（Intrusion）]、[ファイル（File）] タブ：オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング（Logging）] タブ：オプションで接続のロギングを有効にできます。

d) [OK] をクリックします。

ステップ 4 （サイト A、メイン サイト）変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。ウィンドウをアクティブのままにすると、展開が正常に終了した後、保留中の変更はないことが表示されます。

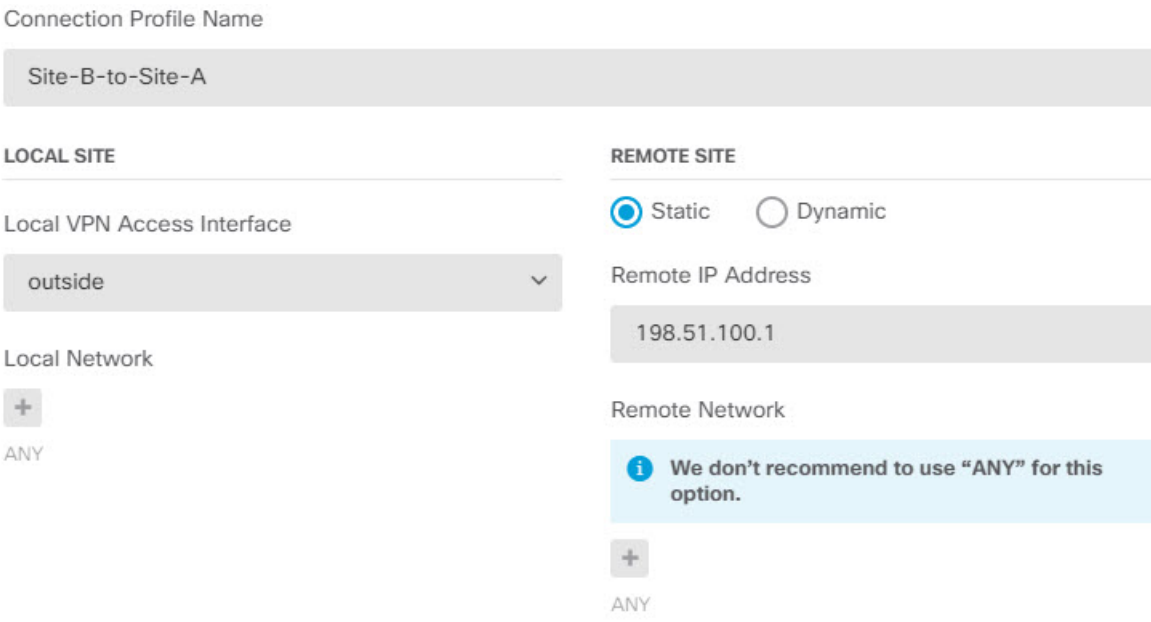
ステップ 5 （サイト B、リモート サイト）リモート サイトのデバイスにログインし、サイト A へのサイト間 VPN 接続を設定します。

サイト A のデバイス設定から取得した接続の概要を使用して、サイト B 側の接続を設定します。

a) [デバイス（Device）] をクリックし、[サイト間VPN（Site-to-Site VPN）] グループで [設定の表示（View Configuration）] をクリックします。
b) [+] をクリックして新しい接続を追加します。
c) 次のようにエンドポイントを定義し、[次へ（Next）] をクリックします。

- [接続プロファイル名（Connection Profile Name）]：わかりやすい接続の名前を付けます。例、Site-B-to-Site-A。
- [ローカルVPNアクセスインターフェイス（Local VPN Access Interface）]：外部インターフェイスを選択します。
- [ローカルネットワーク（Local Network）]：[+] をクリックして、ローカルの保護ネットワークを定義するネットワーク オブジェクトを選択します。この例では192.168.2.0/24です。[ネットワークの新規作成（Create New Network）] をクリックしてすぐにオブジェクトを作成できます。
- [リモートIPアドレス（Remote IP Address）]：メイン サイトの外部インターフェイスの IP アドレスを入力します。この例では、198.51.100.1 です。
- [リモートネットワーク（Remote Network）]：デフォルトの [任意（Any）] のままにします。警告は無視します。この使用例には関係ありません。

次に、最初の手順の状況を図で示します。

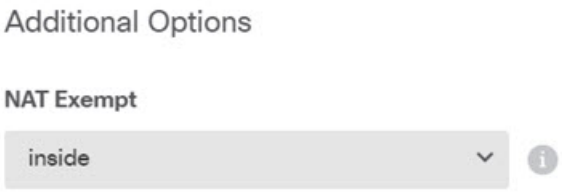


d) プライバシー ポリシーを定義し、[次へ（Next）] をクリックします。

- [IKEポリシー（IKE Policy）]：IKE の設定はヘア ピニングに影響を与えません。サイト A の VPN 接続の終端と同じオプションまたは互換性のあるオプションを設定します。事前共有キーは正しく設定する必要があります。サイト A デバイスに設定されて

いる（IKEv2 の）ローカル キーとリモート キーを切り替えます。IKEv1 の場合、キーは 1 つだけで、両方のピアで同一である必要があります。

- [NAT免除（NAT Exempt）]：[内部（inside）] インターフェイスを選択します。



- [Perfect Forward SecrecyのDiffie Helmanグループ（Diffie Helman Group for Perfect Forward Secrecy）]：この設定はヘア ピニングに影響しません。サイト A の VPN 接続の終端で使用されている設定と照合します。

e) [終了（Finish）] をクリックします。

ステップ 6 （サイト B、リモート サイト）保護ネットワークのすべての NAT ルールを削除し、そのサイトからのトラフィックがすべて VPN トンネルを通過するようにします。

サイト A のデバイスではアドレス変換が行われるため、このデバイスで NAT を実行する必要はありません。ただし、個別の状況を確認してください。複数の内部ネットワークがあり、そのすべてがこの VPN 接続に参加しているわけではない場合は、それらのネットワークに必要な NAT ルールを削除しないでください。

a) **[ポリシー（Policies）]** > **[NAT]** をクリックします。
b) 次のいずれかを実行します。

- ルールを削除するには、[アクション（Action）] 列にマウス オーバーして、[削除（delete）] アイコン（）をクリックします。
- ルールを編集して、保護ネットワークに適用されないようにするには、[アクション（Action）] 列にマウス オーバーして、[編集（edit）] アイコン（）をクリックします。

ステップ 7 （サイト B、リモート サイト）保護ネットワークからインターネットへのアクセスを許可するアクセス制御ルールを設定します。

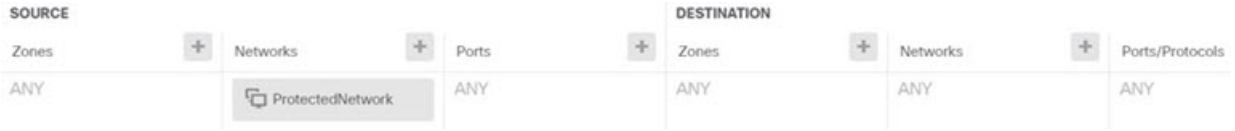
次の例では、保護ネットワークから任意の宛先へのトラフィックが許可されます。これは独自の要件に合わせて調整できます。不要なトラフィックを除外するブロック ルールをルールの前に置くことができます。別のオプションとして、サイト A のデバイスにブロック ルールを設定することもできます。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** をクリックします。
b) [+] をクリックして新しいルールを作成します。
c) 次のプロパティを使用してルールを設定します。

- [順序（Order）]：ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。デフォルトでは、ルールはポリシーの最後に追加

されます。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。

- [タイトル（Title）]：スペースを含めずにわかりやすい名前を入力します。例、Protected-Network-to-Any。
- [アクション（Action）]：[許可（Allow）]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼（Trust）] を選択できます。
- [送信元または宛先（Source/Destination）] タブ：**[送信元（Source）]** > **[ネットワーク（Network）]** で、ローカル ネットワークの VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先（Source and Destination）] の他のすべてのオプションについては、デフォルトの [任意（Any）] のままにします。



- [アプリケーション（Application）]、[URL]、および [ユーザー（Users）] タブ：これらのタブではデフォルトの設定（何も選択しない）のままにします。
- [侵入（Intrusion）]、[ファイル（File）] タブ：オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング（Logging）] タブ：オプションで接続のロギングを有効にできます。

d) [OK] をクリックします。

ステップ 8 （サイト B、リモート サイト）変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックして、展開が完了するまで待ちます。

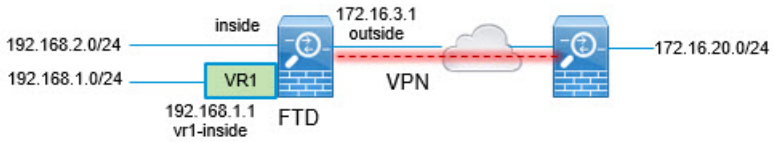
展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。ウィンドウをアクティブのままにすると、展開が正常に終了した後、保留中の変更はないことが表示されます。

サイト間 VPN における複数の仮想ルータのネットワークからのトラフィックを保護する方法

1 つのデバイスに複数の仮想ルータを設定する場合には、グローバル仮想ルータでサイト間 VPN を設定する必要があります。カスタム仮想ルータに割り当てられているインターフェイスにサイト間 VPN を設定することはできません。

仮想ルータのルーティングテーブルはそれぞれ異なるため、サイト間 VPN を介して、カスタム仮想ルータ内でホストされているネットワークとの接続を保護する必要がある場合には、スタティックルートを作成する必要があります。また、前述の付加的なネットワークが含まれるように、サイト間 VPN 接続を更新する必要もあります。

次の例を考えてみます。この例では、サイト間VPNは172.16.3.1の外部インターフェイスで定義されます。この VPN には、内部インターフェイスがグローバル仮想ルータの一部でもあるため、追加の設定なしで内部ネットワーク 192.168.2.0/24 を含めることができます。ただし、VR1 仮想ルータの一部である 192.168.1.0/24 ネットワークにサイト間 VPN サービスを提供する必要がある場合には、双方向のスタティックルートを設定して、このネットワークをサイト間 VPN 設定に追加する必要があります。



始める前に

この例では、すでに 192.168.2.0/24 ローカルネットワークと 172.16.20.0/24 外部ネットワークの間にサイト間 VPN を設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータから VR1 へのルートリークを設定します。

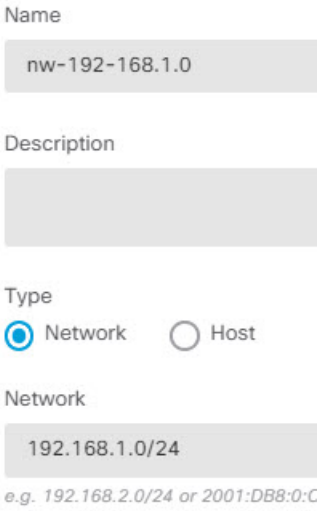
このルートにより、サイト間 VPN の外部（リモート）エンドによって保護されたエンドポイントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできます。

a) **[デバイス（Device）] > [ルーティング（Routing）] > [設定の表示（View Configuration）]** の順に選択します。

b) グローバル仮想ルータの表示アイコン（）をクリックします。

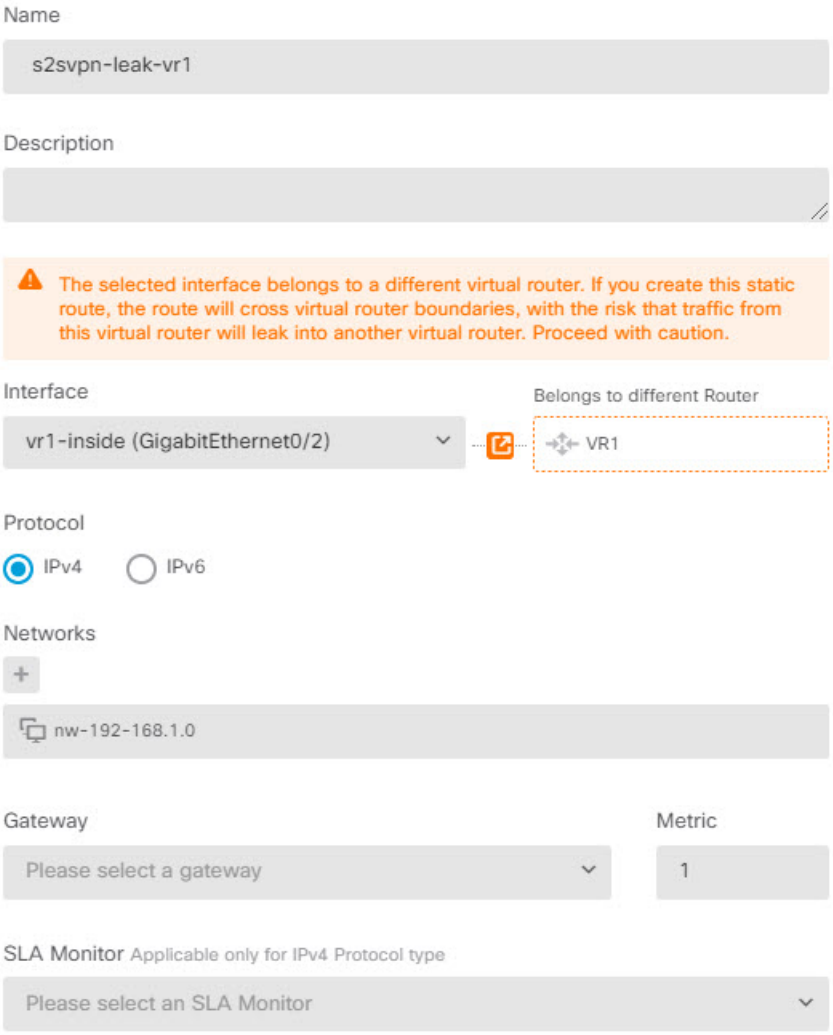
c) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：任意の名前（**s2svpn-leak-vr1** など）を付けることができます。
- [インターフェイス（Interface）]：**vr1-inside** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]：192.168.1.0/24 ネットワークを定義するオブジェクトを選択します。必要な場合には、[新しいネットワークの作成（Create New Network）] をクリックしてオブジェクトを作成します。



- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



d) [OK] をクリック

ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

このルートにより、192.168.1.0/24 ネットワーク上のエンドポイントは、サイト間 VPN トンネルを通過する接続を開始できます。この例では、リモートエンドポイントが 172.16.20.0/24 ネットワークを保護しています。

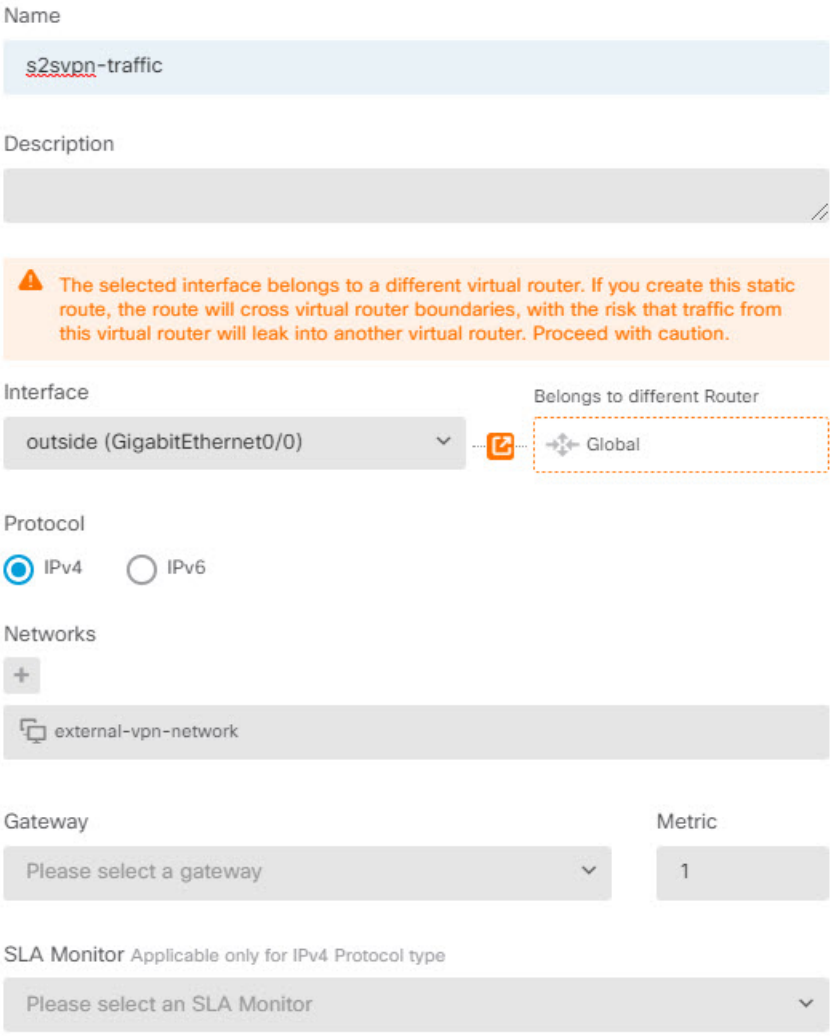
a) 仮想ルータのドロップダウンリストから [VR1] を選択して、VR1 設定に切り替えます。

b) VR1 ルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：任意の名前（**s2svpn-traffic** など）を付けることができます。
- [インターフェイス（Interface）]：**outside** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。

- [ネットワーク（Networks）]：リモートエンドポイントの保護されたネットワークのために作成したオブジェクトを選択します（**external-vpn-network** など）。
- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



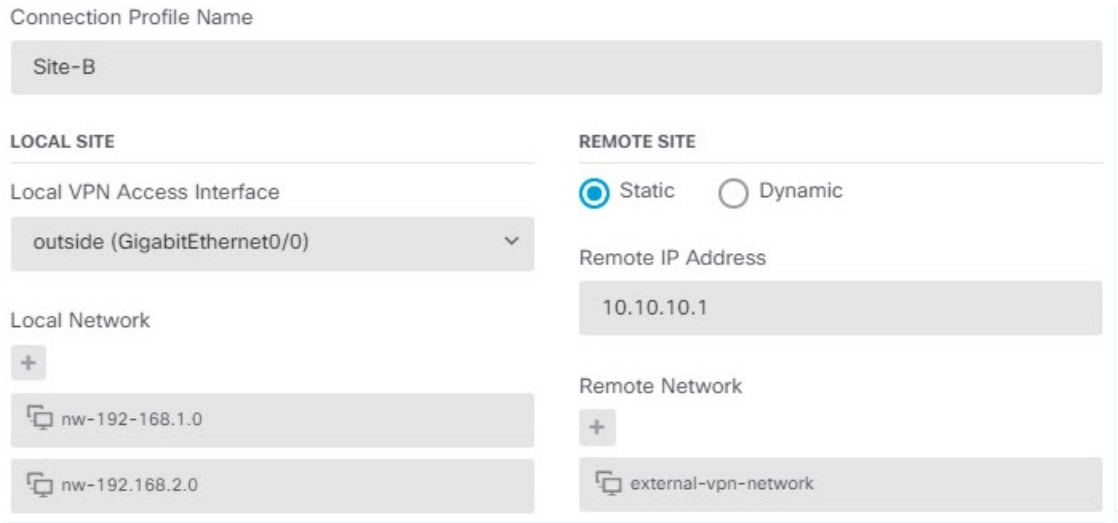
c) [OK] をクリック

ステップ 3 192.168.1.0/24 ネットワークをサイト間 VPN 接続プロファイルに追加します。

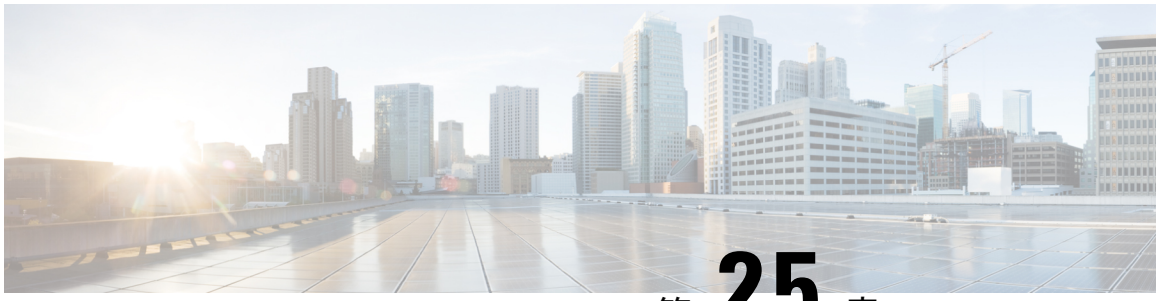
a) **[デバイス（Device）] > [サイト間 VPN（Site-to-Site VPN）] > [設定の表示（View Configuration）]**の順に選択します。

b) 接続プロファイルの編集アイコン（）をクリックします。

c) ウィザードの最初のページで、[ローカルネットワーク（Local Network）] の下の [+] をクリックして、192.168.1.0/24 ネットワークのオブジェクトを追加します。



d) ウィザードを完了します。



第 25 章

リモート アクセス VPN

リモートアクセス 仮想プライベート ネットワーク（VPN）では、各ユーザーがインターネットに接続されたコンピュータまたはその他のサポート対象の iOS または Android デバイスを使用して、離れた場所からネットワークに接続できます。これにより、モバイル ワーカーが各自のホーム ネットワークや公共の Wi-Fi ネットワークなどから接続できるようになります。

ここでは、ネットワークのリモート アクセス VPN を設定する方法について説明します。

リモート アクセス VPN の概要

Device Manager では、セキュアクライアントソフトウェアを使用して SSL 経由でリモートアクセス VPN を設定できます。

セキュアクライアントが Threat Defense デバイスと SSL VPN 接続をネゴシエートする際、Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。クライアントおよび Threat Defense デバイスは、使用する TLS/DTLS バージョンをネゴシエートします。DTLS はクライアントがサポートする場合に使用されます。

デバイス モデル別の同時 VPN セッションの最大数

デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この制限は、システム パフォーマンスが許容できないレベルに低

下しないように設計されています。これらの制限は、キャパシティ プランニングに使用します。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000
Secure Firewall 3140	20,000
Firepower 4100 シリーズ、すべてのモデル	10,000
Firepower 9300 appliance、すべてのモデル	20,000
Threat Defense Virtual：FTDv5	50
Threat Defense Virtual：FTDv10、FTDv20、FTDv30	250
Threat Defense Virtual：FTDv50	750
Threat Defense Virtual：FTDv100	10,000
ISA 3000	25

セキュアクライアント ソフトウェアのダウンロード

リモートアクセス VPN を設定するには、セキュアクライアント ソフトウェアをワークステーションにダウンロードする必要があります。VPN を定義するときに、これらのパッケージをアップロードする必要があります。

最新の機能、バグ修正、セキュリティ パッチを確保するには、最新の セキュアクライアント バージョンをダウンロードする必要があります。脅威に対する防御デバイスのパッケージは定期的に更新してください。

（注） Windows、Mac、Linux の各オペレーティングシステムごとに 1 つの セキュアクライアント パッケージをアップロードできます。1 つの OS タイプに対して複数のバージョンをアップロードすることはできません。

セキュアクライアント ソフトウェアパッケージは software.cisco.com から取得します。クライアントの「フル インストール パッケージ」バージョンをダウンロードしてください。

セキュアクライアント ソフトウェアのインストール方法

VPN 接続を完了するには、ユーザーは セキュアクライアント ソフトウェアをインストールする必要があります。既存のソフトウェア配布方式を使用して、ソフトウェアを直接インストールできます。または、Threat Defense デバイスから セキュアクライアントを直接インストールすることもできます。

ソフトウェアをインストールするには、ユーザにワークステーションでの管理者権限が必要です。

セキュアクライアントがすでにインストールされている場合、新しい セキュアクライアント バージョンがアップロードされると、ユーザーが次に VPN 接続を行った際、新しいバージョンが セキュアクライアント によって検出され、更新されたクライアント ソフトウェアのダウンロードとインストールを指示するメッセージが自動的に表示されます。この自動化により、ソフトウェアの配布が容易になります。

ソフトウェアの最初のインストールを Threat Defense デバイスからユーザーに行ってもらう場合、以下の手順を実行するようにユーザーに指示します。

（注） Android および iOS のユーザーは、適切な App Store から セキュアクライアント をダウンロードする必要があります。

手順

ステップ 1 Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。

このインターフェイスは、リモート アクセス VPN を設定する際に指定します。ログインを指示するメッセージがユーザに示されます。

リモートアクセス VPN 接続用のポートを変更した場合、ユーザーは URL にカスタムポートを含める必要があります。たとえば、ポートを 4443 に変更した場合は、https://ravpn.example.com:4443 のような URL にします。

ステップ 2 サイトにログインします。

ユーザは、リモート アクセス VPN 用に設定されたディレクトリ サーバを使用して認証されます。続行するには、ログインが正常に行われる必要があります。

ログインが成功すると、システムは、必要となるセキュアクライアントのバージョンがインストールされているかを確認します。セキュアクライアントがユーザーのコンピュータにないか、下位のバージョンである場合、システムは自動的に セキュアクライアント ソフトウェアのインストールを開始します。

インストールが終了すると、セキュアクライアント がリモートアクセス VPN 接続を完了します。

RADIUS およびグループ ポリシーを使用したユーザーの権限および属性の制御

外部 RADIUS サーバーまたは 脅威に対する防御 デバイスで定義されているグループポリシーから、RA VPN 接続にユーザーの認可属性（ユーザーの権利または権限とも呼ばれる）を適用できます。脅威に対する防御デバイスがグループポリシーに設定されている属性と競合する外部 AAA サーバーから属性を受信した場合は、AAA サーバーからの属性が常に優先されます。

脅威に対する防御 デバイスは次の順序で属性を適用します。

1. AAA サーバー上で定義されたユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。
2. 脅威に対する防御デバイス上で設定されているグループポリシー：RADIUS サーバーからユーザーの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、脅威に対する防御デバイスはそのユーザーを同じ名前のグループポリシーに入れて、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。
3. 接続プロファイルによって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。脅威に対する防御デバイスに接続するすべてのユーザーは、最初にこのグループに所属します。このグループでは、AAA サーバーから返されるユーザー属性、またはユーザーに割り当てられたグループポリシーにはない属性が定義されています。

Threat Defense デバイスは、ベンダー ID 3076 の RADIUS 属性をサポートします。使用する RADIUS サーバーにこれらの属性が定義されていない場合は、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。

次のトピックでは、サポートされている属性値について、値がRADIUSサーバーで定義されるかどうか、またはRADIUSサーバーにシステムが送信する値であるかどうかに基づいて説明します。

RADIUS サーバーに送信された属性

RADIUS 属性 146 および 150 は、認証および許可の要求のために 脅威に対する防御 デバイスからRADIUSサーバーに送信されます。次の属性はすべて、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 脅威に対する防御 デバイスから RADIUS サーバーに送信されます。

表 *14 : Threat Defense* から *RADIUS* に送信される属性

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
クライアント タイプ（Client Type）	150	整数	シングル	VPNに接続しているクライアントのタイプは次のとおりです。 2 = セキュアクライアント SSL VPN
セッション タイプ	151	整数	シングル	接続の種類： 1 = セキュアクライアント SSL VPN
Tunnel Group Name	146	文字列	シングル	脅威に対する防御デバイスで定義されているセッションの確立に使用された接続プロファイルの名前。名前には 1 ～ 253 文字を使用できます。

RADIUS サーバーから受信した属性

次のユーザー認可属性が RADIUS サーバーから 脅威に対する防御 デバイスに送信されます。

表 *15 :* 送信される *RADIUS* 属性 *Threat Defense*

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	アクセスリスト属性の両方が、脅威に対する防御デバイスで設定されている ACL の名前を使用します。スマート CLI 拡張アクセス リストのオブジェクト タイプを使用して、これらの ACL を作成します（**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Object）]** を選択します）。 これらの ACL は、着信（脅威に対する防御 デバイスに入るトラフィック）または発信（脅威に対する防御デバイスから出るトラフィック）方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	
Address-Pools	217	文字列	シングル	脅威に対する防御 デバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[Objects] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザーがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザーがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されます。
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の [Group Policy] ページでグループポリシーを作成する必要があります。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;
Simultaneous-Logins	2	整数	シングル	ユーザーが確立を許可されている個別の同時接続数。0 ～ 2147483647。
VLAN	140	整数	シングル	ユーザーの接続を制限する VLAN。0 ～ 4094。脅威に対する防御デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

二要素認証

RA VPNの二要素認証を設定できます。二要素認証を使用する場合、ユーザーはユーザー名とスタティックパスワードに加えて、RSA トークンや Duo パスコードなどの追加項目を指定する必要があります。二要素認証が 2 番目の認証ソースを使用することと異なるのは、1 つの認証ソースで2つの要素が設定され、RSA/Duoサーバーとの関係がプライマリ認証ソースに関連付けられている点です。Duo LDAPは例外で、Duo LDAP サーバーをセカンダリ認証ソースとして設定します。

システムは、2 番目の要素のためにモバイルにプッシュされる RSA トークンと Duo パスコードを、ニ要素認証プロセスの最初の要素としてのRADIUSサーバーまたはADサーバーと組み合わせることでテストされています。

RSA 二要素認証

次のいずれかのアプローチを使用してRSAを設定できます。RSA側の設定の詳細については、RSA のマニュアルを参照してください。

- Device Manager で RADIUS サーバーとして RSA サーバーを直接定義し、RA VPN のプライマリ認証ソースとしてサーバーを使用します。

  このアプローチを使用する場合、ユーザーはRSA RADIUSサーバーで設定されているユーザー名を使用して認証する必要があります。また、パスワードとトークンをカンマで区切り（*password,token*）、パスワードと 1 回限りの一時的な RSA トークンを連結します。

  この設定では、認証サービスを提供するために（Cisco ISE で供給されるような）個別の RADIUS サーバーを使用することが一般的です。2 番目の RADIUS サーバーを認証サーバーとして設定し、必要に応じてアカウンティング サーバーとしても設定します。

- RSA サーバーを、直接統合をサポートする RADIUS または AD サーバーと統合し、プライマリ認証ソースとして非 RSA RADIUS または AD サーバーを使用するように RA VPN を設定します。この場合、RADIUS/ADサーバーはRSA-SDIを使用して、クライアントと RSA サーバー間の二要素認証を委任およびオーケストレーションします。

  このアプローチを使用する場合、ユーザーは非 RSA RADIUS または AD サーバーで設定されているユーザー名を使用して認証する必要があります。また、パスワードとトークンをカンマで区切り（*password,token*）、パスワードと 1 回限りの一時的な RSA トークンを連結します。

  この設定では、RSA 以外の RADIUS サーバーを認証サーバーとして設定し、必要に応じてアカウンティング サーバーとしても設定します。

RADIUS を使用した Duo 二要素認証

Duo RADIUS サーバーはプライマリ認証ソースとして設定できます。このアプローチでは、Duo RADIUS 認証プロキシを使用します。

Duo の設定手順の詳細については、https://duo.com/docs/cisco-firepower を参照してください。

その後、最初の認証要素として別の RADIUS サーバー（または AD サーバー）を使用し、2 番目の要素として Duo クラウド サービスを使用するため、プロキシ サーバー宛の認証要求を転送するように Duo を設定します。

このアプローチを使用する場合、ユーザーは、Duo 認証プロキシおよび関連する RADIUS/AD サーバーの両方で設定されているユーザー名と、RADIUS/AD サーバーで設定されたユーザー名のパスワード（その後に次のいずれかの Duo コードが続く）を使用して認証する必要があります。

- *Duo-passcode*。*my-password*,**12345** など
- **push**。たとえば、*my-password*,**push** など。**push** は、ユーザーによるインストールと登録が完了している Duo モバイルアプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- **sms**：たとえば、*my-password*,**sms** など。**sms** は、ユーザーのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。**sms** を使用すると、ユーザーの認証試行は失敗します。ユーザーは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。
- **phone**：*my-password*,**phone** など。**phone** は、電話コールバック認証を実行するように Duo に指示する場合に使用します。

ユーザー名/パスワードが認証されると、Duo 認証プロキシは Duo クラウドサービスに接続し、Duo クラウドサービスは、その要求が設定されている有効なプロキシデバイスからのものであることを検証してから、指示に従ってユーザーのモバイルデバイスに一時的なパスコードをプッシュ送信します。ユーザーがこのパスコードを受け入れると、セッションは Duo で認証済みとマークされ、RA VPN が確立されます。

LDAP を使用した Duo 二要素認証

プライマリ ソースとしての Microsoft Active Directory（AD）または RADIUS サーバーとともに、セカンダリ認証ソースとして Duo LDAP サーバーを使用できます。Duo LDAP を使用すると、セカンダリ認証により、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールで検証されます。

脅威に対する防御 デバイスは、ポート TCP/636 経由で LDAPS を使用して、Duo LDAP と通信します。

Duo LDAP サーバーは認証サービスのみを提供し、アイデンティティサービスを提供しないことに注意してください。そのため、プライマリ認証ソースとして Duo LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザー名は表示されず、これらのユーザーに対してアクセス制御ルールを作成することはできません。

このアプローチを使用する場合は、RADIUS/AD サーバーと Duo LDAP サーバーの両方で設定されているユーザー名を使用して認証する必要があります。セキュアクライアントによってログインするように求められた場合は、プライマリ [パスワード（Password）] フィールドに RADIUS/AD のパスワードを入力します。[セカンダリパスワード（Secondary Password）] では、次のいずれかを使用して Duo で認証します。詳細については、https://guide.duo.com/anyconnect を参照してください。

- [Duoパスコード（Duo passcode）]：Duo Mobile で生成され、SMS を介して送信され、ハードウェア トークンによって生成されるパスコード、または管理者によって提供されるパスコードを使用して、認証します。1234567 などです。
- [プッシュ（push）]：Duo Mobile アプリをインストールしてアクティブにしている場合は、ログイン要求を電話機にプッシュします。要求を確認し、[承認（Approve）] をタップしてログインします。
- [電話（phone）]：電話機のコールバックを使用して認証します。
- [sms]：Duo パスコードをテキスト メッセージで要求します。ログイン試行は失敗します。新しいパスコードを使用して再度ログインします。

Duo LDAP の詳細な説明と例については、Duo LDAP を使用した二要素認証の設定方法 （878 ページ）を参照してください。

リモート アクセス VPN のライセンス要件

リモート アクセス VPN を設定する前に、基本デバイス ライセンスがエクスポート要件を満たす必要があります。デバイスを登録するとき、エクスポート制御機能が有効になっている Smart Software Managerのアカウントを使用して登録する必要があります。また、評価ライセンスを使用して機能を設定することはできません。

さらに、次のいずれかのリモートアクセス VPN ライセンスを購入し、有効にする必要があります：Secure Client Advantage、Secure Client Premier、Secure Client VPN のみ。これらのライセンスは、ASA ソフトウェアベースのヘッドエンドで使用される場合、さまざまな機能セットを許可するように設計されていますが、Threat Defense デバイスでは同様に扱われます。

ライセンスを有効にするには、**[デバイス（Device）]**>**[スマートライセンス（Smart License）]**>**[設定の表示（View Configuration）]** を選択し、[RA VPNライセンス（RA VPN License）] グループで適切なライセンスを選択します。Smart Software Manager Account で使用可能なライセンスが必要です。ライセンスの有効化の詳細については、オプション ライセンスの有効化または無効化 （109 ページ）を参照してください。

詳細については、『Cisco AnyConnect Ordering Guide』（http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf）を参照してください。http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html には、使用できるその他のデータシートもあります。

リモート アクセス VPN に関する注意事項と制限事項

RA VPN を設定する際は、次の注意事項と制限事項に注意してください。

- 同じ TCP ポートの同じインターフェイスで、Device Manager アクセス（管理アクセスリストの HTTPS アクセス）とリモートアクセス SSL VPN の両方を設定することはできません。たとえば、外部インターフェイスにリモートアクセス SSL VPN を設定する場合、ポー

ト 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。同じインターフェイスで両方の機能を設定する場合は、競合を回避するために、必ず、これらのサービスの少なくとも 1 つの HTTPS ポートを変更してください。

- RA VPN 外部インターフェイスはグローバル設定です。異なるインターフェイスに個別の接続プロファイルを設定することはできません。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。
- RADIUS トークンと RSA トークンを使用して二要素認証を設定すると、ほとんどの場合、デフォルトの 12 秒の認証タイムアウトでは短すぎて正常な認証が行われません。クライアント プロファイルの設定およびアップロード（840 ページ）で説明しているように、カスタム セキュアクライアントプロファイルを作成し、それを RA VPN 接続プロファイルに適用することにより、認証タイムアウト値を増やすことができます。認証タイムアウトを 60 秒以上にすることをお勧めします。これにより、ユーザーの認証および RSA トークンの貼り付けと、トークンのラウンドトリップ検証のための十分な時間が得られます。
- RA VPN ヘッドエンドなどに対する **curl** などのコマンドの実行は直接サポートされていないため、望ましい結果が得られない可能性があります。たとえば、ヘッドエンドは HTTP HEAD リクエストに応答しません。

リモート アクセス VPN の設定

クライアントのリモート アクセス VPN を有効化するには、いくつかの項目を設定する必要があります。次の手順を実行します。

手順

ステップ 1 ライセンスを設定します。

次の 2 つのライセンスを有効にする必要があります。

- デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。リモートアクセス VPN を設定するには、その前に基本ライセンスが輸出規制要件を満たす必要があります。また、評価ライセンスを使用して機能を設定することはできません。デバイスを登録する手順については、デバイスの登録 （107 ページ）を参照してください。
- リモート アクセス VPN ライセンス。詳細は、リモート アクセス VPN のライセンス要件（837 ページ）を参照してください。ライセンスを有効にするには、オプション ライセンスの有効化または無効化 （109 ページ）を参照してください。

ステップ 2 証明書を設定します。

証明書は、クライアントとデバイスの間のSSL接続を認証するために必要です。事前定義された VPN 用の DefaultInternalCertificate を使用することも、独自に作成することもできます。

認証に使われるディレクトリ レルムに暗号化接続を使用する場合は、信頼されるCA証明書をアップロードする必要があります。

証明書とそれらのアップロード方法の詳細については、証明書の設定 （183 ページ）を参照してください。

ステップ 3 （任意）TLS/SSL を設定します。

デフォルトでは、システムは、システムでサポートされている任意の TLS バージョンと暗号化方式を使用して、リモートユーザーがリモートアクセス VPN に接続できるようにします。ただし、よりセキュアな接続を実現するため、許可されるTLS/DTLSバージョン、暗号、およびDiffie-Hellmanグループを制限することもできます。TLS/SSL 暗号設定の設定 （967 ページ）を参照してください。

ステップ 4 （任意） クライアント プロファイルの設定およびアップロード （840 ページ）。

ステップ 5 リモート ユーザを認証する目的で使用されるアイデンティティ ソースを設定します。

リモート アクセス VPN へのログインを許可するユーザ アカウントに次のソースを使用できます。代わりに、クライアント証明書を単独で、またはアイデンティティソースと連携させて、認証に使用することができます。

- Active Directory アイデンティティ レルム：プライマリ認証ソースとして。ユーザ アカウントは Active Directory（AD）サーバで定義されます。「AD アイデンティティ レルムの設定 （195 ページ）」を参照してください。
- RADIUS サーバーグループ：プライマリまたはセカンダリ認証ソースとして。認可およびアカウンティングにも。「RADIUS サーバー グループの設定 （203 ページ）」を参照してください。
- LocalIdentitySource（ローカル ユーザ データベース）：プライマリ ソースまたはフォールバック ソースとして。デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。フォールバック ソースとしてローカル データベースを使用する場合は、必ず外部サーバで定義したものと同じユーザ名/パスワードを定義します。「ローカル ユーザーの設定 （214 ページ）」を参照してください。
- Duo LDAP サーバー：プライマリまたはセカンダリ認証ソースとして使用できます。Duo LDAP サーバーをプライマリ ソースとして使用することはできますが、通常の設定ではありません。通常は、プライマリ Active Directory または RADIUS サーバーとともに二要素認証を提供するためのセカンダリ ソースとして使用します。詳細は、Duo LDAP を使用した二要素認証の設定方法 （878 ページ）を参照してください。

ステップ 6 （オプション） RA VPN のグループ ポリシーの設定 （857 ページ）

グループポリシーは、ユーザーに関連する属性を定義します。グループメンバーシップに基づいて、リソースへの差分アクセスを提供するためにグループポリシーを設定することができます。または、すべての接続でデフォルトポリシーを使用することもできます。

ステップ 7 RA VPN 接続プロファイルの設定 （847 ページ）。

ステップ 8 リモート アクセス VPN によるトラフィックの許可 （843 ページ）。

ステップ 9 リモート アクセス VPN 設定の確認 （844 ページ）。

接続の完了に関する問題が発生した場合は、リモート アクセス VPN のトラブルシューティング （865 ページ）を参照してください。

ステップ 10 （オプション）アイデンティティ ポリシーを有効にして、パッシブ認証のルールを設定します。

パッシブ ユーザ認証を有効にすると、リモート アクセス VPN 経由でログインするユーザがダッシュボードに表示され、ポリシー内のトラフィック一致基準としても使用できます。パッシブ認証を有効にしない場合、RA VPN ユーザはアクティブ認証ポリシーに一致する場合にのみ使用できます。ダッシュボードのユーザー情報またはトラフィック照合用のユーザー情報を取得するには、アイデンティティ ポリシーを有効にする必要があります。

クライアント プロファイルの設定およびアップロード

セキュアクライアントプロファイルは、セキュアクライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーがセキュアクライアントの設定および詳細設定からオプションを変更することを許可するかどうかを定義します。

リモートアクセスVPN接続を設定する際に外部インターフェイスの完全修飾ホスト名（FQDN）を設定すると、システムが自動的にクライントプロファイルを作成します。このプロファイルでは、デフォルトの設定が有効にされます。クライントプロファイルを作成してアップロードする必要があるのは、デフォルト以外の動作が必要な場合のみです。クライントプロファイルはオプションであることに注意してください。クライントプロファイルをアップロードしなければ、セキュアクライアントはプロファイルで制御されるすべてのオプションにデフォルトの設定を使用します。

（注） 初回の接続時に、ユーザーが制御できる設定のすべてをセキュアクライアントに表示させるには、VPN プロファイルのサーバーリストに、Threat Defense デバイスの外部インターフェイスを含める必要があります。アドレスまたは FQDN をホスト エントリとしてプロファイルに追加していない場合、セッションにフィルタは適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、プロファイルにデバイスをホストエントリとして追加しなければ、この証明書照合は無視されます。

セキュアクライアントのプロファイルに加えて、必要に応じて セキュアクライアント で使用できるさまざまなモジュール（AMP イネーブラなど）のプロファイルを作成できます。これらのモジュールのプロファイルをアップロードできますが、Device Manager は、セキュアクライアントプロファイルの作成のみをサポートしています。ただし、Device Manager を介して任意の種類のプロファイルをアップロードしてから、Threat Defense API を使用して（API Explorer

から）、オブジェクトのプロファイルタイプを変更できます。[プロファイル（Profiles）]ページには任意のタイプのすべてのプロファイルが表示されますが、リストにはプロファイルタイプは示されません。次の手順では、これを実行する方法について説明します。

次に、オブジェクトページからオブジェクトを直接作成および編集する方法について説明します。オブジェクトリストに表示される **[新規Secure Clientプロファイルの作成（Create New Secure Client Profile）]** リンクをクリックして、セキュアクライアント プロファイル オブジェクトをプロファイルプロパティの編集中に作成することもできます。

始める前に

クライアントプロファイルをアップロードするには、その前に、以下の作業を行う必要があります。

- セキュアクライアントの「Profile Editor：Windows/Standalone installer インストーラ（MSI）」をダウンロードしてインストールします。このインストールファイルはWindows 専用で、ファイル名は anyconnect-profileeditor-win-<version>-k9.msi です。ここで、<version> はセキュアクライアントのバージョンです（ファイル名は変更される場合があります）。たとえば、anyconnect-profileeditor-win-4.3.04027-k9.msi のような名前になります。プロファイル エディタをインストールする前に、Java JRE（1.6 以降）もインストールする必要があります。software.cisco.com から セキュアクライアント プロファイルエディタを入手します。このパッケージには、VPN クライアントのプロファイルエディタだけでなく、すべてのプロファイルエディタが含まれていることに注意してください。
- プロファイル エディタを使用して、必要なプロファイルを作成します。プロファイルには、外部インターフェイスのホスト名または IP アドレスを指定する必要があります。詳細については、エディタのオンライン ヘルプを参照してください。

手順

ステップ 1 [オブジェクト（Objects）] を選択してから、目次で **[Secure Clientプロファイル（Secure Client Profiles）]** を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。
- オブジェクトに関連付けられているプロファイルをダウンロードする場合は、対象のオブジェクトの [ダウンロード（download ）] アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 名前を入力し、オプションでオブジェクトの説明を入力します。

モジュールプロファイルをアップロードする場合は、セキュアクライアントプロファイルと区別しやすいように、モジュールタイプを示すオブジェクト名を使用してください。

ステップ 4 [アップロード（Upload）] をクリックし、プロファイルエディタを使って作成したファイルを選択します。

ステップ 5 [開く（Open）] をクリックしてプロファイルをアップロードします。

ステップ 6 [OK] をクリックしてオブジェクトを追加します。

ステップ 7 作成したプロファイルが実際にセキュアクライアントプロファイルとは異なるタイプである場合は、次の手順を実行してオブジェクトのプロファイルタイプを変更します。

a) [詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

ブラウザの設定に応じて、API エクスプローラが別のタブまたはウィンドウで開きます。

b) AnyConnectClientProfile リソースを開きます。

c) GET /object/anyconnectclientprofiles メソッドを選択し、[試行する（Try It Out!）] ボタンをクリックします。

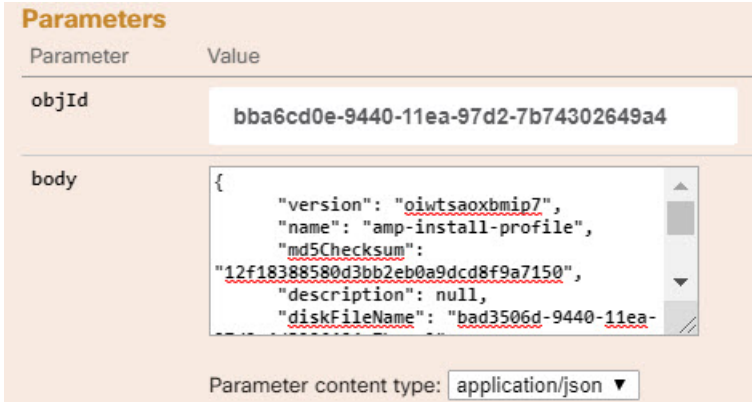
各プロファイルオブジェクトは次のように表されます。強調表示されている属性は、変更する必要がある属性です。

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) 出力でオブジェクトを見つけて、コードを選択し、Ctrl キーを押しながらクリックしてクリップボードにコピーします。

e) PUT /object/anyconnectclientprofiles/{objId} メソッドを選択し、その内容を [body] フィールドに貼り付けます。

f) [id] 値をコピーし、本文の上にある [objId] 編集ボックスに貼り付けます。オブジェクト ID は「自己」URL の末尾でも確認できます。



g) オブジェクトの本文にある [anyConnectModuleType] フィールドを見つけて、その値をプロファイルタイプの値に置き換えます。DART、FEEDBACK、WEB_SECURITY、ANY_CONNECT_CLIENT_PROFILE、AMP_ENABLER、NETWORK_ACCESS_MANAGER、NETWORK_VISIBILITY、START_BEFORE_LOGIN、ISE_POSTURE、UMBRELLA から選択してください。

h) 再び [body] で、[links] 属性を削除（[type] 値の後のカンマを含め）します。

オブジェクト本文は、次のようになります。

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "AMP_ENABLER",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile"
      }
```

i) [試してみる（Try It Out!）] をクリックします。応答を調べて、オブジェクトが正しく変更されたことを確認します。応答コードが 200 であり、応答本文で変更がエコーされている必要があります。GET メソッドを使用することで、結果のさらなる確認を行うことができます。

リモート アクセス VPN によるトラフィックの許可

リモートアクセス VPN トンネル内のトラフィックフローを有効にするには、次の方法のいずれかを使用します。

- **sysopt connection permit-vpn** コマンドを設定します。これにより、VPN 接続と一致するトラフィックがアクセス コントロール ポリシーから免除されます。このコマンドのデフォルトは **no sysopt connection permit-vpn** で、VPN トラフィックをアクセス コントロール ポリシーでも許可する必要があることを意味します。

これは、外部ユーザーがリモート アクセス VPN アドレス プール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点はVPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

このコマンドを設定するには、RA VPN 接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（Bypass Access Control policy for decrypted traffic）] オプションを選択します。

- リモート アクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザーが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

リモート アクセス VPN 設定の確認

リモート アクセス VPN を設定し、設定をデバイスに展開した後で、リモート接続を行えることを確認します。

問題が発生した場合は、トラブルシューティング トピックに目を通し、問題の分離と修正に役立てます。リモート アクセス VPN のトラブルシューティング （865 ページ）を参照してください。

手順

ステップ 1 外部ネットワークから、セキュアクライアントを使用して VPN 接続を確立します。

Web ブラウザを使用して、**https://***ravpn-address* を開きます。*ravpn-address* は、VPN 接続を許可する外部インターフェイスの IP アドレスまたはホスト名です。必要に応じて、クライアント ソフトウェアをインストールし、接続を完了します。「セキュアクライアント ソフトウェアのインストール方法 （831 ページ）」を参照してください。

リモートアクセス VPN 接続用のポートを変更した場合は、URL にカスタムポートを含める必要があります。たとえば、ポートを 4443 に変更した場合は、https://ravpn.example.com:4443 のような URL にします。

グループ URL を設定した場合は、グループ URL も試してください。

ステップ 2 デバイス CLI にログインします（CLI（コマンドライン インターフェイス）へのログイン （9 ページ）を参照）。または、CLI コンソールを開きます。

ステップ 3 **show vpn-sessiondb** コマンドを使用して、現在の VPN セッションに関する概要情報を表示します。

統計情報では、アクティブな セキュアクライアントセッション、および累積セッション数、ピーク同時セッション数、非アクティブセッション数の情報が示されます。次は、コマンドからの出力例です。

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
----------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     50
Device Total VPN Capacity   :  10000
Device Load                 :     0%
----------------------------------------------------------------------------

----------------------------------------------------------------------------
Tunnels Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
Clientless                  :      0 :          1 :               1
AnyConnect-Parent           :      1 :         49 :               3
SSL-Tunnel                  :      1 :         46 :               3
DTLS-Tunnel                 :      1 :         46 :               3
----------------------------------------------------------------------------
Totals                      :      3 :        142
----------------------------------------------------------------------------

----------------------------------------------------------------------------
IPv6 Usage Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
AnyConnect SSL/TLS/DTLS     :        :           :
  Tunneled IPv6             :      1 :         20 :           2
----------------------------------------------------------------------------
```

ステップ 4 **show vpn-sessiondb anyconnect** コマンドを使用して、現在の VPN セッションに関する詳細情報を表示します。

詳細情報には、使用されている暗号化、送信バイト数と受信バイト数などの統計情報が含まれます。VPN接続を使用する場合、このコマンドを再発行すると送信バイト数と受信バイト数が変わるのがわかります。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel:
```

```
(1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                 Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy        Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                  Tunnel Zone  : 0
```

リモート アクセス VPN 設定の管理

リモートアクセス VPN 接続プロファイルは、外部ユーザーが セキュアクライアントを使用してシステムに VPN に接続することを許可するという接続特性を定義します。各プロファイルは、ユーザーの認証に使用される AAA サーバーと証明書、ユーザーの IP アドレスを割り当てるためのアドレス プール、およびさまざまなユーザー向け属性を定義するグループ ポリシーを定義します。

異なるユーザーグループに異なるサービスを提供する必要がある場合、または異なる認証ソースがある場合は、複数のプロファイルを作成します。たとえば、自分の組織が異なる認証サーバーを使用する別の組織とマージする場合、別の組織の認証サーバーを使用する新しいグループのプロファイルを作成できます。

手順

ステップ 1 **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次の [接続プロファイル（Connection Profiles）] をクリックします（未選択の場合）。

ステップ 3 次のいずれかを実行します。

- 新しい接続プロファイルを作成するには、[+] ボタンをクリックします。詳細な手順については、RA VPN 接続プロファイルの設定 （847 ページ）を参照してください。
- 表示ボタン（）をクリックして、接続プロファイルの概要と接続手順を開きます。サマリー内で、[編集（Edit）] をクリックして変更できます。
- 削除ボタン（）をクリックすると、不要な接続プロファイルを削除できます。

- コンテンツテーブルで[グループポリシー（Group Policies）]を選択して、接続プロファイルのユーザー指向属性を定義します。RA VPN のグループ ポリシーの設定 （857 ページ）を参照してください。

RA VPN 接続プロファイルの設定

リモートアクセス VPN 接続プロファイルを作成すると、ホームネットワークなどの外部ネットワークからでも、ユーザーは内部ネットワークに接続できるようになります。異なる認証方式に対応するために、個別のプロファイルを作成します。

始める前に

リモート アクセス（RA）VPN 接続を設定する前に、以下のことを行います。

- 必要な セキュアクライアント ソフトウェアパッケージを software.cisco.com からワークステーションにダウンロードします。
- リモートアクセス VPN 接続を終了する外部インターフェイスは、同じポートで HTTPS 接続を許可する管理アクセスリストを持つこともできません。管理アクセス用に別のポートを設定するか（データインターフェイスでの管理アクセス用の HTTPS ポートの設定 （926 ページ）を参照）、接続プロファイル用に別のポートを設定します。どちらのサービスもデフォルトでポート 443 を使用するため、いずれかを変更する必要があります。

手順

ステップ 1 **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次の [接続プロファイル（Connection Profiles）] をクリックします（未選択の場合）。

ステップ 3 次のいずれかを実行します。

- 新しい接続プロファイルを作成するには、[+] ボタンをクリックします。
- 表示ボタン（  ）をクリックして、接続プロファイルの概要と接続手順を開きます。サマリー内で、[編集（Edit）] をクリックして変更できます。

ステップ 4 基本接続の属性を設定します。

- [接続プロファイル名（Connection Profile Name）]：スペースを含めずに最大 50 文字で、この接続の名前を指定します。例、MainOffice。IP アドレスは名前として使用できません。

（注） ここで入力する名前が、セキュアクライアントクライアントの接続リストに表示されます。ユーザーにとって意味のある名前を選択します。

- [グループエイリアス（Group Alias）]、[グループURL（Group URL）]：エイリアスには特定の接続プロファイルの代替名または URL を含めることができます。VPN ユーザーは、脅威に対する防御 デバイスへの接続時に、セキュアクライアント クライアントの接続リストでエイリアス名を選択できます。接続プロファイル名はグループのエイリアスとして自動的に追加されます。エイリアスは最大 31 文字です。

  グループ URL のリストも設定できます。このリストは、リモートアクセス VPN 接続を開始するときにエンドポイントが選択できるリストです。ユーザーがグループ URL を使用して接続すると、システムはその URL に一致する接続プロファイルを自動的に使用します。この URL は、セキュアクライアント クライアントをまだインストールしていないクライアントによって使用されます。

  グループエイリアスと URL を必要な数だけ追加します。これらのエイリアスと URL は、デバイスで定義されているすべての接続プロファイルで一意である必要があります。グループ URL は https:// で始まる必要があります。

  たとえば、「Contractor」というエイリアスとグループ URL「https://ravpn.example.com/contractor」があるとします。セキュアクライアント クライアントをインストールすると、ユーザーは単純に セキュアクライアント VPN の接続ドロップダウンリストでグループエイリアスを選択します。

ステップ 5 プライマリ アイデンティティ ソース、および必要に応じてセカンダリ ソースを設定します。

これらのオプションにより、リモートアクセス VPN 接続を有効にするための、デバイスへのユーザー認証方法が決定されます。最も簡単なアプローチは、AAA のみを使用し、AD レルムを選択するか、または LocalIdentitySource を使用する方法です。[認証タイプ（Authentication Type）] として次のアプローチを使用できます。

- [AAAのみ（AAA Only）]：ユーザー名とパスワードに基づいてユーザーを認証および認可します。詳細は、接続プロファイルのための AAA の設定 （851 ページ）を参照してください。
- [クライアント証明書のみ（Client Certificate Only）]：クライアント デバイス アイデンティティ証明書に基づいてユーザーを認証します。詳細は、接続プロファイルのための証明書認証の設定 （855 ページ）を参照してください。
- [AAAおよびクライアント認証（AAA and Client Certificate）]：ユーザー名/パスワードと、クライアント デバイス アイデンティティ証明書の両方を使用します。
- [SAML]：プライマリ認証で SAML サーバーを使用します。SAML を使用する場合は、フォールバックまたはセカンダリ認証ソースを設定できません。詳細については、接続プロファイルのための AAA の設定 （851 ページ）を参照してください。

ステップ 6 クライアントのアドレスプールを設定します。

アドレスプールは、リモートクライアントが VPN 接続を確立するときに、システムがリモートクライアントに割り当てることができる IP アドレスを定義します。詳細については、「RA VPN のクライアント アドレス指定の設定 （856 ページ）」を参照してください。

ステップ 7 [Next] をクリックします。

ステップ 8 このプロファイルに使用する [グループポリシー（Group Policy）] を選択します。

グループポリシーは、トンネル確立後のユーザー接続の期間を設定します。システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

グループポリシーを選択すると、グループの特性の概要が表示されます。サマリー内で、[編集（Edit）] をクリックして変更できます。

必要なグループ ポリシーが存在しない場合は、ドロップダウンリストの [新しいグループポリシーの作成（Create New Group Policy）] をクリックします。

グループポリシーの詳細については、RA VPN のグループ ポリシーの設定 （857 ページ）を参照してください。

ステップ 9 [Next] をクリックします。

ステップ 10 グローバル設定を行います。

これらのオプションは、すべての接続プロファイルに適用されます。最初の接続プロファイルを作成すると、これらのオプションは、後続の各プロファイルに対して事前に設定されます。変更すると、設定済みのすべての接続プロファイルが変更されます。

- [デバイスアイデンティティ証明書（Certificate of Device Identity）]：デバイスのアイデンティティを確立するために使用する内部証明書を選択します。安全な VPN 接続を完了するには、クライアントがこの証明書を承認する必要があります。まだ証明書がない場合、ドロップダウンリストの [新規内部証明書の作成（Create New Internal Certificate）] をクリックします。証明書を設定する必要があります。
- [外部インターフェイス（Outside Interface）]：リモート アクセス VPN 接続を確立するときにユーザーが接続するインターフェイス。通常、これは外部（インターネット側）インターフェイスですが、サポートされるデバイスおよびエンドユーザー間の任意のインターフェイスを選択できます。
- [外部インターフェイスの完全修飾ドメイン名（Fully-qualified Domain Name for the Outside Interface）]：インターフェイスの名前。例、ravpn.example.com。名前を指定すると、クライアント プロファイルが作成されます。

  （注） ユーザーは、クライアントによって VPN で使用される DNS サーバーが、この名前から外部インターフェイスの IP アドレスを解決できるようにする責任があります。関連する DNS サーバーに FQDN を追加します。

- [ポート（Port）]：RA VPN 接続に使用する TCP ポート。デフォルトは 443 です。RA VPN に使用されているインターフェイスで Device Manager に接続する必要がある場合は、接続プロファイルまたは Device Manager のポート番号を変更する必要があります。どちらのサービスもデフォルトでポート 443 を使用します。リモートアクセス VPN 接続のポー

トを変更する場合、ユーザーは URL にポート番号を含める必要があることに注意してください。

- [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：VPN トラフィックにアクセス制御ポリシーを適用するかどうか。復号された VPN トラフィックは、デフォルトでアクセス コントロール ポリシー インスペクションの対象となります。[復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] を有効にすると、アクセス制御ポリシーはバイパスされますが、リモートアクセス VPN の場合、VPN フィルタ ACL および AAA サーバーからダウンロードされた認証 ACL は引き続き VPN トラフィックに適用されます。

  このオプションを選択すると、システムによりグローバル設定である **sysopt connection permit-vpn** コマンドが設定されることに注意してください。これは、サイト間 VPN 接続の動作にも影響を及ぼします。また、接続プロファイル間でこのオプションの選択を変えることはできません。この機能は、すべてのプロファイルに対してオンまたはオフにします。

  このオプションを選択しない場合、外部ユーザーがリモートアクセス VPN アドレスプール内の IP アドレスをスプーフィングし、ネットワークにアクセスするおそれがあります。この理由は、アドレスプールに内部リソースへのアクセスを許可するアクセスコントロールルールを作成する必要があるためです。アクセスコントロールルールを使用する場合は、送信元 IP アドレスだけではなく、ユーザーの仕様を使用してアクセスを制御することを検討してください。

  このオプションを選択することの欠点は、VPN トラフィックが検査されないことです。つまり、侵入およびファイル保護、URL フィルタリング、またはその他の高度な機能がトラフィックに適用されません。つまり、このトラフィックに対する接続イベントは生成されず、VPN 接続は統計ダッシュボードには反映されません。

- [NAT免除（NAT Exempt）]：リモートアクセス VPN エンドポイントとの入出力トラフィックに対する NAT 変換を免除するには、NAT 免除を有効にします。VPN トラフィックを NAT 免除にしない場合は、外部および内部インターフェイスに対する既存の NAT ルールが RA VPN アドレス プールに適用されないことを確認してください。NAT 免除 ルールは特定の送信元/宛先インターフェイスとネットワークの組み合わせに対する手動スタティック アイデンティティ NAT ルールですが、NAT ポリシーには反映されず、非表示になります。NAT 免除を有効にした場合、以下も設定する必要があります。

  これはすべての接続プロファイルに適用されるグローバルオプションであることに注意してください。したがって、インターフェイスおよび内部ネットワークは追加するだけで、交換しないでください。そうでない場合、すでに定義済みのその他の接続プロファイルすべてに対する NAT 免除設定が変更されます。

  - [内部インターフェイス（Inside Interfaces）]：リモート ユーザーがアクセスする内部ネットワークのインターフェイスを選択します。これらのインターフェイスに対して NAT ルールが作成されます。

- [内部ネットワーク（Inside Networks）]：リモート ユーザーがアクセスする内部ネットワークを表すネットワーク オブジェクトを選択します。ネットワーク リストには、サポートしているアドレス プールと同じ IP タイプを含める必要があります。

- **[Secure Clientパッケージ（Secure Client Package）]**：RA VPN 接続でサポートする セキュアクライアント の完全インストール ソフトウェア イメージ。パッケージごとに、ファイル名（拡張子を含む）を 60 文字以下で指定します。Windows、Mac、Linux のエンドポイントに対して別々のパッケージをアップロードできます。ただし、異なる接続プロファイルに対しては異なるパッケージを設定できません。別のプロファイルパッケージがすでに設定されている場合、パッケージは事前に選択されます。これを変更すると、すべてのプロファイルに対して変更されます。

  Software.cisco.com からパッケージをダウンロードします。エンドポイントに適切なパッケージがインストールされていない場合、ユーザーは、ユーザー認証後にパッケージをダウンロードしてインストールするよう求められます。

ステップ 11 [Next] をクリックします。

ステップ 12 サマリーを確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順（Instructions）] をクリックして、セキュアクライアント ソフトウェアをインストールし、VPN接続を完了できることをテストするためにエンドユーザーが最初に行う必要がある内容を確認します。[コピー（Copy）]をクリックしてこれらの手順をクリップボードにコピーし、ユーザーに配布します。

ステップ 13 [終了（Finish）] をクリックします。

次のタスク

リモート アクセス VPN によるトラフィックの許可 （843 ページ）で説明したように、トラフィックが VPN トンネルで許可されていることを確認します。

接続プロファイルのための AAA の設定

認証、許可、およびアカウンティング（AAA） サーバーは、ユーザー名とパスワードを使用して、ユーザーのリモートアクセス VPN へのアクセスを許可するかどうかを判断します。RADIUS サーバを使用する場合は、認証されたユーザー間で許可レベルを区別して、保護されたリソースへの差別化されたアクセスを提供できます。使用状況を追跡するために RADIUS アカウンティングサービスを使用することもできます。

AAA を設定する場合は、プライマリ アイデンティティ ソースを設定する必要があります。セカンダリ ソースとフォールバック ソースはオプションです。RSA トークンや DUO などを使用する二重認証を実装する場合は、セカンダリ ソースを使用します。

プライマリ アイデンティティ ソースのオプション

- [ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：リモート ユーザーの認証に使用されるプライマリ アイデンティティ ソース。VPN 接続を完了するには、エンド ユーザがこのソースか任意のフォールバック ソースで定義されている必要があります。次のいずれかを選択します。
  - Active Directory（AD）のアイデンティ レルム。必要なレルムがまだ存在していない場合は、[新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。
  - RADIUS サーバーグループ。
  - LocalIdentitySource（ローカル ユーザ データベース）：デバイスで直接ユーザを定義できます。外部サーバを使用することはできません。
  - Duo LDAP サーバー。ただし、これは、Duo LDAP を使用した二要素認証の設定方法（878 ページ）の説明に従って二要素認証を提供するためのセカンダリ認証ソースとして使用することを推奨します。プライマリ ソースとして使用する場合、ユーザー ID 情報は取得されません。ダッシュボードにユーザー情報が表示されず、ユーザーベースのアクセス制御ルールを作成することもできません。
  - SAML サーバー。SAML サーバーを使用する場合は、フォールバックまたはセカンダリ認証ソースを設定できません。RADIUS を認可サーバーとして使用できますが、認証が不要になるように RADIUS サーバーを設定する必要があります。つまり、接続が SAML によって認証された後に RADIUS サーバーが認可情報を提供するようにします。
- [SAMLログインエクスペリエンス（SAML Login Experience）]：プライマリ認証ソースとして SAML を選択した場合は、Web 認証を完了するために使用するクライアントブラウザを選択する必要があります。
  - [VPNクライアント組み込みブラウザ（VPN Client embedded browser）]：VPN クライアントは Web 認証に組み込みブラウザを使用するため、認証は VPN 接続にのみ適用されます。これはデフォルトであり、追加の設定は必要ありません。
  - [デフォルトOSブラウザ（Default OS Browser）]：VPN クライアントは、Web 認証にシステムのデフォルトブラウザを使用します。このオプションは、VPN認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。組み込みブラウザでは実行できない Web 認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。

    ブラウザで Web 認証を有効にするパッケージをアップロードする必要があります。パッケージは software.cisco.com から取得します。アップロードするパッケージは、デフォルトの OS ブラウザで SAML を使用するすべての接続プロファイルで使用されます。パッケージはグローバルであり、接続プロファイル固有ではありません。
- [フォールバックローカルアイデンティティソース（Fallback Local Identity Source）]：プライマリ ソースが外部サーバーの場合、プライマリ サーバーが使用できない場合のフォールバックとして LocalIdentitySource を選択できます。フォールバック ソースとしてローカ

ル データベースを使用する場合は、必ず外部サーバで定義したものと同じローカル ユーザ名/パスワードを定義します。

[詳細オプション（Advanced Options）]：[詳細（Advanced）] リンクをクリックして、次のオプションを設定します。

- [削除オプション（Strip options）]：レルムとは管理ドメインのことです。次のオプションを有効にすると、ユーザー名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
  - [ユーザー名からアイデンティティソースサーバーを削除（Strip Identity Source Server from Username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からアイデンティティソース名を削除するかどうか。たとえば、このオプションを選択してユーザーがユーザー名として domain\username を入力すると、ドメインがユーザー名から取り除かれ、認証用に AAA サーバーに送信されます。デフォルトでは、このオプションはオフになっています。
  - [ユーザー名からグループを削除（Strip Group from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー名からグループを削除するかどうか。このオプションは、username@domain 形式で指定された名前に適用されます。選択すると、domain と @ 記号が削除されます。デフォルトでは、このオプションはオフになっています。
- [パスワード管理を有効にする（Enable Password Management）]：パスワードの有効期限が切れたときにユーザーにパスワードの変更を許可するかどうかを指定します。このオプションを選択しない場合、ユーザーのパスワードが期限切れになると、セキュアクライアント は接続を拒否するため、ユーザーは AAA サーバーにアクセスして、パスワードを変更する必要があります。このオプションを選択すると、セキュアクライアントはパスワードの有効期限が切れたときにパスワードの変更をユーザーに要求します。これは、ユーザーにとって非常に便利です。次のオプションのいずれかを選択します。また、AAA サーバーで MSCHAPv2 を有効にします。
  - [パスワードの有効期限の x 日前にユーザーに通知（Notify user x days prior to password expiration）]（LDAP のみ）：指定した日数から始めて、パスワードの有効期限が近づいていることをユーザーに警告します。1 ー 180 日の範囲で警告を設定できます。デフォルトは 14 です。
  - [パスワードの有効期限の日にユーザーに通知（Notify user on the day of password expiration）]：ユーザーに警告は表示されませんが、パスワードの有効期限が切れると、パスワードの変更を求められます。警告期間を設定している場合でも、RADIUS ユーザーは常にパスワードの変更を求められます。

セカンダリ アイデンティティ ソース

- [ユーザー認証用のセカンダリアイデンティティソース（Secondary Identity Source for User Authentication）]：オプションの 2 番目のアイデンティティ ソースです。ユーザーがプライマリ ソースで正常に認証されると、セカンダリ ソースでの認証が求められます。AD レ

ルム、RADIUS サーバーグループ、Duo LDAP サーバー、またはローカル アイデンティティ ソースを選択できます。

- [詳細オプション（Advanced options）]：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。
  - [セカンダリ用フォールバックローカルアイデンティティソース（Fallback Local Identity Source for Secondary）]：セカンダリソースが外部サーバーの場合、セカンダリサーバーが使用できない場合のフォールバックとしてLocalIdentitySourceを選択できます。フォールバックソースとしてローカルデータベースを使用する場合は、必ずセカンダリ外部サーバーで定義したものと同じローカルユーザー名/パスワードを定義します。
  - [セカンダリログインにプライマリユーザー名を使用（Use Primary Username for Secondary Login）]：デフォルトでは、セカンダリ アイデンティティ ソースを使用する場合、セカンダリ ソースに対してユーザー名とパスワードの両方が求められます。このオプションを選択すると、システムはセカンダリパスワードの入力のみを求め、プライマリ アイデンティティ ソースに対して認証されたものと同じユーザー名をセカンダリ ソースに対して使用します。プライマリとセカンダリの両方のアイデンティティソースで同じユーザー名を設定する場合は、このオプションを選択します。
  - [セッションサーバーのユーザー名（Username for Session Server）]：認証に成功すると、ユーザー名はイベントと統計ダッシュボードに表示され、ユーザーベースまたはグループベースのSSL復号化およびアクセス制御ルールに一致するものを判断するために使用され、アカウンティングに使用されます。2 つの認証ソースを使用しているため、ユーザーアイデンティティとして、プライマリまたはセカンダリのどちらのユーザー名を使用するのかシステムに通知する必要があります。デフォルトでは、プライマリ名が使用されます。
  - [パスワードタイプ（Password Type）]：セカンダリ サーバーのパスワードを取得する方法。このフィールドは、認証タイプに [AAA とクライアント証明書（AAA and Client Certificate）] を選択した場合にのみ適用されます。証明書オプションでは、[ユーザーログインウィンドウの証明書からユーザー名を事前入力（Prefill username from certificate on user login window）] と [ログインウィンドウでユーザー名を非表示にする（Hide username in login window）] の両方を選択します。デフォルトは [プロンプト（Prompt）] で、ユーザーはパスワードの入力が求められることを意味します。

    プライマリサーバーへのユーザー認証時に入力したパスワードを自動的に使用するには、[プライマリアイデンティティソースのパスワード（Primary Identity Source Password）] を選択します。

    すべてのユーザーに同じパスワードを使用するには [共通パスワード（Common Password）] を選択し、[共通パスワード（Common Password）] フィールドにそのパスワードを入力します。

その他のオプション

- [認証サーバー（Authorization Server）]：リモート アクセス VPN ユーザーを認証するように設定された RADIUS サーバー グループです。

認証の完了後、認可によって、認証済みの各ユーザーが使用できるサービスおよびコマンドが制御されます。認可は、ユーザーが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザーに対して同じアクセス権を提供します。認可のためのRADIUSの設定の詳細については、RADIUSおよびグループポリシーを使用したユーザーの権限および属性の制御 （832 ページ）を参照してください。

システムがグループポリシーで定義されているものと重複する認可属性を RADIUS サーバーから取得した場合、RADIUS 属性は、グループポリシー属性をオーバーライドすることに注意してください。

- [アカウンティングサーバー（Accounting Server）]：（オプション）リモートアクセス VPN セッションへのアカウンティングに使用する RADIUS サーバーグループ。

  アカウンティングは、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワークリソース量を追跡します。脅威に対する防御デバイスは、RADIUSサーバーにユーザーアクティビティを報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

接続プロファイルのための証明書認証の設定

リモートアクセス VPN 接続を認証するために、クライアントデバイスにインストールされた証明書を使用することができます。証明書認証を使用している場合は、リモートアクセスユーザー接続の検証に使用する信頼できる CA 証明書に、[検証の使用（Validation Usage）] の [SSL クライアント（SSL Client）] オプションが含まれていることを確認します。

クライアント証明書を使用していても、セカンダリ アイデンティティ ソース、フォールバック ソース、および認証およびアカウンティングサーバーを引き続き設定できます。これらは AAA オプションです。詳細については接続プロファイルのための AAA の設定 （851 ページ）を参照してください。

以下に、証明書固有の属性を示します。これらの属性は、プライマリ アイデンティティ ソースとセカンダリ アイデンティティ ソースに対して個別に設定できます。セカンダリソースの設定はオプションです。

- [証明書のユーザー名（Username from Certificate）]：次のいずれかを選択します。
  - [マップ固有フィールド（Map Specific Field）]：証明書の要素を [プライマリフィールド（Primary Field）] および [セカンダリフィールド（Secondary Field）] の順番で使用します。デフォルトはCN（共通名）と OU（組織単位）です。組織に適したオプションを選択します。これらのフィールドを組み合わせてユーザー名が提供され、このユーザー名がイベント、ダッシュボード、さらにSSL復号とアクセス制御ルールでのマッチング目的に使用されます。
  - [DN（識別名）全体をユーザー名として使用（Use entire DN (distinguished name) as username）]：システムが自動的に DN フィールドからユーザー名を導出します。

- [詳細オプション（Advanced options）]：[詳細（Advanced）] リンクをクリックし、次のオプションを設定します。
  - [ユーザーログインウィンドウの証明書からユーザー名を事前入力（Prefill username from certificate on user login window）]：ユーザーに認証を要求するときに、取得したユーザー名をユーザー名フィールドに入力するかどうか。
  - [ログインウィンドウでユーザー名を非表示にする（Hide username in login window）]：[事前入力（Prefill）] オプションを選択すると、ユーザー名を非表示にできます。これは、ユーザーがパスワードプロンプトでユーザー名を編集できないことを意味します。

RA VPN のクライアント アドレス指定の設定

リモートアクセス VPN に接続するエンドポイントにシステムが IP アドレスを提供するための方法が必要です。これらのアドレスは、AAA サーバー、DHCP サーバー、グループポリシーで設定されている IP アドレスプール、または接続プロファイルで設定された IP アドレスプールによって提供されます。システムは、この順序でこれらのリソースを試行し、使用可能なアドレスを取得すると停止し、次にアドレスをクライアントに割り当てます。このように、同時接続数が異常な場合のフェールセーフを作成するために複数のオプションを設定できます。

接続プロファイルのアドレスプールを設定するには、次の方法の 1 つ以上を使用します。

- [AAA サーバー（AAA Server）]：まず、アドレスプールのサブネットを指定する Threat Defense デバイスのネットワークオブジェクトを設定します。次に、RADIUS サーバーで、そのオブジェクト名を使用してユーザーの Address-Pools（217）属性を設定します。また、接続プロファイルで認証用の RADIUS サーバーを指定します。
- [DHCP]：まず、1 つ以上の IPv4 アドレス範囲を持つ RA VPN の DHCP サーバーを設定します（DHCP を使用して IPv6 プールを設定することはできません）。次に、DHCP サーバーの IP アドレスを使用してホスト ネットワーク オブジェクトを作成します。その後、このオブジェクトは接続プロファイルの [DHCPサーバー（DHCP Servers）] 属性で選択できます。最大 10 台の DHCP サーバーを設定できます。

  DHCP サーバーに複数のアドレス プールがある場合、[DHCPスコープ（DHCP Scope）] 属性を接続プロファイルにアタッチするグループポリシーで使用して、使用するプールを選択することができます。プールのネットワークアドレスを使用して、ホストネットワークオブジェクトを作成します。たとえば、DHCP プールに 192.168.15.0/24 および 192.168.16.0/24 が含まれている場合、DHCP スコープを 192.168.16.0 に設定すると、192.168.16.0/24 サブネットからのアドレスが必ず選択されるようになります。
- [ローカルIPアドレスプール（Local IP address pools）]：まず、サブネットを指定する最大 6 つのネットワーク オブジェクトを作成します。IPv4 と IPv6 に別々のプールを設定できます。次に、グループポリシーまたは接続プロファイルの [IPv4アドレスプール（IPv4 Address Pool）] および [IPv6アドレスプール（IPv6 Address Pool）] オプションで、これらのオブジェクトを選択します。IPv4 と IPv6 の両方を設定する必要はなく、サポートするアドレス方式のみを設定します。

また、グループポリシーと接続プロファイルの両方でプールを設定する必要もありません。グループポリシーは接続プロファイル設定をオーバーライドします。そのため、グループポリシーでプールを設定する場合は、接続プロファイルのオプションを空白のままにしてください。

プールはリストの順序で使用されることに注意してください。

RA VPN のグループ ポリシーの設定

グループポリシーは、リモートアクセス VPN 接続のための一連のユーザー指向の属性と値のペアです。接続プロファイルでは、トンネル確立後、ユーザー接続の条件を設定するグループポリシーが使用されます。グループポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

システムには、DfltGrpPolicy という名前のデフォルトグループポリシーがあります。必要なサービスを提供するために追加のグループポリシーを作成することができます。

手順

ステップ 1 **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

グループには、現在設定されている接続プロファイルおよびグループポリシーの数に関する概要情報が表示されます。

ステップ 2 目次で [グループポリシー（Group Policies）] をクリックします。

ステップ 3 次のいずれかを実行します。

- [+] ボタンをクリックして、新しいエンドポイント ID グループを作成します。グループポリシーのページの属性の説明については、次のトピックを参照してください。
  - 一般属性 （858 ページ）
  - セッション設定属性 （859 ページ）
  - アドレス割り当て属性 （859 ページ）
  - スプリット トンネリング属性 （860 ページ）
  - セキュアクライアント 属性 （861 ページ）
  - トラフィック フィルタ属性 （863 ページ）
  - Windows ブラウザ プロキシ属性 （864 ページ）
- 既存のグループポリシーを編集するには、編集ボタン（）をクリックします。

- 不要なグループを削除するには、削除ボタン（）をクリックします。現在、グループを接続プロファイルで使用することはできません。

一般属性

グループポリシーの全般的な属性では、グループの名前およびその他の基本設定を定義します。名前属性は唯一の必須属性です。

- [名前（Name）]：グループ ポリシーの名前。名前には最大 64 文字の長さを使用でき、スペースも使用できます。
- [説明（Description）]：デバイス グループの説明。説明には、最大 1,024 文字を使用できます。
- [DNSサーバー（DNS Servers）]：VPNに接続する際、クライアントがドメイン名の解決に使用する DNS サーバーを定義する DNS サーバーグループを選択します。必要なグループがまだ定義されていない場合は、[DNSグループの作成（Create DNS Group）] をクリックしてすぐに作成します。
- [バナー（Banner）]：ユーザーのログイン時に表示するバナーテキストまたはウェルカムメッセージです。デフォルトでは、バナーは表示されません。最大文字数は 496 文字です。セキュアクライアントは、 部分的な HTML をサポートしています。リモート ユーザーへバナーが適切に表示されることを確認するには、
 タグを使用して改行を示します。
- [デフォルトドメイン（Default Domain）]：RA VPN内のユーザーのデフォルトドメインの名前。例、example.com。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。
- **[Secure Clientプロファイル（Secure Client Profiles）]**：[+] をクリックし、このグループに使用するセキュアクライアントプロファイルを選択します。外部インターフェイスの完全修飾ドメイン名を設定すると（接続プロファイルで）、デフォルトプロファイルが自動的に作成されます。代わりに、自分用のクライアントプロファイルをアップロードすることもできます。スタンドアロン セキュアクライアント プロファイルエディタを使用してこれらのプロファイルを作成します。スタンドアロンAnyConnectプロファイルエディタは、software.cisco.comからダウンロードしてインストールできます。クライアントプロファイルを選択しない場合、セキュアクライアントクライアントはすべてのオプションにデフォルト値を使用します。このリストの項目は、プロファイル自体ではなくセキュアクライアントプロファイルオブジェクトです。新しいプロファイルを作成（およびアップロード）するには、ドロップダウンリストで **[新規Secure Clientプロファイルの作成（Create New Secure Client Profile）]** をクリックします。

  セキュアクライアントプロファイルに加えて、AMP イネーブラなどの セキュアクライアントモジュールプロファイルを選択できます。モジュールタイプごとに1つのプロファイルを選択できます。

セッション設定属性

グループポリシーのセッションの設定は、VPNを通じて接続できる時間と、接続を確立できる個別の接続数を制御します。

- [最大接続時間（Maximum Connection Time）]：ユーザーがログアウト、再接続せずにVPNに接続したままにできる最大時間（分）で、1～4473924または空白で指定します。デフォルトは無制限（空白）ですが、その場合でもアイドル タイムアウトは適用されます。
- [接続時間のアラート間隔（Connection Time Alert Interval）]：最大接続時間を指定した場合、アラート間隔は、次回の自動切断についてユーザーに警告を表示する、最大時間に達するまでの時間を定義します。ユーザーは、接続を終了し、再接続してタイマーを再起動することを選択できます。デフォルトは1分です。1 ～ 30 分を指定できます。
- [アイドルタイム（Idle Time）]：VPN 接続が自動的に閉じられる前にアイドル状態になる時間（分）で、1～35791394で指定します。指定した時間、接続で通信アクティビティがない場合、システムは接続を停止します。デフォルトは30分です。
- [アイドル時間のアラート間隔（Idle Time Alert Interval）]：アイドル セッションが原因の次回の自動切断について、ユーザーにアラートを表示するアイドル時間に達するまでの時間。アクティビティがあるとタイマーがリセットされます。デフォルトは1分です。1 ～ 30 分を指定できます。
- [ユーザーあたり同時ログイン（Simultaneous Logins Per User）]：ユーザーに許可する同時接続の最大数。デフォルトは3です。1～2147483647個の接続を指定できます。複数の同時接続を許可するとセキュリティの低下を招き、パフォーマンスに影響を及ぼすおそれがあります。

アドレス割り当て属性

グループポリシーのアドレスの割り当て属性は、グループのIPアドレスプールを定義します。ここで定義されているプールで、このグループを使用するすべての接続プロファイルで定義済みのプールがオーバーライドされます。接続プロファイルで定義済みのプールを使用する場合は、これらの設定を空白のままにします。

- [IPv4アドレスプール（IPv4 Address Pool）]、[IPv6アドレスプール（IPv6 Address Pool）]：これらのオプションは、リモートエンドポイントのアドレスプールを定義します。クライアントには、VPN 接続のために使用する IP バージョンに基づき、これらのプールからアドレスが割り当てられます。サポートする IP タイプごとにサブネットを定義するネットワーク オブジェクトを選択します。当該 IP バージョンをサポートしない場合は、リストを空のままにします。たとえば、IPv4 プールを「10.100.10.0/24」と定義できます。アドレス プールは、外部インターフェイスの IP アドレスと同じサブネット上に存在することはできません。

  ローカルアドレスの割り当てに使用する最大6個のアドレスプールのリストを指定できます。プールの指定順序は重要です。システムでは、プールの表示順に従いプールからアドレスが割り当てられます。

- [DHCPスコープ（DHCP Scope）]：接続プロファイルのアドレス プールにDHCPサーバーを設定した場合、DHCPスコープはこのグループのプールに使用するサブネットを識別します。DHCPサーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用するDHCPサーバーで定義されているアドレスプールのサブセットを選択できます。

  ネットワーク スコープを定義しない場合、DHCPサーバーはアドレス プールの設定順にプール内を探してIPアドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

  スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを含むネットワークオブジェクトを選択します。DHCPサーバーは、このIPアドレスが属するサブネットを判別し、そのプールからのIPアドレスを割り当てます。

  ルーティングの目的で可能な場合は常に、インターフェイスのIPアドレスを使用することを推奨します。たとえば、プールが10.100.10.2 ～ 10.100.10.254で、インターフェイスアドレスが10.100.10.1/24の場合、DHCPスコープとして10.100.10.1を使用します。ネットワーク番号は使用しないでください。オブジェクトがまだ存在しない場合は、[新しいネットワークの作成（Create New Network）]をクリックします。DHCPはIPv4アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

スプリット トンネリング属性

グループポリシーのスプリットトンネリング属性は、システムが内部ネットワーク用のトラフィックと外部方向トラフィックを処理する方法を定義します。スプリットトンネリングは、VPNトンネル（暗号化）とVPNトンネル外の残りのネットワークトラフィック（非暗号化、つまりクリアテキスト）を介して一部のネットワークトラフィックを誘導します。

- [IPv4スプリットトンネリング（IPv4 Split Tunneling）]、[IPv6スプリットトンネリング（IPv6 Split Tunneling）]：トラフィックがIPv4またはIPv6アドレスを使用するかどうかによって、さまざまなオプションを指定できますが、それぞれのオプションは同じです。スプリットトンネリングを有効にする場合は、ネットワークオブジェクトを選択する必要があるオプションのいずれかを指定します。
  - [トンネル経由のトラフィックをすべて許可する（Allow all traffic over tunnel）]：スプリット トンネリングを行いません。ユーザーがRA VPN接続を行うと、ユーザーのすべてのトラフィックは保護されたトンネルを通過します。これがデフォルトです。最も安全なオプションであるとも考えられます。
  - [トンネル経由で指定されたトラフィックを許可する（Allow specified traffic over the tunnel）]：宛先ネットワークとホスト アドレスを定義するネットワーク オブジェクトを選択します。これらの宛先へのトラフィックすべては、保護されたトンネルを通過します。その他のすべての宛先へのトラフィックは、クライアントによって、トンネル外の接続（ローカルWi-Fiまたはネットワーク接続など）にルーティングされます。

- [以下に指定したネットワークを除外する（Exclude networks specified below）]：宛先ネットワークまたはホストアドレスを定義するネットワークオブジェクトを選択します。これらの宛先へのトラフィックは、クライアントによって、トンネルの外の接続にルーティングされます。他の宛先へのトラフィックはトンネルを通過します。

- [スプリットDNS（Split DNS）]：クライアントが、クライアントで設定されている DNS サーバーに他の DNS 要求を送信することを許可しながら、セキュアな接続を介していくつかの DNS 要求を送信するようにシステムを設定することができます。次の DNS 動作を設定できます。

  - [スプリットトンネルポリシーに従ってDNS要求を送信する（Send DNS Request as per split tunnel policy）]：このオプションでは、スプリット トンネル オプションが定義されているのと同じ方法で DNS 要求が処理されます。スプリットトンネリングを有効にすると、DNS 要求は宛先アドレスに基づいて送信されます。スプリットトンネリングを有効にしていない場合、DNS 要求はすべて保護された接続を介します。

  - [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）]：スプリット トンネリングを有効にするが、すべての DNS 要求をグループで定義された DNS サーバーに保護された接続を介して送信する場合は、このオプションを選択します。

  - [指定したドメインのみをトンネル経由で送信（Send only specified domains over tunnel）]：保護された DNS サーバーが特定のドメインのアドレスだけを解決するようにしたい場合は、このオプションを選択します。次に、ドメインを指定します。ドメイン名はコンマで区切ります。例：example.com, example1.com。内部 DNS サーバーが内部ドメインの名前を解決し、外部 DNS サーバーが他のすべてのインターネットトラフィックを処理するようにする場合は、このオプションを使用します。

セキュアクライアント 属性

グループポリシーの セキュアクライアント 属性は、セキュアクライアントでリモートアクセス VPN 接続に使用されるいくつかの SSL および接続設定を定義します。

SSL 設定

- [Datagram Transport Layer Security（DTLS）の有効化（Enable Datagram Transport Layer Security (DTLS)）]：セキュアクライアントが SSL トンネルおよび DTLS トンネルの 2 つのトンネルを同時に使用することを許可するかどうか。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイムアプリケーションのパフォーマンスが向上します。DTLS を有効にしない場合、SSL VPN 接続を確立している セキュアクライアントユーザーは SSL トンネルのみで接続します。

- [DTLS圧縮（DTLS Compression）]：LZS を使用してこのグループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうか。[DTLS圧縮（DTLS Compression）] はデフォルトで無効になっています。

- [SSL圧縮（SSL Compression）]：データ圧縮を有効にするかどうか。有効にする場合は、使用するデータ圧縮の方法（[圧縮（Deflate）] または [LZS（LZS）]）。[SSL圧縮（SSL Compression）] はデフォルトで無効になっています。データ圧縮は、伝送速度を上げますが、各ユーザー セッションのメモリ要件と CPU 使用率も高めます。SSL 圧縮はデバイスの全体的なスループットを低下させます。

- [SSLキーの再生成方法（SSL Rekey Method）]、[SSLキーの再生成間隔（SSL Rekey Interval）]：クライアントは、暗号キーと初期化ベクトルを再ネゴシエートしながら VPN 接続キーを再生成して、接続のセキュリティを強化します。[なし（None）] を選択して、キーの再生成を無効にします。キーの再生成を有効にするには、新しいトンネルを作成するたびに [新しいトンネル（New Tunnel）] を選択します（[既存のトンネル（Existing Tunnel）] オプションは、[新しいトンネル（New Tunnel）] と同じアクションになります）。キーの再生成を有効にする場合は、キーの再生成間隔も設定します。デフォルトは 4 分です。間隔は、4 ～ 10080 分（1 週間）の範囲で設定できます。

接続の設定

- [DF（フラグメント化しない）ビットを無視する（Ignore the DF (Don't Fragment) bit）]：フラグメント化が必要なパケットの Don't Fragment（DF）ビットを無視するかどうか。DF ビットが設定されているパケットの強制フラグメンテーションを許可し、それらのパケットがトンネルを通過できるようにするには、このオプションを選択します。

- [クライアントバイパスプロトコル（Client Bypass Protocol）]：セキュア ゲートウェイによる（IPv6 トラフィックだけを予期しているときの）IPv4 トラフィックの管理方法や、（IPv4 トラフィックだけを予期しているときの）IPv6 トラフィックの管理方法を設定することができます。

  セキュアクライアントがヘッドエンドに VPN 接続するときに、ヘッドエンドは IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ヘッドエンドが セキュアクライアント 接続に IPv4 アドレスのみ、または IPv6 アドレスのみを割り当てた場合に、ヘッドエンドが IP アドレスを割り当てなかったネットワークトラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか（デフォルト、無効、オフ）、またはヘッドエンドをバイパスしてクライアントからの暗号化なし、つまり「クリアテキスト」としての送信を許可するか（有効、オン）を設定できるようになりました。

  たとえば、セキュアゲートウェイが セキュアクライアント 接続に IPv4 アドレスだけを割り当て、エンドポイントがデュアルスタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコルが無効の場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルが有効の場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

- [MTU]：セキュアクライアントによって確立された SSL VPN 接続の最大伝送ユニット（MTU）サイズ。デフォルトは 1406 バイトで、範囲は 576 ー 1462 バイトです。

- **[Secure ClientとVPNゲートウェイ間のキープアライブメッセージ（Keepalive Messages Between Secure Client and VPN Gateway）]**：トンネルでのデータの送受信にピアを使用で

きることを示すために、ピア間でキープアライブメッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信されます。デフォルトの間隔は 20 秒、有効な範囲は 15 ～ 600 秒です。

- [ゲートウェイ側の間隔でのDPD（DPD on Gateway Side Interval）]、[クライアント側の間隔でのDPD（DPD on Client Side Interval）]：ピアが応答しなくなったときに VPN ゲートウェイまたは VPN クライアントによる迅速な検出を確実に実行するには、Dead Peer Detection（DPD）を有効にします。ゲートウェイまたはクライアント DPD を個別に有効にすることができます。DPD メッセージのデフォルトの送信間隔は 30 秒です。間隔は、5～3600 秒にすることができます。

トラフィック フィルタ属性

グループポリシーのトラフィックフィルタ属性は、グループに割り当てられているユーザーに適用する制限を定義します。アクセス コントロール ポリシー ルールを作成する代わりにこれらの属性を使用することで、ホストまたはサブネット アドレスとプロトコル、または VLAN に基づいて、特定のリソースに RA VPN ユーザーを制限することができます。

デフォルトでは、RA VPN ユーザーは、保護されたネットワーク上の宛先へのアクセスがグループポリシーによって制限されることはありません。

- [アクセスリストのフィルタ（Access List Filter）]：拡張アクセス コントロール リスト（ACL）を使用してアクセスを制限します。スマート CLI の拡張 ACL オブジェクトを選択するか、[拡張アクセスリストの作成（Create Extended Access List）] をクリックして作成します。

  拡張 ACL では、送信元アドレス、宛先アドレス、およびプロトコル（IP TCP など）に基づいたフィルタリングが可能です。ACL はトップダウン方式で最初に一致したものから評価されるため、具体的なルールはより一般的なルールの前に配置してください。ACL の末尾には、暗黙的な「deny any」があります。そのため、いくつかのサブネットへのアクセスだけを拒否しながら、他のすべてのアクセスを許可する場合は、ACL の最後に「permit any」ルールを含めるようにしてください。VPN フィルタは初期接続にのみ適用されます。アプリケーションインスペクションのアクションによって開かれた SIP メディア接続などのセカンダリ接続には適用されません。

  拡張 ACL スマート CLI オブジェクトを編集しながらネットワークオブジェクトを作成することはできないため、グループポリシーを編集する前に、ACL を作成する必要があります。そうしないと、単純にオブジェクトを作成し、後でもう一度ネットワークオブジェクトを作成し、その後で必要なすべてのアクセス制御エントリを作成する必要があります。ACL を作成するには、**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Object）]** に移動し、オブジェクトを作成して、オブジェクトタイプとして [拡張アクセスリスト（Extended Access List）] を選択します。例については、グループによって RA VPN アクセスを制御する方法（908 ページ）を参照してください。

- [VPNをVLANに制限（Restrict Access to VLAN）]：（オプション）「VLAN マッピング」とも呼ばれます。この属性により、このグループ ポリシーが適用されるセッションの出力

VLANインターフェイスを指定します。システムは、このグループからのトラフィックすべてを、選択した VLAN に転送します。

この属性を使用して VLAN をグループ ポリシーに割り当て、アクセス コントロールを簡素化します。この属性に値を割り当てる方法は、ACL を使用してセッションのトラフィックをフィルタリングする方法の代替方法です。デバイスのサブインターフェイスで定義されている VLAN 番号を指定していることを確認します。値の範囲は 1 ～ 4094 です。

Windows ブラウザ プロキシ属性

グループポリシーの Windows ブラウザプロキシ属性は、ユーザーのブラウザで定義されたプロキシが動作しているかどうか、およびその動作方法を判断します。

[VPNセッション中のブラウザプロキシ（Browser Proxy During VPN Session）] に対して次のいずれかの値を選択できます。

- [エンドポイント設定のまま（No change in endpoint settings）]：HTTP のブラウザプロキシを設定するかどうかをユーザーが決定できます。設定されている場合、そのプロキシが使用されます。
- [ブラウザプロキシの無効化（Disable browser proxy）]：ブラウザに定義されているプロキシ（ある場合）を使用しません。どのブラウザ接続もプロキシを経由しません。
- [自動検出設定（Auto detect settings）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用を有効にします。
- [カスタム設定を使用（Use custom settings）]：HTTP トラフィックに対してすべてのクライアント デバイスで使用する必要があるプロキシを定義します。次を設定します。
  - [プロキシサーバーのIPまたはホスト名（Proxy Server IP or Hostname）]、[ポート（Port）]：プロキシ サーバーの IP アドレスまたはホスト名、およびプロキシ サーバーが使用するプロキシ接続のポート。ホストとポートを組み合わせた文字数が 100 文字を超えることはできません。
  - [ブラウザ免除リスト（Browser Exemption List）]：免除リストにあるホスト/ポートへの接続はプロキシを経由しません。プロキシを使用すべきでない宛先のすべてのホスト/ポート値を追加します。たとえば、www.example.com ポート 80 などです。リストに項目を追加するには、[追加（Add）] リンクをクリックします。項目を削除するには、ごみ箱アイコンをクリックします。すべてのアドレスとポートを合わせたプロキシ例外リスト全体で、255 文字を超えることはできません。

リモート アクセス VPN のモニタリング

リモート アクセス VPN 接続をモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。

- **show vpn-sessiondb** は VPN セッションに関する情報を表示します。これらの統計は **clear vpn-sessiondb** コマンドを使用してリセットできます。

- **show webvpn** *keyword* はリモートアクセス VPN 設定に関する情報を表示します。統計情報とインストールされている AnyConnect イメージが含まれます。**show webvpn ?** と入力し、使用可能なキーワードを確認します。
- **show aaa-server** はリモートアクセス VPN とともに使用されるディレクトリサーバーに関する統計情報を表示します。

リモート アクセス VPN のトラブルシューティング

リモート アクセス VPN 接続の問題の原因は、クライアントまたは Threat Defense のデバイス設定の可能性があります。次の各項で、発生する可能性のある主な問題のトラブルシューティングについて説明します。

SSL 接続問題のトラブルシューティング

ユーザーが セキュアクライアントをダウンロードするため、外部 IP アドレスに対し セキュアクライアント を使用せずに初めて SSL 接続しようとしたが接続できない場合には、次の手順を実行します。

1. リモートアクセス VPN 接続プロファイルにデフォルト以外のポートを設定した場合は、ユーザーが URL にポート番号を含めていることを確認します。たとえば、https://ravpn.example.com:4443 です。
2. クライアント ワークステーションから、外部インターフェイスの IP アドレスに ping を実行できるかどうかを確認します。実行できない場合は、ユーザのワークステーションからそのアドレスまでのルートが存在しない原因を特定します。
3. クライアント ワークステーションから、外部インターフェイスの完全修飾ドメイン名（FQDN）に ping を実行できるかどうかを確認します。この FQDN は、リモート アクセス（RA）VPN 接続プロファイルで定義されているものです。IP アドレスを ping できても、FQDN を ping できない場合は、クライアントおよび RA VPN 接続プロファイルで使用されている DNS サーバを更新し、FQDN と IP アドレスのマッピングを追加する必要があります。
4. 外部インターフェイスで提示される証明書をユーザが承認していることを確認します。ユーザはこの証明書を永久に受け入れる必要があります。
5. RA VPN 接続設定を調べ、正しい外部インターフェイスを選択していることを確認します。よくある誤りとして、RA VPN ユーザに面している外部インターフェイスではなく、内部ネットワークに面している内部インターフェイスを選択していることがあります。
6. SSL 暗号化が適切に設定されている場合は、外部スニファを使用して、TCP スリーウェイハンドシェイクが正常に実行されるかどうかを確認します。

セキュアクライアントのダウンロードおよびインストールの問題のトラブルシューティング

ユーザーが外部インターフェイスに SSL 接続可能で、セキュアクライアント パッケージをダウンロードおよびインストールできない場合、次の点を考慮してください。

- クライアントのオペレーティングシステムに対応する セキュアクライアント パッケージをアップロードしていることを確認してください。たとえば、ユーザーのワークステーションにLinuxが搭載されているのに、Linuxセキュアクライアントイメージをアップロードしなかった場合、インストールできるパッケージはありません。
- Windowsクライアントの場合、ソフトウェアのインストールには管理者権限が必要です。
- Windows クライアントの場合は、ワークステーションで ActiveX を有効にするか、または JRE 1.5 以降（JRE 7 を推奨）をインストールする必要があります。
- Safari ブラウザの場合、Java が有効であることが必要です。
- 別のブラウザを試してみてください。あるブラウザでは失敗しても、別のブラウザでは成功することがあります。

セキュアクライアント 接続問題のトラブルシューティング

外部インターフェイスに接続し、セキュアクライアントをダウンロードしてインストールできても、セキュアクライアントを使用して接続を完了できなかった場合、次のことを確認してください。

- DHCP を使用してクライアントに IP アドレスを提供しており、クライアントがアドレスを取得できない場合は、NAT ルールを確認します。RA VPN ネットワークに適用される NAT ルールには、ルート ルックアップ オプションが含まれている必要があります。ルートルックアップは、DHCP 要求が適切なインターフェイスを介して DHCP サーバーに確実に送信されるようにするために役立つ場合があります。
- 認証が失敗した場合、ユーザーが正しいユーザー名とパスワードを入力しており、ユーザー名が認証サーバーで正しく定義されていることを確認してください。認証サーバーもデータインターフェイスのいずれかを使用してアクセス可能である必要があります。

（注） 認証サーバーが外部ネットワークにある場合は、外部ネットワークへのサイト間 VPN 接続を設定し、リモートアクセス VPN インターフェイスアドレスを VPN 内に含める必要があります。詳細は、リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方法（892 ページ）を参照してください。

- リモートアクセス（RA）VPN 接続プロファイルで外部インターフェイスの完全修飾ドメイン名（FQDN）を設定した場合、クライアントデバイスから FQDN を ping できることを確認します。IP アドレスを ping できても、FQDN を ping できない場合は、クライアントおよび RA VPN 接続プロファイルで使用されている DNS サーバーを更新し、FQDN と IP アドレスのマッピングを追加する必要があります。外部インターフェイスの FQDN を指定した時に生成されたデフォルトの セキュアクライアントプロファイルを使用している場合、DNS が更新されるまでは IP アドレスを使用するようにサーバーアドレスを編集する必要があります。
- 外部インターフェイスで提示される証明書をユーザが承認していることを確認します。ユーザはこの証明書を永久に受け入れる必要があります。
- ユーザーのセキュアクライアントに複数の接続プロファイルが含まれている場合、正しいプロファイルを選択していることを確認します。
- クライアント側の設定がすべて正しいと考えられる場合は、Threat Defense デバイスに SSH 接続し、**debug webvpn** コマンドを入力します。接続試行中に表示されたメッセージを確認します。

RA VPN トラフィック フローの問題のトラブルシューティング

ユーザが安全なリモート アクセス（RA）VPN 接続を確立できても、トラフィックの送受信ができない場合は、次の操作を実行してください。

1. クライアントを切断して再接続します。これで、問題が解決することがあります。
2. セキュアクライアントで、トラフィック統計を確認して、送信カウンタと受信カウンタの両方が増えているかどうかを確認します。受信パケットカウントがゼロのままの場合、Threat Defense デバイスはトラフィックを返していません。Threat Defense の設定に問題がある可能性があります。一般的な問題を次に示します。
   - アクセスルールでトラフィックをブロックしている。アクセス制御ポリシーのルールで、ネットワーク内と RA VPN アドレス プール間のトラフィックを妨害しているルールがないかを確認します。デフォルトのアクションでトラフィックがブロックされている場合は、明示的な [許可（Allow）] ルールを作成する必要があります。
   - VPN フィルタがトラフィックをブロックしています。接続プロファイルのグループポリシーで設定されている ACL トラフィック フィルタまたは VLAN フィルタを確認します。グループポリシーに基づいてトラフィックをフィルタリングしている場合、またはその方法によっては、ACL で調整を行うか、VLAN を変更する必要があります。
   - NAT ルールが、RA VPN トラフィックでバイパスされていない。すべての内部インターフェイスの RA VPN 接続で NAT がオフに設定されていることを確認してください。または、NAT ルールが内部ネットワークとインターフェイス、および RA VPN アドレス プールと外部インターフェイス間の通信を妨害していないことを確認してください。

- ルートが誤って設定されている。すべての定義されたルートが有効で正しく機能していることを確認します。たとえば、外部インターフェイス用に定義したスタティック IP アドレスがある場合、ルーティング テーブルにデフォルト ルート（0.0.0.0/0 および ::/0）が含まれていることを確認します。
- RA VPN の DNS サーバとドメイン名が正しく設定されており、クライアント システムで正しく使用されていることを確認します。DNS サーバに到達可能であることを確認します。
- RA VPN でスプリットトンネリングが有効になっている場合、指定した内部ネットワークへのトラフィックがトンネルを通っており、他のすべてのトラフィックがトンネルをバイパスしている（Threat Defense デバイスが認識しない）ことを確認します。

3. Threat Defense デバイスに SSH 接続し、リモートアクセス VPN との間でトラフィックが送受信されていることを確認します。次のコマンドを使用します。
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

リモート アクセス VPN の例

以下に、リモート アクセス VPN を設定する例を示します。

RADIUS 認可変更の実装方法

ダイナミック認証とも呼ばれる RADIUS 認可変更（CoA）は、脅威に対する防御 リモートアクセス VPN にエンドポイントセキュリティを提供します。RA VPN の重要な課題は、侵害されたエンドポイントに対して内部ネットワークを保護し、ウイルスやマルウェアの影響を受けたときに、エンドポイントへの攻撃を修復することによって、エンドポイント自体を保護することです。エンドポイントと内部ネットワークは、RA VPN セッションの前、最中、および後のすべてのフェーズで保護する必要があります。RADIUS CoA 機能は、この目標を達成するのに役に立ちます。

Cisco Identity Services Engine（ISE）RADIUS サーバーを使用する場合は、認可変更ポリシーの適用を設定できます。

ISE 認可変更機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザーまたはユーザーグループのポリシーが変更されると、ISE は CoA メッセージを 脅威に対する防御 デバイスに送信して認証を再初期化し、新しいポリシーを適用します。Inline Posture Enforcement Point（IPEP）では、脅威に対する防御 デバイスによって確立された各 VPN セッションにアクセスコントロールリスト（ACL）を適用する必要はありません。

CoA 中に変更できる属性は、リダイレクト URL、リダイレクト ACL、およびセキュリティグループタグです。

ここでは、CoA の動作とその設定方法について説明します。

認可変更へのシステム フロー

Cisco ISE には、プロセス、ファイル、レジストリエントリ、ウイルス対策保護、スパイウェア対策保護、およびホストにインストールされているファイアウォール ソフトウェアなどの条件に対するエンドポイントのコンプライアンスを評価するクライアント ポスチャ エージェントがあります。管理者はその後、エンドポイントが条件に準拠するまでネットワークアクセスを制限したり、修復方法を確立できるようにローカルユーザーの権限を昇格したりできます。ISE ポスチャは、クライアント側評価を実行します。クライアントは、ISE からポスチャ要件ポリシーを受信し、ポスチャデータ収集を実行し、結果をポリシーと比較し、評価結果を ISE に返します。

次に、認可変更（CoA）処理のための 脅威に対する防御 デバイス、ISE、および RA VPN クライアントの間のシステム フローを示します。

1. リモートユーザーは、セキュアクライアントを使用して、脅威に対する防御デバイスとの RA VPN セッションを開始します。
2. 脅威に対する防御 デバイスはそのユーザーの RADIUS Access-Request メッセージを ISE サーバーに送信します。
3. クライアントポスチャはこの時点で不明であるため、ISE は不明なポスチャに対して設定されている認証ポリシーにユーザーを一致させます。このポリシーは、ISE が RADIUS Access-Accept の応答で 脅威に対する防御 に送信する次の cisco-av-pair オプションを定義します。

   - **url-redirect-acl=***acl_name*。ここで *acl_name* は、脅威に対する防御 デバイスで設定されている拡張 ACL の名前です。この ACL は、どのユーザー トラフィックを ISE サーバーにリダイレクトすべきか（HTTP トラフィック）を定義します。次に例を示します。

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*：トラフィックのリダイレクト先 URL。次に例を示します。

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   ホスト名を解決できるように、データインターフェイスの DNS を設定する必要があります。接続プロファイルのグループポリシーにトラフィックフィルタリングも設定する場合は、クライアントプールがポート（この例ではTCP/8443）経由でISEサーバーに到達できることを確認します。
4. 脅威に対する防御 デバイスは RADIUS Accounting-Request 開始パケットを送信し、ISE から応答を受信します。アカウンティング要求には、セッション ID、VPN クライアントの外部 IP アドレス、脅威に対する防御 デバイスの IP アドレスを含む、セッションの詳細がすべて含まれます。ISEはセッションIDを使用してそのセッションを識別します。脅威に対する防御デバイスはさらに、定期的な中間アカウント情報を送信します。この情報で最

も重要な属性は、脅威に対する防御デバイスによってクライアントに割り当てられている IP アドレスを持つ Framed-IP-Address です。

5. ポスチャ状態が不明な場合、脅威に対する防御 デバイスはリダイレクト ACL に一致するクライアントからのトラフィックをリダイレクト URL にリダイレクトします。ISE は、必要なポスチャ コンプライアンス モジュールがクライアントにあるかどうかを判断し、必要に応じてユーザーにインストールを指示します。

6. エージェントは、クライアントデバイスにインストールされると、ISE ポスチャポリシーで設定されたチェックを自動的に実行します。クライアントは ISE と直接通信します。クライアントは ISE にポスチャレポートを送信します。このレポートには、SWISS プロトコルおよびポート TCP/UDP 8905 を使用した複数の交換を含めることができます。

7. ISE がエージェントからポスチャレポートを受信すると、認証ルールをもう一度処理します。この時点で、ポスチャの結果が認識され、別のルールがクライアントと一致するようになります。ISE は RADIUS CoA のパケットを送信します。このパケットには準拠または非準拠のいずれかのエンドポイント向けのダウンロード可能 ACL（DACL）が含まれます。たとえば、準拠 DACL はすべてのアクセスを許可しますが、非準拠 DACL はすべてのアクセスを拒否することがあります。DACL の内容は、ISE 管理者によって設定されます。

8. 脅威に対する防御 デバイスがリダイレクションを削除します。このデバイスが DACL をキャッシュしていない場合、デバイスは ISE からダウンロードするために Access-Request を送信する必要があります。特定の DACL が VPN セッションに関連付けられますが、デバイス構成の一部にはなりません。

9. RA VPN ユーザーがもう一度 Web ページにアクセスしようとすると、ユーザーはそのセッション用に 脅威に対する防御 デバイスにインストールされている DACL によって許可されたすべてのリソースにアクセスできます。

（注） エンドポイントが必須要件を満たしていない場合、および手動修復が必要な場合は、セキュアクライアントで修復ウィンドウが開き、アクションを必要とする項目が表示されます。修復ウィンドウはバックグラウンドで実行されるため、ネットワーク アクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。セキュアクライアントの ISE ポスチャタイル部分で [詳細（Details）] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。

Threat Defense デバイスでの認可変更の設定

認可変更ポリシーのほとんどは、ISE サーバーで設定されます。ただし、脅威に対する防御デバイスは適切に ISE に接続するように設定する必要があります。次の手順では、この設定の 脅威に対する防御 側の設定方法について説明します。

始める前に

任意のオブジェクトでホスト名を使用する場合、データおよび管理トラフィック用の DNS の設定 （943 ページ）で説明したように、データインターフェイスと一緒に使用できるように

DNS サーバーが設定されていることを確認します。通常は、システムを完全に機能させるために DNS を設定する必要があります。

手順

ステップ 1 ISE への初期接続をリダイレクトするように、拡張アクセスコントロールリスト（ACL）を設定します。

リダイレクト ACL の目的は、ISE がクライアントポスチャを評価できるように、初期トラフィックを ISE に送信することです。ACL は、ISE に HTTPS トラフィックを送信しますが、ISE 宛てのトラフィックや、名前解決のために DNS サーバーに送信されるトラフィックは送信しません。リダイレクト ACL の例を次に示します。

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

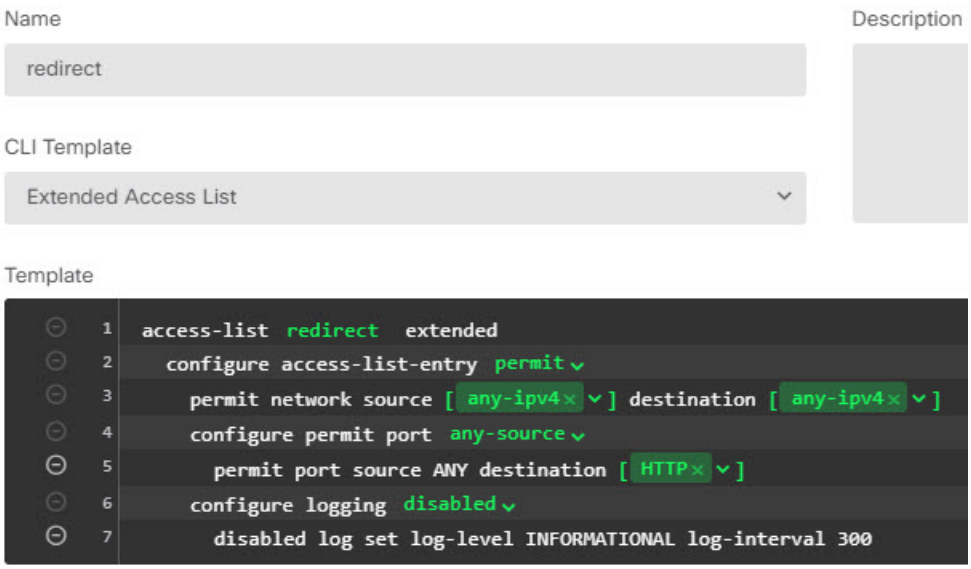
ただし、ACL には、最後のアクセス制御エントリ（ACE）として暗黙の「deny any any」が含まれることに注意してください。この例では、TCP ポート www（つまりポート 80）に一致する最後の ACE は、最初の 3 つの ACE に一致するすべてのトラフィックと一致しないため、これらは冗長となります。単純に最後の ACE を使用して ACL を作成し、同じ結果を得ることもできます。

リダイレクト ACL では、permit および deny アクションによって、ACL に一致するトラフィックが特定されることに注意してください（permit は一致、deny は不一致）。トラフィックは実際にはドロップされず、拒否されたトラフィックは ISE にリダイレクトされません。

リダイレクト ACL を作成するには、Smart CLI オブジェクトを設定する必要があります。

a) **[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [スマートCLI（Smart CLI）] > [オブジェクト（Objects）]** を選択します。
b) [+] をクリックして新しいオブジェクトを作成します。
c) ACL の名前を入力します。たとえば、**redirect** などと入力します。
d) [CLIテンプレート（CLI Template）] の場合は、[拡張アクセスリスト（Extended Access List）] を選択します。
e) [テンプレート（Template）] 本文で次のように設定します。
   - configure access-list-entry action = permit
   - source-network = any-ipv4
   - destination-network = any-ipv4
   - configure permit port = any-source
   - destination-port = HTTP
   - configure logging = disabled

ACE は次のようになります。



f) [OK] をクリックします。

この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

（注） この ACL は IPv4 にのみ適用されます。IPv6 のサポートも追加したい場合は、属性がすべて同じ 2 つ目の ACE を追加します。ただし、送信元ネットワークと宛先ネットワークに any-ipv6 を選択します。ISE または DNS サーバーへのトラフィックはリダイレクトされないようにするために、他の ACE を追加することもできます。最初に、それらのサーバーの IP アドレスを保持するホストネットワーク オブジェクトを作成する必要があります。

ステップ 2 RADIUS サーバーグループをダイナミック認証用に設定します。

ダイナミック認証とも呼ばれる認可変更を有効にするには、RADIUS サーバーとサーバーグループオブジェクトでいくつかの重要なオプションを正確に選択する必要があります。次の手順では、これらの属性に焦点を当てています。これらのオブジェクトの詳細については、RADIUS サーバおよびグループ （200 ページ）を参照してください。

a) **[オブジェクト（Objects）]** > **[アイデンティティ ソース（Identity Sources）]** を選択します。

b) **[+]** > **[RADIUSサーバー（RADIUS Server）]** をクリックします。

c) サーバーの名前と、ISE RADIUS サーバーのホスト名または IP アドレス、認証ポート、およびサーバーに設定されている秘密鍵を入力します。必要に応じてタイムアウトを調整します。これらのオプションは、ダイナミック認証には直接関連していません。

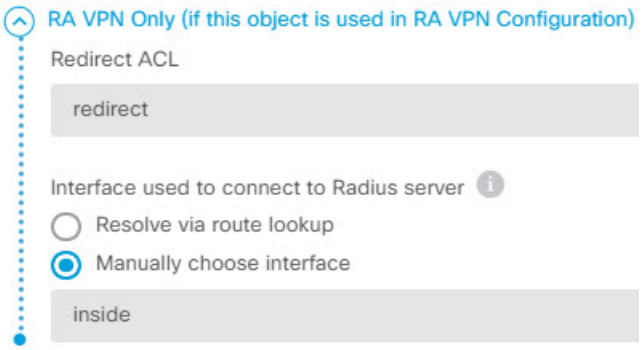
d) [RA VPN専用（RA VPN Only）] リンクをクリックし、次のオプションを設定します。

- [リダイレクトACL（Redirect ACL）]：リダイレクト用に作成した拡張 ACL を選択します。この例では、redirect という名前の ACL を使用します。

- [RADIUSサーバーに接続するために使用されるインターフェイス（Interface Used to Connect to RADIUS Server）]：[インターフェイスを手動で選択する（Manually Choose Interface）] を選択し、サーバーに到達できるインターフェイスを選択します。システムがインターフェイスでCoAリスナーを適切に有効化できるように、特定のインターフェイスを選択する必要があります。

  Device Manager 管理アクセスにもこのサーバーを使用する場合、このインターフェイスは無視されます。管理アクセスの試行は、常に管理IPアドレスを介して認証されます。

次の例は、内部インターフェイスに設定されているオプションを示しています。



e) [OK] をクリックしてサーバーオブジェクトを保存します。

複数の重複する ISE RADIUS サーバーによる冗長設定がある場合、これらのサーバーそれぞれにサーバーオブジェクトを作成します。

f) **[+] > [RADIUSサーバーグループ（RADIUS Server Group）]** をクリックします。

g) サーバーグループの名前を入力し、必要な場合は、デッドタイムと最大試行回数を調整します。

h) ISE サーバーが別のポートを使用するように設定されている場合は、**[ダイナミック認証（Dynamic Authorization）]** オプションを選択し、ポート番号を変更します。ポート 1700 は、CoA パケットをリッスンするために使用されるデフォルトのポートです。

i) AD サーバーを使用してユーザーを認証するように RADIUS サーバーが設定されている場合は、この RADIUS サーバーと組み合わせて使用される AD サーバーを指定する [RADIUSサーバーをサポートするレルム（Realm that Supports the RADIUS Server）] を選択します。レルムが存在していない場合は、リストの下部にある [新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックして作成します。

j) [RADIUSサーバー（RADIUS Server）] の下で [+] をクリックし、RA VPN 用に作成したサーバーオブジェクトを選択します。

k) [OK] をクリックしてサーバーグループオブジェクトを保存します。

ステップ 3 **[デバイス（Device）] > [RA VPN] > [接続プロファイル（Connection Profiles）]** を選択し、この RADIUS サーバーグループを使用する接続プロファイルを作成します。

[AAA認証（AAA Authentication）] を使用し（単独または証明書と一緒に）、[ユーザー認証用のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]、[認可

（Authorization）]、および [アカウンティング（Accounting）] オプションでサーバー グループを選択します。

組織での要件に応じて、その他すべてのオプションを設定します。

（注） DNS サーバーに VPN ネットワーク経由で到達する場合、接続プロファイルで使用されるグループ ポリシーを編集し、スプリット トンネリング属性ページで [スプリットDNS（Split DNS）] オプションを設定します。

ISE での認可変更の設定

認可変更設定のほとんどは、ISE サーバーで設定されます。ISE にはエンドポイントデバイス上で実行されるポスチャ アセスメント エージェントがあり、ISE はデバイスと直接通信してポスチャ ステータスを決定します。脅威に対する防御デバイスは基本的に、特定のエンドユーザーの処理に関する ISE からの指示を待ちます。

ポスチャ アセスメント ポリシーの設定の詳細は、このドキュメントの範囲外です。ただし、次の手順では、いくつかの基本について説明します。この手順を ISE の設定の開始点として使用します。正確なコマンドパス、ページ名、および属性名は、リリースごとに変更される場合があることに注意してください。使用している ISE のバージョンによっては、異なる用語または構成を使用する場合があります。

サポートされる最小の ISE リリースは 2.2 パッチ 1 です。

始める前に

この手順では、ISE RADIUS サーバーでユーザーがすでに設定済みであると想定しています。

手順

ステップ 1 **[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] > [ネットワーク デバイス（Network Devices）]** を選択し、脅威に対する防御 デバイスを ISE ネットワーク デバイス インベントリに追加して、RADIUS の設定を行います。

[RADIUS認証設定（RADIUS Authentication Settings）] を選択し、脅威に対する防御 RADIUS サーバー オブジェクトで設定されているものと同じ [共有秘密（Shared Secret）] を設定します。必要な場合は、[CoA ポート（CoA Port）] 番号を変更し、脅威に対する防御 RADIUS サーバー グループ オブジェクトで同じポートを設定していることを確認します。

ステップ 2 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [ダウンロード可能ACL（Downloadable ACLs）]** を選択します。

2 つのダウンロード可能 ACL（DACL）を作成します。一つは準拠エンドポイント用、もう一つは非準拠エンドポイント用です。

たとえば、非準拠エンドポイントへのすべてのアクセスを拒否（deny ip any any）し、準拠エンドポイントのすべてのアクセスを許可（deny ip any any）することができます。ユーザーに求められる正確なアクセスを準拠状態に基づいて提供するために、これらのDACLは必要なだけ複雑にすることができます。これらの DACL は認証プロファイルで使用します。

ステップ 3 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認可（Authorization）] > [認可プロファイル（Authorization Profile）]** を選択し、必要なプロファイルを設定します。

次の状態のプロファイルが必要です。それぞれの最小属性が表示されます。

- [不明（Unknown）]：不明なポスチャ プロファイルはデフォルトのポスチャ プロファイルです。すべてのエンドポイントは、RA VPN 接続の最初の確立時にこのポリシーに一致します。このルールのポイントは、リダイレクト ACL と URL を適用し、ポスチャエージェントがエンドポイント上に存在していない場合は、これをダウンロードすることです。エンドポイントは、エージェントがインストールされていない場合、またはインストールが失敗した場合、このプロファイルが適用されたままとなります。そうでない場合、エンドポイントはポスチャを評価した後に準拠または非準拠プロファイルに移行します。

  最小属性は次のとおりです。

  - [名前（Name）]：PRE_POSTURE など。
  - [アクセスタイプ（Access Type）]：[ACCESS_ACCEPT] を選択します。
  - [共通タスク（Common Tasks）]：[Webリダイレクション（CWA、DRW、MDM、NSP、CPP）（Web Redirection (CWA, DRW, MDM, NSP, CPP)）] を選択し、次に [クライアント プロビジョニング（ポスチャ）（Client Provisioning (Posture)）] を選択し、脅威に対する防御 デバイスで設定したリダイレクト ACL の名前を入力します。[値（Value）] では、[クライアントプロビジョニング ポータル（Client Provisioning Portal）] を選択します（まだ選択していない場合）。
  - [属性の詳細（Attribute Details）] には、url-redirect-acl および url-redirect の 2 つの cisco-av-pair 値が表示されている必要があります。ISE はこのデータを 脅威に対する防御 デバイスに送信します。これにより、RA VPN ユーザーセッションに条件が適用されます。

- [準拠（Compliant）]：ポスチャ アセスメントが完了した後、エンドポイントに設定されたすべての要件を満たしている場合、クライアントは準拠と見なされてこのプロファイルを取得します。通常、このクライアントにはフルアクセスを付与します。

  最小属性は次のとおりです。

  - [名前（Name）]：FULL_ACCESS など。
  - [アクセスタイプ（Access Type）]：[ACCESS_ACCEPT] を選択します。
  - [共通タスク（Common Tasks）]：[DACL名（DACL Name）] を選択し、準拠ユーザー向けに PERMIT_ALL_TRAFFIC などのダウンロード可能 ACL を選択します。ISE は ACL を 脅威に対する防御 デバイスに送信します。デバイスは、これをユーザーセッ

ションに適用します。このDACLは、ユーザーセッションの初期のリダイレクトACLを置き換えます。

- [非準拠（Non-compliant）]：ポスチャアセスメントによってエンドポイントがすべての要件を満たしていないことが決定された場合、必要な更新プログラムをインストールするなどにより、クライアントがエンドポイントを準拠させることができるカウントダウンが存在します。セキュアクライアントは、準拠の問題をユーザーに通知します。カウントダウンの間、エンドポイントは不明な準拠状態になります。カウントダウンの期限が切れてもエンドポイントが非準拠のままである場合、セッションは非準拠としてマークされ、非準拠プロファイルが取得されます。通常、このエンドポイントに対するすべてのアクセスを禁止するか、少なくとも何らかの方法でアクセスを制限します。

  最小属性は次のとおりです。

  - [名前（Name）]：Non_Compliant など。
  - [アクセスタイプ（Access Type）]：[ACCESS_ACCEPT] を選択します。
  - [共通タスク（Common Tasks）]：[DACL名（DACL Name）] を選択し、非準拠ユーザー向けに DENY_ALL_TRAFFIC などのダウンロード可能 ACL を選択します。ISE は ACL を 脅威に対する防御 デバイスに送信します。デバイスは、これをユーザーセッションに適用します。このDACLは、ユーザーセッションの初期のリダイレクトACL を置き換えます。

ステップ 4 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアントプロビジョニング（Client Provisioning）] > [リソース（Resources）]** を選択し、次のリソースを設定します。

- [AnyConnectパッケージ（AnyConnect package）]：software.cisco.com からダウンロードしたヘッドエンドパッケージ ファイル。サポートするクライアント プラットフォームごとに個別のパッケージが必要です。そのため、AnyConnectDesktopWindows などの複数のタイプを設定する必要があります。
- [ISEポスチャ設定ファイル（タイプ：AnyConnectProfile）（ISE Posture Configuration File (Type: AnyConnectProfile)）]：この設定ファイルは、コンプライアンス モジュールがエンドユーザーのデバイスを評価するために使用する設定を定義します。このファイルはまた、ユーザーが非準拠デバイスを準拠させるために使用できる時間の長さを定義します。
- [コンプライアンス モジュール パッケージ（タイプ：ComplianceModule）（Compliance Module Package (Type: ComplianceModule)）]：セキュアクライアント コンプライアンス モジュールファイルは、エンドポイントのコンプライアンスを確認するためにインストールされたAnyConnectパッケージにプッシュされるファイルです。[Ciscoサイトからリソースを追加（Add Resource from Cisco Site）] コマンドを使用してこのファイルをダウンロードします。設定した セキュアクライアント パッケージに基づいた正しいモジュールをダウンロードしてください。そうしないと、ユーザーはダウンロードに失敗します。software.cisco.com で、ISEComplianceModule フォルダ内の セキュアクライアント リストでこれらのファイルを検索することもできます。

- [AnyConnect設定ファイル（タイプ：AnyConnectConfig）（AnyConnect Configuration File (Type: AnyConnectConfig)）]：これらの セキュアクライアント リリース固有設定は、[AnyConnectパッケージ（AnyConnect Package）]、[コンプライアンスモジュール（Compliance Module）]、および適用する [ISEポスチャ（ISE Posture）] を定義します。パッケージは OS 固有であるため、サポートするクライアント OS（Windows、MAC、Linux など）ごとに個別の設定ファイルを作成します。

ステップ 5 **[ポリシー（Policy）] > [クライアントプロビジョニング（Client Provisioning）]** を選択し、クライアント プロビジョニング ポリシーを設定します。

CoA を実装する必要があるオペレーティングシステムごとに、CoA_ClientProvisionWin などの名前を持つ新しいルールを作成します。ルールに適したオペレーティングシステムを選択し、[結果（Results）] で、OS 用に作成した セキュアクライアント 設定ファイルを [エージェント（Agent）] として選択します。

置換するデフォルトの OS 固有のルールを無効にします。

ステップ 6 ポスチャポリシーを設定します。

この手順では、組織に適したポスチャ要件を作成します。

- **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）]** を選択し、満たす必要がある単純なポスチャ条件を定義します。たとえば、ユーザーに特定のアプリケーションのインストールを要求する場合があります。
- **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ポスチャ（Posture）] > [要件（Requirements）]** を選択し、エンドポイントのコンプライアンスモジュール要件を定義します。
- **[ポリシー（Policy）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）]** を選択し、サポートされるオペレーティングシステムのポリシーを設定します。

ステップ 7 **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）] > [デフォルト（Default）] > [認証ポリシー（Authorization Policy）]** を選択し、ポリシーを作成します。

準拠条件ごとにルールを追加します。次のサンプル値は、前の手順の例に基づいています。

- [不明（Unknown）]：pre-posture およびポスチャ ダウンロード用。
  - [名前（Name）]：PRE_POSTURE など
  - [条件（Conditions）]：”Session-PostureStatus EQUALS Unknown” および “Radius-NAS-Port-Type EQUALS Virtual”。
  - [プロファイル（Profiles）]：PRE_POSTURE など。
- [準拠（Compliant）]：ポスチャ要件を満たすクライアント用。
  - [名前（Name）]：FULL_ACCESS など
  - [条件（Conditions）]：”Session-PostureStatus EQUALS Compliant” および “Radius-NAS-Port-Type EQUALS Virtual”。

- [プロファイル（Profiles）]：FULL_ACCESS など

- [非準拠（Non-compliance）]：ポスチャ要件を満たさないクライアント用。
  - [名前（Name）]：Non_Compliant など。
  - [条件（Conditions）]：”Session-PostureStatus EQUALS NonCompliant” および “Radius-NAS-Port-Type EQUALS Virtual”。
  - [プロファイル（Profiles）]：Non_Compliant など

ステップ 8 （オプション）**[管理（Administration）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[再評価（Reassessments）]** を選択し、ポスチャ再評価を有効にします。

デフォルトでは、ポスチャは接続時にのみ評価されます。ポスチャ再評価を有効にして、接続されたエンドポイントのポスチャを定期的に確認できます。再評価間隔を設定して、発生頻度を決定できます。

システムが再評価に失敗した場合は、システムの応答方法を定義できます。ユーザーの続行を許可する（接続したまま）、ユーザーをログオフさせる、またはユーザーにシステムの修復を依頼することができます。

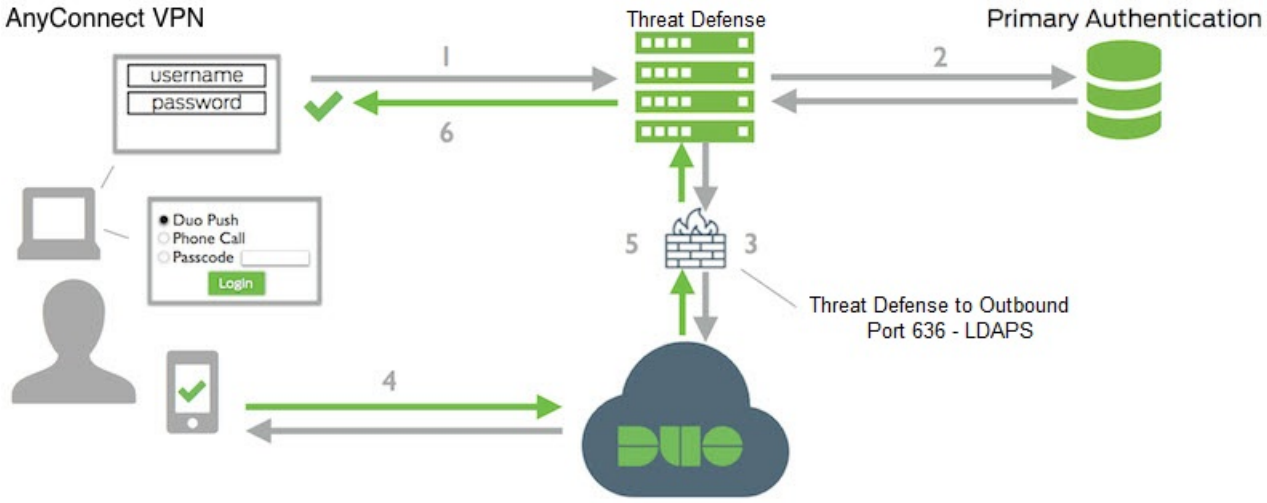
Duo LDAP を使用した二要素認証の設定方法

プライマリソースとしての Microsoft Active Directory（AD）または RADIUS サーバーとともに、セカンダリ認証ソースとして Duo LDAP サーバーを使用できます。Duo LDAP を使用すると、セカンダリ認証により、プライマリ認証が Duo パスコード、プッシュ通知、または電話コールで検証されます。

以降のトピックでは設定についてさらに詳しく説明します。

Duo LDAP セカンダリ認証のシステム フロー

次の図は、LDAP を使用した二要素認証を実現するために、脅威に対する防御 と Duo がどのように連携するかを示しています。



次に、システムフローについて説明します。

1. ユーザーは、脅威に対する防御 デバイスへのリモートアクセス VPN 接続を確立し、ユーザー名とパスワードを提供します。
2. Threat Defense は、プライマリ認証サーバー（Active Directory や RADIUS など）でプライマリ認証の試行を認証します。
3. プライマリ認証が機能する場合、脅威に対する防御 は Duo LDAP サーバーにセカンダリ認証の要求を送信します。
4. 要求を受けた Duo は、プッシュ構成、パスコード付きのテキストメッセージ、または電話コールによって、ユーザーを個別に認証します。ユーザーはこの認証を正常に完了する必要があります。
5. Duo は 脅威に対する防御 デバイスに応答して、ユーザーが正常に認証されたかどうかを示します。
6. セカンダリ認証が成功すると、脅威に対する防御 デバイスは、ユーザーの セキュアクライアント クライアントとのリモートアクセス VPN 接続を確立します。

Duo LDAP セカンダリ認証の設定

次の手順では、セカンダリ認証ソースとして Duo LDAP を使用して、リモートアクセス VPN の二要素認証を設定するエンドツーエンドのプロセスについて説明します。この設定を完了するには、Duo のアカウントを取得し、Duo から情報を取得する必要があります。

手順

ステップ 1 Duo アカウントを作成し、統合鍵、秘密鍵、および API ホスト名を取得します。

次に、プロセスの概要を示します。詳細については、Duo の Web サイト（https://duo.com）を参照してください。

a) Duo アカウントにサインアップします。
b) Duo Admin Panel にログインし、[アプリケーション（Applications）] に移動します。
c) [アプリケーションの保護（Protect an Application）] をクリックし、アプリケーションリストで Cisco SSL VPN を探します。[アプリケーションの保護（Protect this Application）] をクリックし、統合鍵、秘密鍵、および API ホスト名を取得します。詳細については、Duo の『*Getting Started*』ガイド（https://duo.com/docs/getting-started）を参照してください。

ステップ 2 Duo LDAP サーバーの Duo LDAP アイデンティティソースを作成します。

Duo LDAP オブジェクトを作成するには、脅威に対する防御 API を使用する必要があります。Device Manager を使用して作成することはできません。API Explorer を使用するか、独自のクライアント アプリケーションを作成してオブジェクトを作成できます。次の手順では、API Explorer を使用してオブジェクトを作成する方法について説明します。

a) Device Manager にログインし、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

ブラウザの設定に応じて、API エクスプローラが別のタブまたはウィンドウで開きます。

b) （オプション）Duo LDAP サーバーに接続するためにシステムが使用するインターフェイスの特定に必要な値を取得します。

インターフェイスを指定しない場合は、ルーティングテーブルが使用されます。必要に応じて、Duo LDAP サーバーのスタティックルートを作成できます。または、Duo LDAP オブジェクトで使用するインターフェイスを指定できます。インターフェイスを指定する場合は、インターフェイスグループのさまざまなGETメソッドを使用して、必要な値を取得します。物理インターフェイス、サブインターフェイス、EtherChannel、または VLAN インターフェイスを使用できます。たとえば、物理インターフェイスの値を取得するには、GET/ devices/default/interfaces メソッドを使用して、使用する必要があるインターフェイスのオブジェクトを検索します。インターフェイス オブジェクトから次の値が必要です。

- id
- type
- version
- name

c) [DuoLDAPIdentitySource] 見出しをクリックして、グループを開きます。
d) [POST /object/duoldapidentitysources] メソッドをクリックします。
e) [パラメータ（Parameters）] 見出しの [本文（body）] 要素について、右側の [データタイプ（Data Type）] 列の [サンプル値表示（Example Value display）] ボックスをクリックします。このアクションにより、本文の値の編集ボックスに例がロードされます。
f) [本文の値（body value）] 編集ボックスで、次の手順を実行します。

- 属性行 [version]、[id] を削除します（これらの属性は、PUT 呼び出しには必要ですが POST には必要ありません）。
- [名前（name）] には、Duo-LDAP-server などのオブジェクトの名前を入力します。

- [説明（description）] では、参照用にオブジェクトのわかりやすい説明を入力するか、属性行を削除します。
- [apiHostname] には、Duo アカウントから取得した API ホスト名を入力します。ホスト名は API-XXXXXXXX.DUOSECURITY.COM のような形式になります。X を一意の値に置き換えます。大文字は必須ではありません。
- [ポート（port）] には、LDAPS に使用する TCP ポートを入力します。Duo から別のポートを使用するように指示されていない限り、この値は 636 になります。アクセス制御リストで、必ずこのポートを介した Duo LDAP サーバーへのトラフィックを許可してください。
- [タイムアウト（timeout）] には、Duo サーバーに接続する際のタイムアウトを秒単位で入力します。値は 1 ー 300 秒です。デフォルトは 120 です。デフォルトを使用するには、120 を入力するか、属性行を削除します。
- [IntegrationKey] には、Duo アカウントから取得した統合キーを入力します。
- [secretKey] には、Duo アカウントから取得した秘密キーを入力します。この鍵はその後マスクされます。
- [インターフェイス（interface）] には、Duo LDAP サーバーに接続するために使用するインターフェイスの ID、タイプ、バージョン、および名前の値を入力するか、インターフェイス属性を定義するために使用する 6 つの行を削除します（末尾の閉じ括弧を含む）。
- [タイプ（type）] では、値は duoldapidentitysource のままにします。

たとえば、オブジェクトの本文は次のようになります。apiHostname と integrationKey は不明瞭にしてありますが、秘密キーは意図的に仮のものを示しています。

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) [試してみる（Try It Out!）] ボタンをクリックします。

システムは、**curl** コマンドを発行してオブジェクトをデバイス設定にポストします。curl コマンド、応答本文、および応答コードが表示されます。有効な本文を作成した場合は、[応答コード（Response Code）] フィールドに **200** と表示されます。

エラーが発生した場合は、応答本文でエラーメッセージを確認します。本文の値を修正して再試行できます。

h) トップメニューで [デバイス（Device）] をクリックして、Device Manager に戻ります。

i) [オブジェクト（Objects）] を選択し、目次から [アイデンティティソース（Identity Sources）] を選択します。

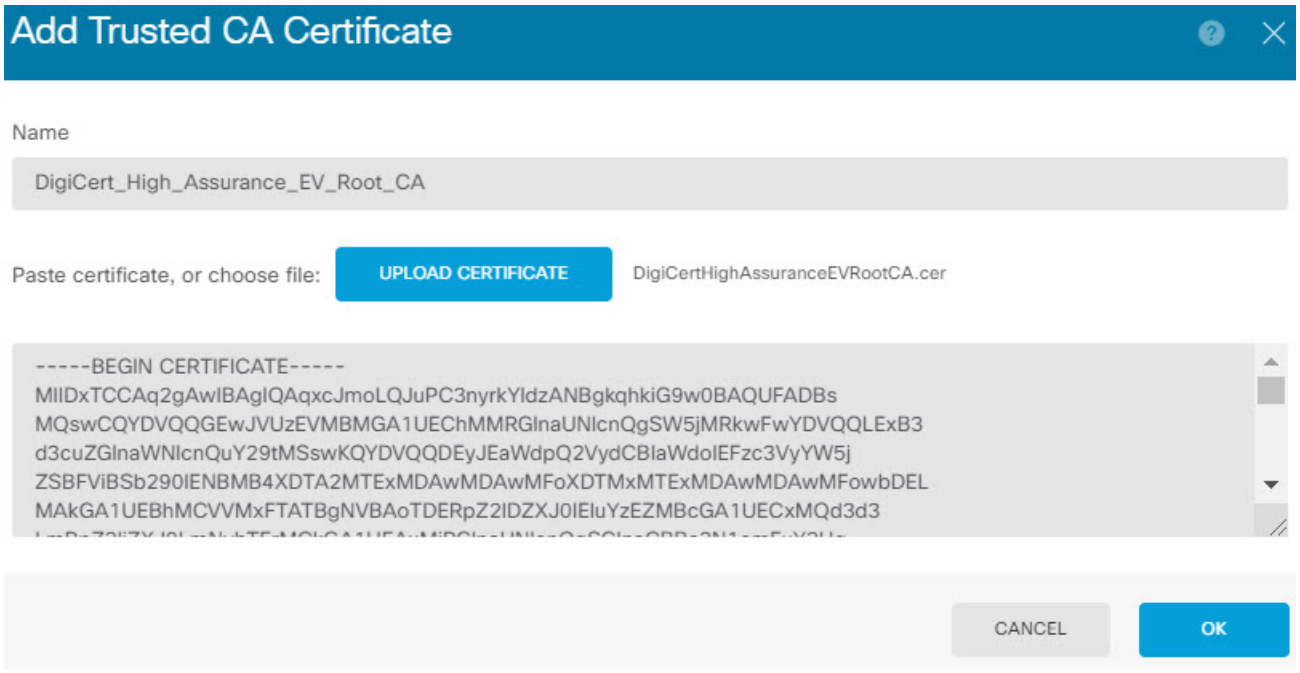
Duo LDAP オブジェクトがリストに表示されます。表示されない場合は、API Explorer に戻り、オブジェクトの作成を再試行します。GET メソッドを使用して、実際に作成されたかどうかを確認できます。

Device Manager を使用してオブジェクトを削除できますが、編集したりその内容を表示したりすることはできません。これらの操作には API を使用する必要があります。関連するメソッドは [DuoLDAPIdentitySource] グループに表示されます。

ステップ 3 Duo Web サイトの信頼できる CA 証明書を Device Manager にアップロードします。

Threat Defense システムには、Duo LDAP サーバーへの接続を検証するために必要な証明書がなければなりません。Google Chrome ブラウザで実行する次の手順を使用して、証明書を取得してアップロードできます。ご使用のブラウザの手順は異なる場合があります。または、https://www.digicert.com/digicert-root-certificates.htm に直接移動して証明書をダウンロードすることもできますが、次の手順は一般的なものであり、任意のサイトの信頼できるルート CA 証明書を取得するために使用できます。

a) ブラウザで https://duo.com を開きます。
b) ブラウザの URL フィールドでサイト情報リンクをクリックし、[証明書（Certificate）] リンクをクリックします。この操作により、証明書情報ダイアログボックスが開きます。
c) [証明のパス（Certificate path）] タブをクリックし、パスのルート（最上位）を選択します。この場合は DigiCert です。
d) DigiCert を選択した状態で、[証明書の表示（View Certificate）] をクリックします。この操作により、新しい [証明書] ダイアログボックスが開き、[全般（General）] タブに、DigiCert High Assurance EV Root CA に発行されたことが示されます。これは、Device Manager にアップロードする必要があるルート CA 証明書です。
e) [詳細（Details）] タブをクリックし、[ファイルにコピー（Copy to File）] ボタンをクリックして、証明書のダウンロードウィザードを起動します。
f) ウィザードを使用して、ワークステーションに証明書をダウンロードします。デフォルトの DER 形式を使用してダウンロードします。
g) Device Manager で、**[オブジェクト（Objects）] > [証明書（Certificates）]** を選択します。
h) **[+] > [信頼済みCAの証明書の追加（Add Trusted CA Certificate）]** をクリックします。
i) 証明書の名前を入力します（例：DigiCert_High_Assurance_EV_Root_CA）(スペースは使用できません)。
j) [証明書のアップロード（Upload Certificate）] をクリックし、ダウンロードしたファイルを選択します。



k) [OK] をクリック

ステップ 4 セキュアクライアント プロファイルエディタを使用して、認証タイムアウトに 60 秒以上を指定するプロファイルを作成します。

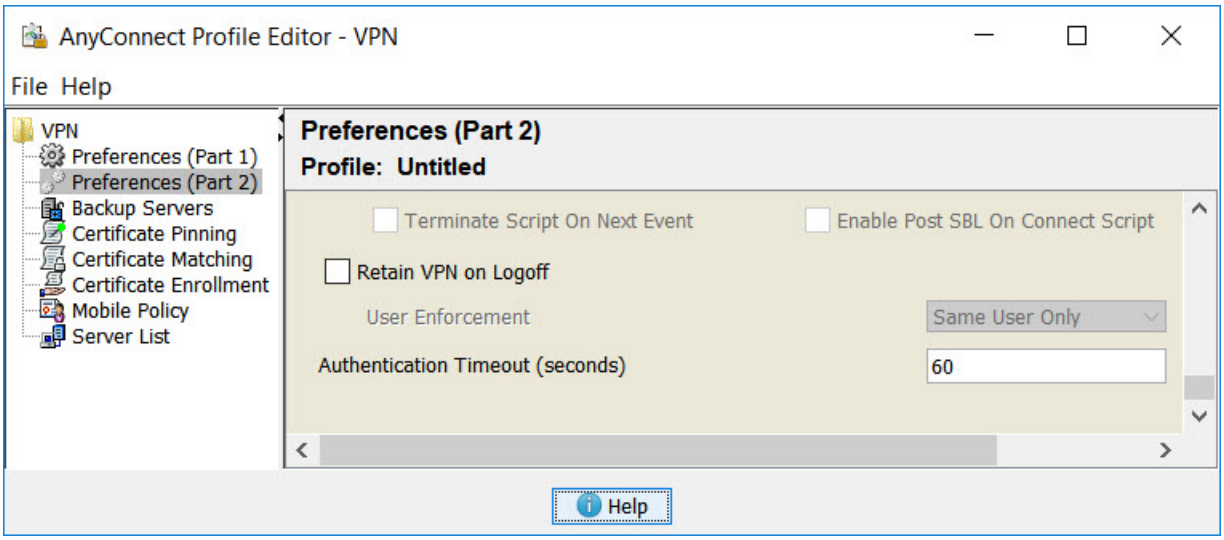
ユーザーが Duo のパスコードを取得し、セカンダリ認証を完了できるように、指定する時間に余裕を持たせる必要があります。60 秒以上を推奨します。

セキュアクライアント プロファイルの作成とアップロードの詳細については、クライアント プロファイルの設定およびアップロード（840 ページ）を参照してください。次の手順では、認証タイムアウトのみを設定してから、Threat Defense にプロファイルをアップロードする方法について説明します。他の設定を変更する場合は、ここで行ってください。

a) セキュアクライアント プロファイル エディタ パッケージをダウンロードしてインストールします（まだ行っていない場合）。このパッケージは、Cisco Software Center（software.cisco.com）の使用しているセキュアクライアント バージョンのフォルダにあります。

b) セキュアクライアント の **VPN プロファイルエディタ**を開きます。

c) 目次の [設定（パート2）（Preferences (Part 2)）] を選択し、ページの最後までスクロールして、[認証タイムアウト（Authentication Timeout）] を 60 以上に変更します。次の図は AnyConnect 4.7 VPN プロファイルエディタからの引用です。それより前のバージョンや後のバージョンでは、内容が異なる場合があります。



d) **[ファイル（File）]** > **[保存（Save）]** を選択し、プロファイル XML ファイルに適切な名前（duo-ldap-profile.xml など）を付けてワークステーションに保存します。

これで、VPN プロファイル エディタ アプリケーションを閉じることができます。

e) Device Manager で、**[オブジェクト（Objects）]** > **[Secure Clientプロファイル（Secure Client Profiles）]** を選択します。

f) [+] をクリックして新しいプロファイルオブジェクトを作成します。

g) [名前（Name）] にオブジェクトの名前を入力します。たとえば、Duo-LDAP-profile と入力します。

h) [アップロード（Upload）] をクリックし、作成した XML ファイルを選択します。

i) [OK] をクリック

ステップ 5 グループポリシーを作成し、ポリシーで セキュアクライアント プロファイルを選択します。

ユーザーに割り当てるグループポリシーは、接続のさまざまな側面を制御します。次の手順では、プロファイル XML ファイルをグループに割り当てる方法について説明します。グループポリシーで実行できる操作の詳細については、RA VPN のグループ ポリシーの設定 （857 ページ）を参照してください。

a) **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** で [設定の表示（View Configuration）] をクリックします。

b) 目次の [グループポリシー（Group Policies）] を選択します。

c) DfltGrpPolicy を編集するか、[+] をクリックして新しいグループポリシーを作成します。たとえば、すべてのユーザーに対して 1 つのリモートアクセス VPN 接続プロファイルが必要な場合は、デフォルトのグループポリシーを編集することが適切です。

d) [全般（General）] ページで、次のプロパティを設定します。

- [名前（Name）]：新しいプロファイルの場合は、名前を入力します。たとえば、Duo-LDAP-group と入力します。
- **[Secure Clientプロファイル（Secure Client Profiles）]**：[+] をクリックし、作成したセキュアクライアント プロファイルを選択します。

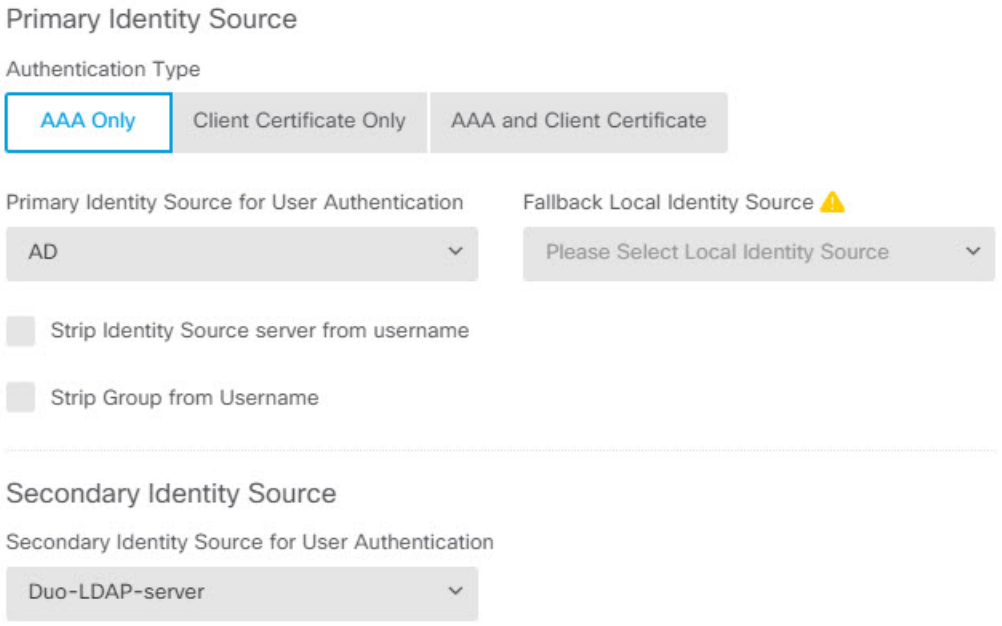
e) [OK] をクリックしてグループプロファイルを保存します。

ステップ 6 Duo LDAP セカンダリ認証に使用するリモートアクセス VPN 接続プロファイルを作成または編集します。

接続プロファイルを設定するには数多くの手順があります。詳細については、RA VPN 接続プロファイルの設定 （847 ページ）を参照してください。次の手順では、Duo-LDAP をセカンダリ認証ソースとして有効にし、セキュアクライアントクライアントプロファイルを適用するための主な変更について説明します。新しい接続プロファイルの場合は、残りの必須フィールドも設定する必要があります。この手順では、既存の接続プロファイルを編集しており、これら 2 つの設定だけ変更する必要があると仮定しています。

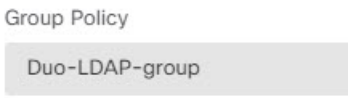
a) [RA VPN] ページで、目次の [接続プロファイル（Connection Profiles）] を選択します。
b) 既存の接続プロファイルを編集するか、新規に作成します。
c) [プライマリアイデンティティソース（Primary Identity Source）] で、次を設定します。

- [認証タイプ（Authentication Type）]：[AAAのみ（AAA Only）] または [AAAとクライアント証明書（AAA and Client Certificate）] のいずれかを選択します。AAA を使用していない場合、二要素認証を設定できません。
- [ユーザー認証のプライマリアイデンティティソース（Primary Identity Source for User Authentication）]：プライマリ Active Directory または RADIUS サーバーを選択します。プライマリソースとして Duo-LDAP アイデンティティソースを選択できることに注意してください。ただし、Duo-LDAP は認証サービスのみを提供し、アイデンティティサービスは提供しないため、プライマリ認証ソースとして Duo-LDAP を使用する場合、どのダッシュボードにも RA VPN 接続に関連付けられているユーザー名は表示されず、これらのユーザーに対してアクセス制御ルールを作成することはできません（必要に応じて、ローカル アイデンティティ ソースへのフォールバックを設定できます）。
- [セカンダリ アイデンティティ ソース（Secondary Identity Source）]：Duo-LDAP のアイデンティティソースを選択します。



d) [Next] をクリックします。

e) [リモートユーザーエクスペリエンス（Remote User Experience）] ページで、作成または編集した [グループポリシー（Group Policy）] を選択します。



f) このページの [次へ（Next）] をクリックし、次のページの [グローバル設定（Global Settings）] をクリックします。

g) [完了（Finish）] をクリックして、接続プロファイルへの変更を保存します。

ステップ 7 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

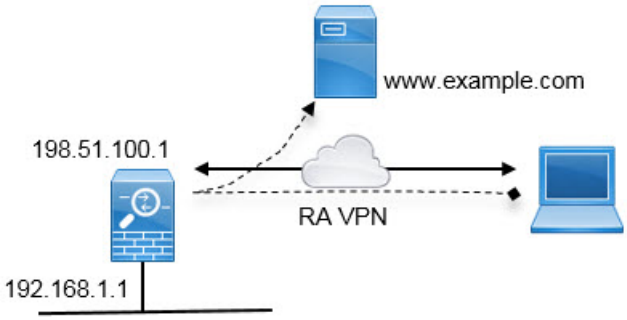
b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

外部インターフェイスでリモート アクセス VPN ユーザーにインターネット アクセスを提供する方法（ヘア ピニング）

リモート アクセス VPN では、リモート ネットワーク上のユーザに自分のデバイスを介してインターネットにアクセスさせたい場合があります。ただし、インターネットに接続している同一インターフェイス（外部インターフェイス）上のデバイスにリモートユーザーがアクセスしているため、インターネット トラフィックが外部インターフェイスの外側からそのまま返される必要があります。この手法はヘア ピニングと呼ばれる場合もあります。

次の図は例を示しています。外部インターフェイス、198.51.100.1 に設定されているリモート アクセス VPN があります。リモートユーザの VPN トンネルを分割し、インターネットに向かうトラフィックを外部インターフェイスから戻し、内部ネットワークに向かうトラフィックはデバイスを通過し続けるようにできます。そのため、リモート ユーザがインターネット上のサーバ（www.example.com など）にアクセスする場合、接続は最初に VPN を通過し、その後 198.51.100.1 インターフェイスからインターネットにルートバックされます。



次の手順では、このサービスの設定方法について説明します。

始める前に

この例は、デバイスが登録済み、リモートアクセス VPN ライセンスが適用済み、セキュアクライアントイメージがアップロード済みであることを前提としています。アイデンティティポリシーでも使用されるアイデンティティ レルムも設定済みであると想定しています。

手順

ステップ 1 リモートアクセス VPN 接続を設定します。

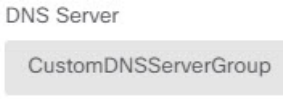
設定には、接続プロファイルだけでなく、カスタマイズされたグループポリシーが必要です。ヘアピニングは一般的な設定であり、グループポリシーで必要な設定がほぼ該当するため、この例では新しいグループポリシーを作成するのではなく、デフォルトグループポリシーを編集します。どちらのアプローチも取ることができます。

a) **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。

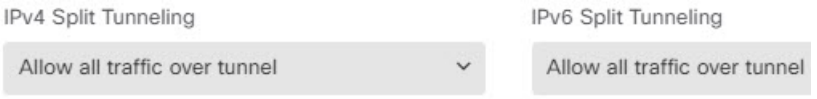
b) 目次で [グループポリシー（Group Policies）] をクリックし、DfltGrpPolicy オブジェクトの編集アイコン（）をクリックします。

c) デフォルトグループポリシーに次の変更を加えます。

- [全般（General）] ページの [DNSサーバー（DNS Server）] で、VPN エンドポイントがドメイン名を解決するために使用する必要があるサーバーを定義する DNS サーバーグループを選択します。



- [スプリットトンネリング（Split Tunneling）] ページで、**IPv4** と IPv6 の両方の**スプリットトンネリング**で [すべてのトラフィックをトンネル経由で許可（Allow all traffic on tunnel）] オプションを選択します。これはデフォルト設定であるため、すでに正しく設定されている可能性があります。



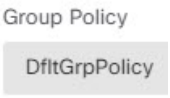
（注） **これは、ヘアピン接続を有効にするための重要な設定です。**すべてのトラフィックを VPN ゲートウェイに向かわせる場合、スプリット トンネリングは、リモート クライアントが VPN の外部にあるローカル サイトやインターネット サイトに直接アクセスできるようにするための方法です。

d) [OK] をクリックして、デフォルトグループポリシーの変更を保存します。

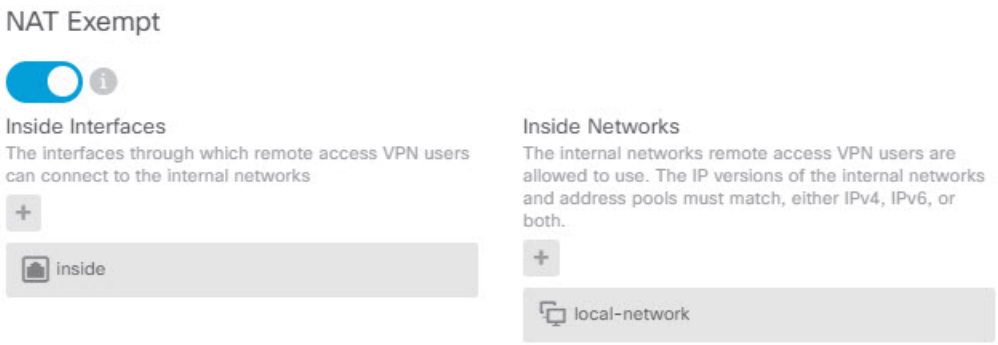
e) [接続プロファイル（Connection Profiles）] をクリックし、既存のプロファイルを編集するか、または新しいプロファイルを作成します。

f) 接続プロファイルで、ウィザードのページを表示し、他の RA VPN 設定の場合と同じようにすべてのオプションを設定します。ただし、ヘアピン接続を有効にするには、次のオプションを正しく設定する必要があります。

- 手順 2 の [グループポリシー（Group Policy）]。ヘアピニング用にカスタマイズしたグループポリシーを選択します。



- 手順 3 の [NAT免除（NAT Exempt）]。この機能を有効にします。内部インターフェイスを選択し、内部ネットワークを定義するネットワーク オブジェクトを選択します。この例では、オブジェクトは 192.168.1.0/24 を指定します。内部ネットワークに向かう RA VPN トラフィックは、アドレス変換されません。ただし、ヘア ピニングされたトラフィックは外部インターフェイスの外に出るため、引き続き NAT が行われます。これは、NAT 免除は内部インターフェイスにのみ適用されるためです。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。



（注） [NAT 免除（NAT Exempt）] オプションは、ヘアピン設定のもう一つの重要な設定です。

g) （オプション）[グローバル設定（Global Settings）] で、[復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択します。

このオプションを選択すると、RA VPN プールアドレスからのトラフィックを許可するアクセス制御ルールを設定する必要がなくなります。このオプションはセキュリティを向上させますが（外部ユーザーがプール内のアドレスをスプーフィングできません）、RA VPN トラフィックが、URL フィルタリングや侵入防御を含むインスペクションから除外されることを意味します。このオプションを決定する前に、長所と短所を考慮してください。

h) RA VPN の設定を確認してから [完了（Finish）] をクリックします。

ステップ 2 外部インターフェイスから送信されたすべての接続を外部 IP アドレス（インターフェイス PAT）のポートに変換するよう NAT ルールを設定します。

デバイスの初期設定を完了すると、InsideOutsideNatRule という名前の NAT ルールが作成されます。このルールは、外部インターフェイス経由でデバイスを抜ける任意のインターフェイスから、インターフェイス PAT を IPv4 トラフィックに充当します。外部インターフェイスは「任意の」送信元インターフェイスに含まれるため、必要なルールは、編集または削除していない限り、すでに存在しています。

次の手順で、必要なルールを作成する方法を説明します。

a) **[ポリシー（Policies）] > [NAT]** をクリックします。

b) 次のいずれかを実行します。

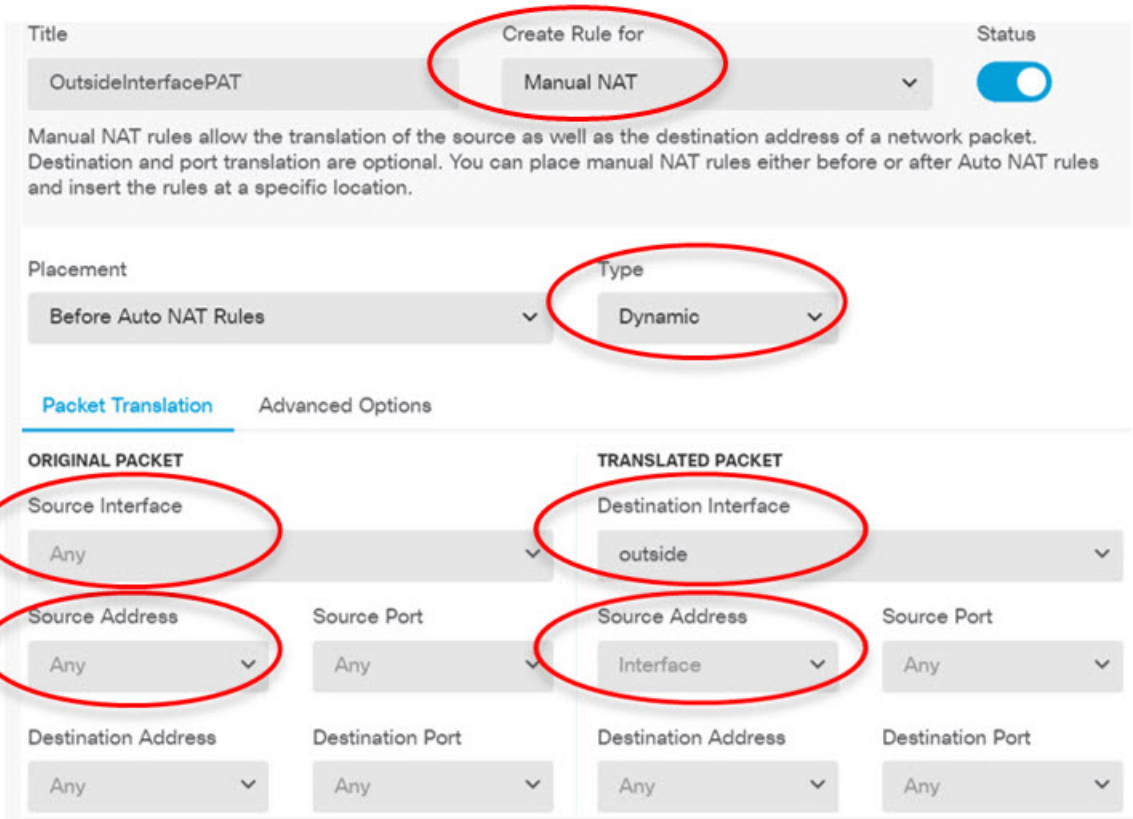
- InsideOutsideNatRule を編集するには、[アクション（Action）] 列にマウス オーバーし、[編集（edit）] アイコン（）をクリックします。
- ルールを新規作成するには、[+] ボタンをクリックします。

c) 次のプロパティを使用してルールを設定します。

- [タイトル（Title）]：新しいルールのわかりやすい名前をスペースを含めず入力します。たとえば、OutsideInterfacePAT と入力します。

- [ルールの作成先（Create Rule For）]：[手動NAT（Manual NAT）]。
- [配置（Placement）]：[自動NATルールの前（Before Auto NAT Rules）]（デフォルト）。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [元のパケット（Original Packet）]：[送信元アドレス（Source Address）]で[任意（Any）]または[any-ipv4]を選択します。[送信元インターフェイス（Source Interface）]で、[任意（Any）]（デフォルト）を選択していることを確認します。[元のパケット（Original Packet）]の他のすべてのオプションは、デフォルトの[任意（Any）]のままにします。
- [変換後のパケット（Translated Packet）]：[宛先インターフェイス（Destination Interface）]で、[外部（outside）]を選択します。[変換後のアドレス（Translated Address）]で、[インターフェイス（Interface）]を選択します。[変換後のパケット（Translated Packet）]の他のすべてのオプションは、デフォルトの[任意（Any）]のままにします。

次の図は、発信元アドレスに[任意（Any）]を選択したシンプルな例を示しています。



d) [OK]をクリックします。

ステップ 3 （接続プロファイルで[復号されたトラフィックでアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]

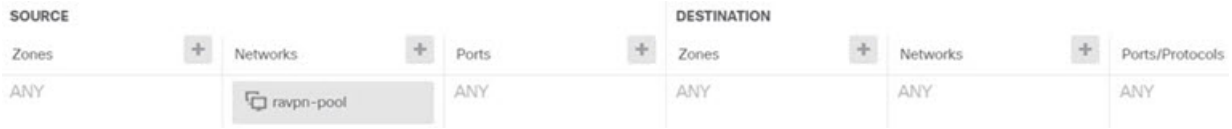
を設定していない場合）リモート アクセス VPN アドレス プールからのアクセスを許可するアクセス制御ルールを設定します。

接続プロファイルで [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] を選択した場合、RA VPN プールアドレスからのトラフィックは、アクセス制御ポリシーをバイパスします。このトラフィックに適用されるアクセス制御ルールを作成することはできません。オプションを無効にした場合にのみ、ルールを作成する必要があります。

次の例では、アドレスプールから任意の宛先へのトラフィックが許可されます。これは独自の要件に合わせて調整できます。不要なトラフィックを除外するブロック ルールをルールの前に置くことができます。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** をクリックします。
b) [+] をクリックして新しいルールを作成します。
c) 次のプロパティを使用してルールを設定します。

- [順序（Order）]：ポリシー内でこれらの接続に一致し、ブロックする可能性のある他のルールの前の位置を選択します。デフォルトでは、ルールはポリシーの最後に追加されます。ルールの位置を後で変更する必要がでてきた場合は、このオプションを編集するか、単にルールをテーブルの右のスロットにドラッグアンドドロップします。
- [タイトル（Title）]：スペースを含めずにわかりやすい名前を入力します。例、RAVPN-address-pool。
- [アクション（Action）]：[許可（Allow）]。このトラフィックのプロトコル違反または侵入を調べない場合は、[信頼（Trust）] を選択できます。
- [送信元または宛先（Source/Destination）] ブ：**[送信元（Source）]** > **[ネットワーク（Network）]** で、アドレス プールの RA VPN 接続プロファイルに使用しているのと同じオブジェクトを選択します。[送信元と宛先（Source and Destination）] の他のすべてのオプションについては、デフォルトの [任意（Any）] のままにします。



- [アプリケーション（Application）]、[URL]、および [ユーザー（Users）] タブ：これらのタブではデフォルトの設定（何も選択しない）のままにします。
- [侵入（Intrusion）]、[ファイル（File）] タブ：オプションで、脅威またはマルウェアを検索する侵入またはファイル ポリシーを選択できます。
- [ロギング（Logging）] タブ：オプションで接続のロギングを有効にできます。

d) [OK] をクリックします。

ステップ 4 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

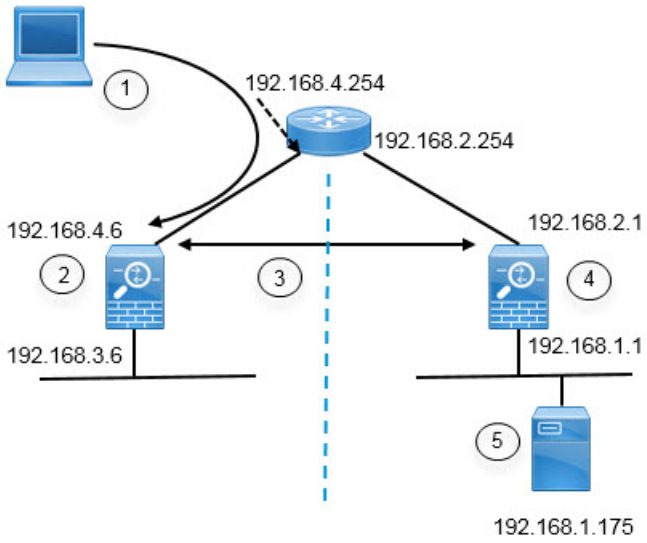
リモート アクセス VPN を使用して外部ネットワークのディレクトリ サーバーを使用する方法

モバイル ワーカーと在宅勤務者が内部ネットワークに安全に接続できるリモートアクセスVPNを設定できます。接続のセキュリティは、ユーザー接続を認証して、認可されたユーザーだけがエントリを取得できるようにするディレクトリ サーバーによって異なります。

ディレクトリ サーバーが内部ネットワークではなく外部ネットワーク上にある場合、外部インターフェイスからディレクトリ サーバーを含むネットワークへのサイト間 VPN 接続を設定する必要があります。**サイト間 VPN の設定の 1つのテクニック**：サイト間 VPN 接続の「内部」ネットワーク内、および背後にディレクトリ サーバーが存在するデバイスのリモート ネットワークに、リモートアクセス VPNデバイスの外部インターフェイス アドレスを含める必要があります。詳細については、次の手順を参照してください。

（注） データインターフェイスを仮想管理インターフェイスのゲートウェイとして使用する場合、この設定により、アイデンティティ ポリシー用のディレクトリの使用も可能になります。データインターフェイスを管理ゲートウェイとして使用しない場合は、管理ネットワークから、サイト間 VPN 接続に参加する内部ネットワークへのルートがあることを確認します。

この使用例では、次のネットワーク シナリオを実装します。



図のコールアウト	説明
1	192.168.4.6 に VPN 接続を行うリモート アクセス ホスト。クライアントは 172.18.1.0/24 アドレス プールにあるアドレスを取得します。
2	リモート アクセス VPN をホストするサイト A。
3	サイト A とサイト B の 脅威に対する防御 デバイスの外部インターフェイス間のサイト間 VPN トンネル。
4	ディレクトリ サーバーをホストするサイト B。
5	サイト B の内部ネットワークにあるディレクトリ サーバー。

始める前に

この使用例は、デバイスのセットアップ ウィザードを使用して、通常のベースラインの構成を構築していることを前提としています。具体的には次のとおりです。

- inside_zone から outside_zone に移動するトラフィックを許可（または信頼）する Inside_Outside_Rule アクセス コントロール ルールがある。
- inside_zone と outside_zone のセキュリティ ゾーン（それぞれ）に、内部インターフェイスと外部インターフェイスが含まれている。
- 内部インターフェイスから外部インターフェイスに移動するすべてのトラフィックに対してインターフェイス PAT を実行する InsideOutsideNATRule がある。デフォルトで内部ブリッジ グループを使用するデバイスに、インターフェイス PAT 用のルールが複数存在する場合がある。
- 外部インターフェイスを指す、0.0.0.0/0 のスタティック IPv4 ルートがある。この例は、外部インターフェイスにスタティック IP アドレスを使用しているが、DHCP を使用してス

タティック ルートの動的取得も可能であることを前提としています。この例の場合、次のスタティック ルートを想定しています。

- サイト A：外部インターフェイス、ゲートウェイは 192.168.4.254 です。
- サイト B：外部インターフェイス、ゲートウェイは 192.168.2.254 です。

手順

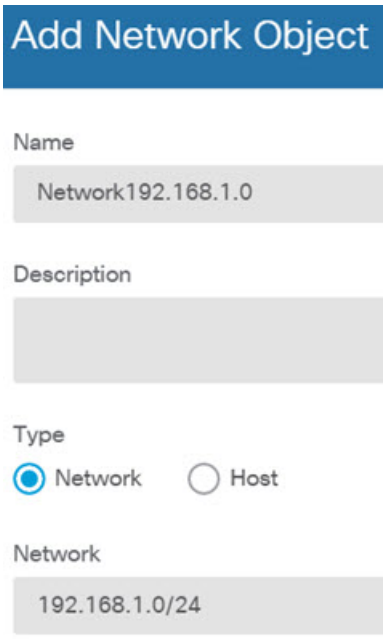
ステップ 1 ディレクトリ サーバーをホストする [サイトB（Site B）] にサイト間 VPN 接続を設定します。

a) [デバイス（Device）] をクリックし、[サイト間VPN（Site-to-Site VPN）] グループで [設定の表示（View Configuration）] をクリックします。

b) [+] ボタンをクリックします。

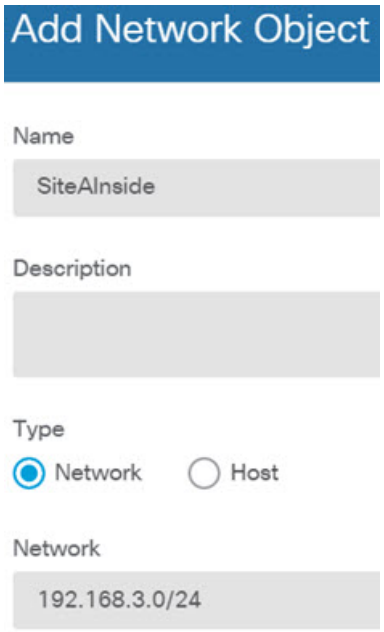
c) [エンドポイントの設定（Endpoint Settings）] に次のオプションを設定します。

- [接続プロファイル名（Connection Profile Name）]：名前を入力します（たとえば、サイト A への接続を示す、SiteA）。
- [ローカルサイト（Local Site）]：これらのオプションでローカル エンドポイントを定義します。
  - [ローカルVPNアクセスインターフェイス（Local VPN Access Interface）]：[外部（outside）]インターフェイス（図の 192.168.2.1 アドレスが付いているインターフェイス）を選択します。
  - [ローカルネットワーク（Local Network）]：[+] をクリックして、VPN 接続に参加する必要があるローカル ネットワークを特定するネットワーク オブジェクトを選択します。ディレクトリ サーバーはこのネットワーク上にあるため、サイト間 VPN に参加できます。オブジェクトがまだ存在していない場合、[新規ネットワークの作成（Create New Network）] をクリックして、192.168.1.0/24 ネットワークのオブジェクトを設定します。オブジェクトを保存したら、ドロップダウン リストでそのオブジェクトを選択し、[OK] をクリックします。

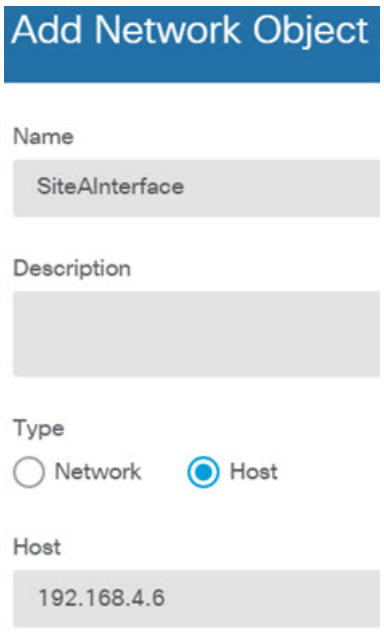


- [リモートサイト（Remote Site）]：これらのオプションでリモート エンドポイントを定義します。
  - [リモートIPアドレス（Remote IP Address）]：VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスである 192.168.4.6 を入力します。
  - [リモートネットワーク（Remote Network）]：[+] をクリックして、VPN 接続に参加する必要があるリモート ネットワークを特定するネットワーク オブジェクトを選択します。[新規ネットワークの作成（Create New Network）] をクリックして、次のオブジェクトを設定し、リストでそれらのオブジェクトを選択します。

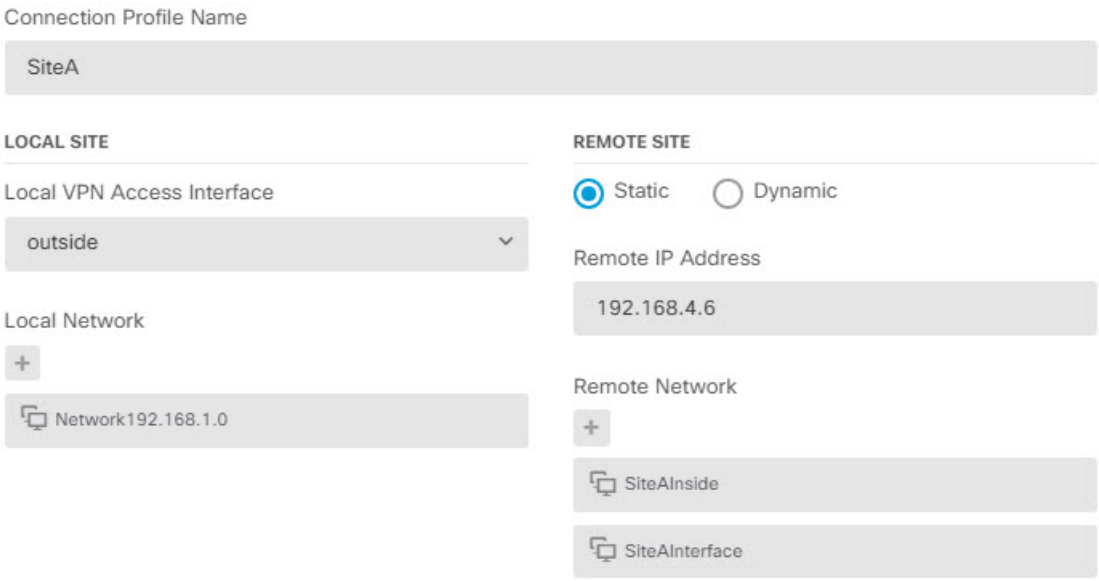
    1. SiteAInside、ネットワーク、192.168.3.0/24。



2. SiteAInterface、ホスト、192.168.4.6。重要ポイント：リモート アクセス VPN 接続ポイントのアドレスをサイト間 VPN 接続用のリモート ネットワークの一部として含めて、当該インターフェイスでホストされている RA VPN でディレクトリ サーバーを使用可能にする必要があります。



終了すると、エンドポイントの設定は次のようになります。



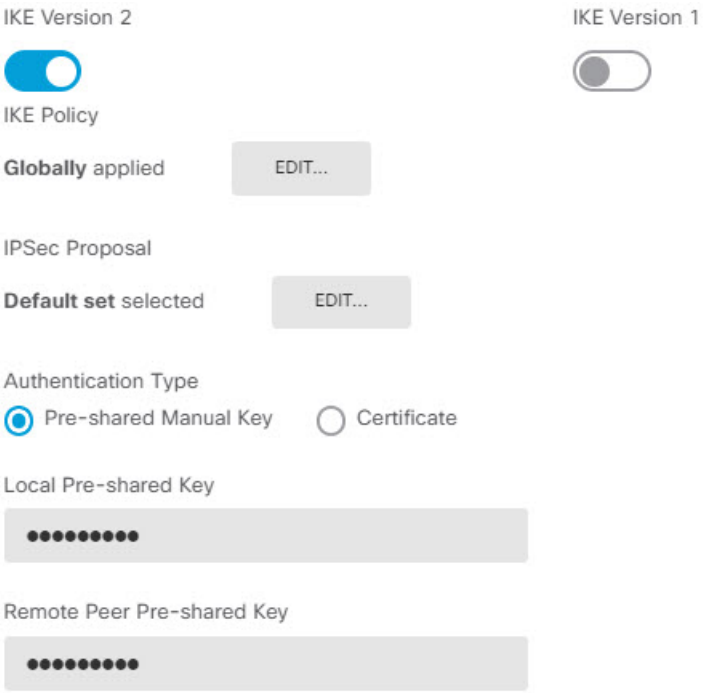
d) [Next] をクリックします。

e) VPN のプライバシー設定を定義します。

この使用例は、強力な暗号化の使用を許可する輸出管理機能を承認していることを前提としています。これらの例の設定は、お客様のニーズとライセンス コンプライアンスに合わせて調整してください。

- [IKEバージョン2（IKE Version 2）]、[IKEバージョン1（IKE Version 1）]：デフォルト（[IKEバージョン2（IKE Version 2）] は有効で、[IKEバージョン1（IKE Version 1）] は無効）のままにします。
- [IKEポリシー（IKE Policy）]：[編集（Edit）] をクリックして、[AES-GCM-NULL-SHA] および [AES-SHA-SHA] を有効にし、[DES-SHA-SHA] を無効にします。
- [IPsecプロポーザル（IPsec Proposal）]：[編集（Edit）] をクリックします。[IPSecプロポーザルの選択（Select IPSec Proposals）] ダイアログボックスで [+] をクリックし、[デフォルトに設定（Set Default）] をクリックしてデフォルトの AES-GCM プロポーザルを選択します。
- [ローカルの事前共有キー（Local Preshared Key）]、[リモートピアの事前共有キー（Remote Peer Preshared Key）]：このデバイスおよび VPN 接続用のリモート デバイスに定義されているキーを入力します。これらのキーは IKEv2 では異なることがあります。このキーには 1 ～ 127 の英数字を指定できます。**サイト A のデバイスでサイト間 VPN 接続を作成するときに同じ文字列を設定する必要があるため、これらのキーは覚えておいてください。**

IKE ポリシーは次のようになります。



f) [追加オプション（Additional Options）] を設定します。

- [NAT免除（NAT Exempt）]：内部ネットワークをホストするインターフェイスを選択します。この例では [内部（inside）]インターフェイス。通常、サイト間 VPN トンネル内のトラフィックの IP アドレスは変換しません。このオプションは、ローカルネットワークが 1 つのルーテッドインターフェイス（ブリッジグループ メンバーではない）の背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッドインターフェイスまたは 1 つ以上のブリッジ グループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、NAT からのサイト間 VPN トラフィックの除外 （809 ページ）を参照してください。
- [Perfect Forward Secrecy用のDiffie-Helmanグループ（Diffie-Helman Group for Perfect Forward Secrecy）]：[グループ19（Group 19）] を選択します。このオプションは、暗号化された交換ごとに固有のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを決定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイント デバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （783 ページ）を参照してください。

このオプションは次のようになります。

g) [次へ（Next）] をクリックします。

h) サマリーを確認し、[終了（Finish）] をクリックします。

サマリー情報がクリップボードにコピーされます。この情報はドキュメントに貼り付けて、リモート ピアの設定、またはピアの設定責任者に送信するために使用できます。

i) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

j) [今すぐ展開（Deploy Now）] ボタンをクリックして、導入が正常に完了するまで待ちます。

これで、サイト B のデバイスがサイト間 VPN 接続の一端をホストできるようになりました。

ステップ 2 [サイトB（Site B）] デバイスからログアウトして、[サイトA（Site A）] デバイスにログインします。

ステップ 3 リモートアクセス VPN をホストする [サイトA（Site A）] にサイト間 VPN 接続を設定します。

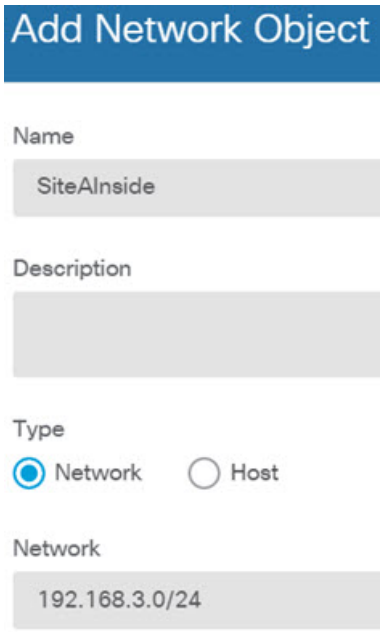
a) [デバイス（Device）] をクリックし、[サイト間VPN（Site-to-Site VPN）] グループで [設定の表示（View Configuration）] をクリックします。

b) [+] ボタンをクリックします。

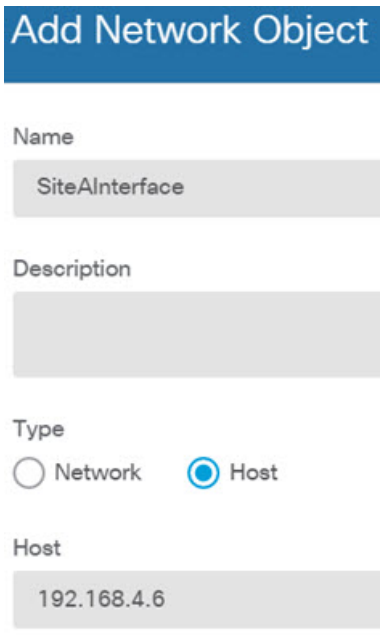
c) [エンドポイントの設定（Endpoint Settings）] に次のオプションを設定します。

- [接続プロファイル名（Connection Profile Name）]：名前を入力します（たとえば、サイト B への接続を示す、SiteB）。
- [ローカルサイト（Local Site）]：これらのオプションでローカル エンドポイントを定義します。
  - [ローカルVPNアクセスインターフェイス（Local VPN Access Interface）]：[外部（outside）] インターフェイス（図内 192.168.4.6 アドレスが付いているインターフェイス）を選択します。
  - [ローカルネットワーク（Local Network）]：[+] をクリックして、VPN 接続に参加する必要があるローカル ネットワークを特定するネットワーク オブジェクトを選択します。[新規ネットワークの作成（Create New Network）] をクリックして、次のオブジェクトを設定し、リストでそれらのオブジェクトを選択します。**サイト B のデバイスに同じオブジェクトを作成しましたが、サイト A のデバイスでも再度同じオブジェクトを作成する必要があります。**

    1. SiteAInside、ネットワーク、192.168.3.0/24。



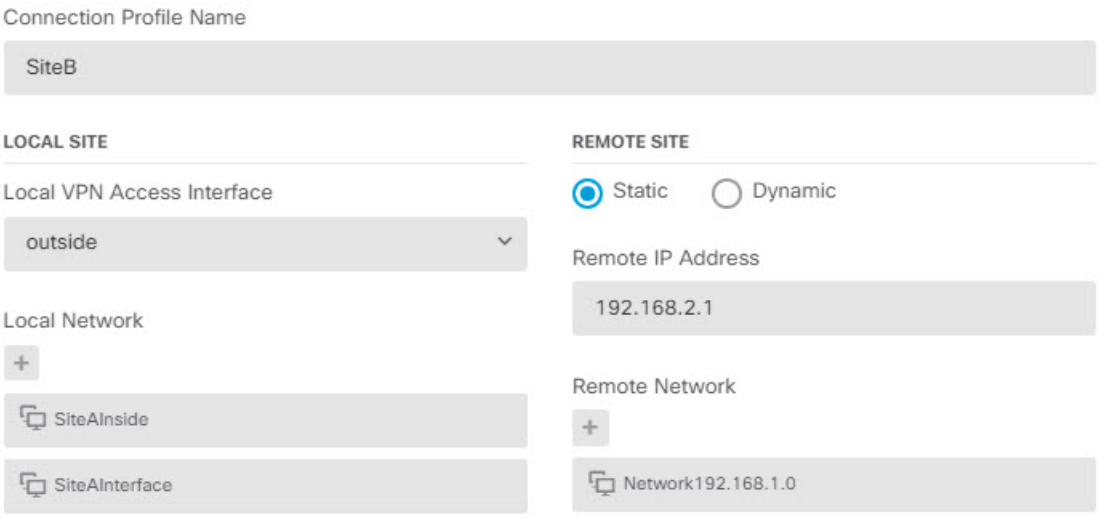
2. SiteAInterface、ホスト、192.168.4.6。**重要ポイント：リモート アクセス VPN 接続ポイントのアドレスをサイト間 VPN 接続用の内部ネットワークの一部として含めて、当該インターフェイスでホストされている RA VPN でリモート ネットワーク上のディレクトリ サーバーを使用可能にする必要があります。**



- [リモートサイト（Remote Site）]：これらのオプションでリモート エンドポイントを定義します。

- [リモートIPアドレス（Remote IP Address）]：VPN 接続をホストするリモート VPN ピアのインターフェイスの IP アドレスである 192.168.2.1 を入力します。
- [リモートネットワーク（Remote Network）]：[+] をクリックして、VPN 接続に参加する必要があるリモート ネットワークを特定する（ディレクトリ サーバーを含んでいる）ネットワーク オブジェクトを選択します。[新規ネットワークの作成（Create New Network）] をクリックし、192.168.1.0/24 ネットワークのオブジェクトを設定します。オブジェクトを保存したら、ドロップダウン リストでそのオブジェクトを選択し、[OK] をクリックします。**サイト B のデバイスに同じオブジェクトを作成しましたが、サイト A のデバイスでも再度同じオブジェクトを作成する必要があります。**

終了すると、エンドポイントの設定は次のようになります。ローカルおよびリモート ネットワークは、サイト B の設定と比べると反転している点に注意してください。これは、ポイントツーポイント接続の両端の通常の外観を示しています。

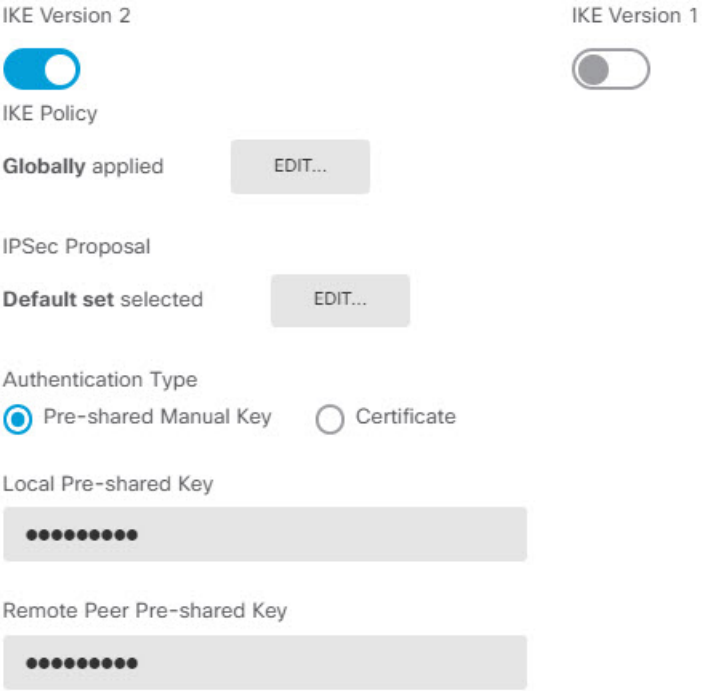


d) [Next] をクリックします。

e) VPN のプライバシー設定を定義します。

サイト B 接続の場合と同じ IKE バージョン、ポリシー、および IPsec プロポーザルと、同じ事前共有キーを設定します。**ただし、必ず、ローカル事前共有キーとリモート事前共有キーを逆にしてください。**

IKE ポリシーは次のようになります。



f) [追加オプション（Additional Options）] を設定します。

- [NAT免除（NAT Exempt）]：内部ネットワークをホストするインターフェイスを選択します。この例では [内部（inside）]インターフェイス。通常、サイト間 VPN トンネル内のトラフィックの IP アドレスは変換しません。このオプションは、ローカル ネットワークが 1 つのルーテッドインターフェイス（ブリッジグループ メンバーではない）の背後にある場合にのみ機能します。ローカル ネットワークが複数のルーテッドインターフェイスまたは 1 つ以上のブリッジ グループのメンバーの背後にある場合、NAT 免除ルールを手動で作成する必要があります。必要なルールを手動で作成する方法の詳細については、NAT からのサイト間 VPN トラフィックの除外 （809 ページ）を参照してください。
- [Perfect Forward Secrecy用のDiffie-Helmanグループ（Diffie-Helman Group for Perfect Forward Secrecy）]：[グループ19（Group 19）] を選択します。

このオプションは次のようになります。

g) [次へ（Next）] をクリックします。
h) サマリーを確認し、[終了（Finish）] をクリックします。
i) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

j) [今すぐ展開（Deploy Now）] ボタンをクリックして、導入が正常に完了するまで待ちます。

これで、サイト A のデバイスがサイト間 VPN 接続のもう一端をホストできるようになりました。サイト B は互換性のある設定ですでに設定されているため、2 台のデバイスは VPN 接続をネゴシエートする必要があります。

デバイスの CLI にログインし、ディレクトリ サーバーに ping することで、接続を確認できます。**show ipsec sa** コマンドを使用して、セッション情報を表示することもできます。

ステップ 4 [サイトA（Site A）] のディレクトリ サーバーを設定します。[テスト（Test）] をクリックして、接続があることを確認します。

a) [オブジェクト（Objects）] を選択し、目次から **[アイデンティティ ソース（Identity Sources）]** を選択します。
b) **[+]** > **[AD]** をクリックします。
c) 基本レルムのプロパティを設定します。

- [名前（Name）]：ディレクトリ レルムの名前。例、AD。

- [タイプ（Type）]：ディレクトリ サーバのタイプ。サポートされるタイプは Active Directory のみで、このフィールドを変更することはできません。
- [ディレクトリユーザ名（Directory Username）]、[ディレクトリパスワード（Directory Password）]：取得するユーザ情報に対して適切な権限を持つユーザの識別用ユーザ名とパスワード。Active Directory では、昇格されたユーザ特権は必要ありません。ドメイン内の任意のユーザを指定できます。ユーザ名は Administrator@example.com などの完全修飾名である必要があります（Administrator だけでなく）。

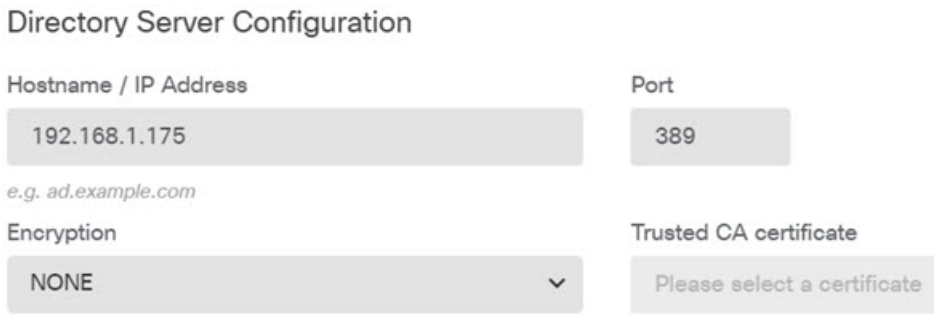
  （注） この情報から ldap-login-dn と ldap-login-password が生成されます。たとえば、Administrator@example.com は cn=adminisntrator,cn=users,dc=example,dc=com に変換されます。cn=users は常にこの変換の一部であるため、ここで指定するユーザは、共通名の「users」フォルダの下で設定する必要があります。

- [ベースDN（Base DN）]：ユーザおよびグループ情報、つまり、ユーザとグループの共通の親を検索またはクエリするためのディレクトリ ツリー。例、cn=users,dc=example,dc=com。ベース DN の検索の詳細については、ディレクトリ ベースの DN の決定 （194 ページ）を参照してください。
- [ADプライマリドメイン（AD Primary Domain）]：デバイスが参加する必要がある完全修飾 Active Directory ドメイン名。例、example.com。

d) ディレクトリ サーバのプロパティを設定します。

- [ホスト名またはIPアドレス（Hostname/IP Address）]：ディレクトリ サーバのホスト名または IP アドレス。サーバに対して暗号化された接続を使用する場合、IP アドレスではなく、完全修飾ドメイン名を入力する必要があります。この例では、「192.168.1.175」と入力します。
- [ポート（Port）]：サーバとの通信に使用するポート番号。デフォルトは 389 です。暗号化方式として LDAPS を選択する場合は、ポート 636 を使用します。この例では、389 のままにします。

- [暗号化（Encryption）]：ユーザーおよびグループ情報のダウンロードに暗号化された接続を使用します。デフォルトは[なし（None）]で、ユーザーおよびグループ情報はクリア テキストでダウンロードされます。RA VPN の場合は、LDAP over SSL である [LDAPS] を使用できます。このオプションを選択する場合は、ポート 636 を使用します。RA VPN は STARTTLS をサポートしていません。この例では、[なし（None）] を選択します。
- [信頼できるCA証明書（Trusted CA Certificate）]：暗号化方式を選択する場合、認証局（CA）の証明書をアップロードして、システムとディレクトリ サーバ間の信頼できる接続を有効にします。認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IPアドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 192.168.1.175 を使用し、証明書では ad.example.com を使用している場合、接続は失敗します。



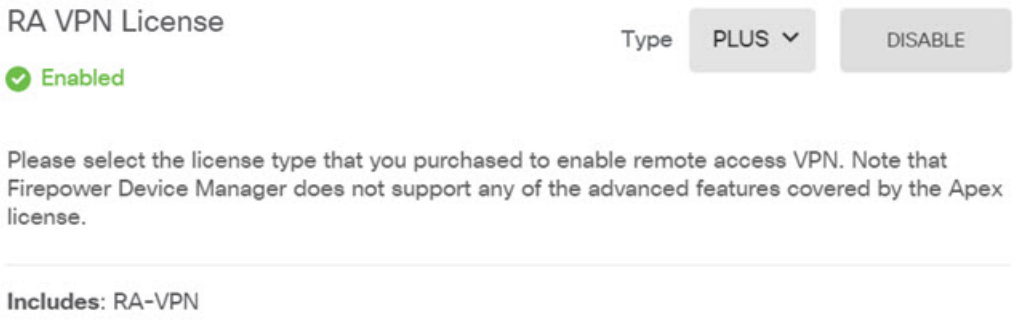
e) [テスト（Test）] ボタンをクリックして、システムがサーバーに接続できることを確認します。

サーバー アクセスには異なるプロセスが使用されるため、アイデンティティ ポリシーには使用できるが、リモート アクセス VPN には使用できないなど、あるタイプの使用においては接続が機能するが別のタイプでは機能しないことを示すエラーが表示されることがあります。サーバーに到達できない場合は、正しい IP アドレスとホスト名を指定していること、DNS サーバーに当該ホスト名のエントリなどが設定されていることを確認します。また、サイト間 VPN 接続が機能していること、サイト A の外部インターフェイス アドレスを VPN に含めていること、および NAT がディレクトリ サーバーのトラフィックを変換していないことを確認します。サーバーのスタティック ルートを設定する必要がある場合もあります。

f) [OK] をクリック

ステップ 5 **[デバイス（Device）]** > **[スマートライセンス（Smart License）]** > **[設定の表示（View Configuration）]** をクリックし、RA VPN ライセンスを有効にします。

RA VPN ライセンスを有効にする場合は、購入したライセンスのタイプ（Plus、Apex（または両方）、VPN Only）を選択します。詳細については、リモート アクセス VPN のライセンス要件 （837 ページ）を参照してください。

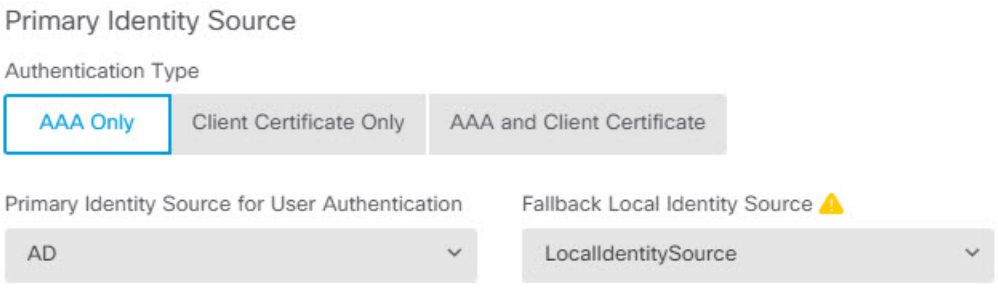


ステップ 6 サイト A のリモート アクセス VPN を設定します。

a) **[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** グループで [設定の表示（View Configuration）] をクリックします。[接続プロファイル（Connection Profiles）] ページを表示していることを確認します。

b) 接続プロファイルを作成または編集します。

c) ウィザードの最初のステップでプロファイル名を設定し、その後にプライマリ認証ソースとして AD レルムを選択します。必要に応じて、フォールバック アイデンティティ ソースとしてローカルデータベースを選択できます。



d) アドレスプールを設定します。

この例では、[+] をクリックしてから IPv4 アドレスプールで [新しいネットワークの作成（Create New Network）] を選択し、172.18.1.0/24 ネットワークのオブジェクトを作成し、そのオブジェクトを選択します。クライアントには、このプールからアドレスが割り当てられます。IPv6 プールは空白のままにします。アドレス プールを外部インターフェイスの IP アドレスと同じサブネット上に設定することはできません。

オブジェクトは次のようになります。

プールの仕様は次のようになります。

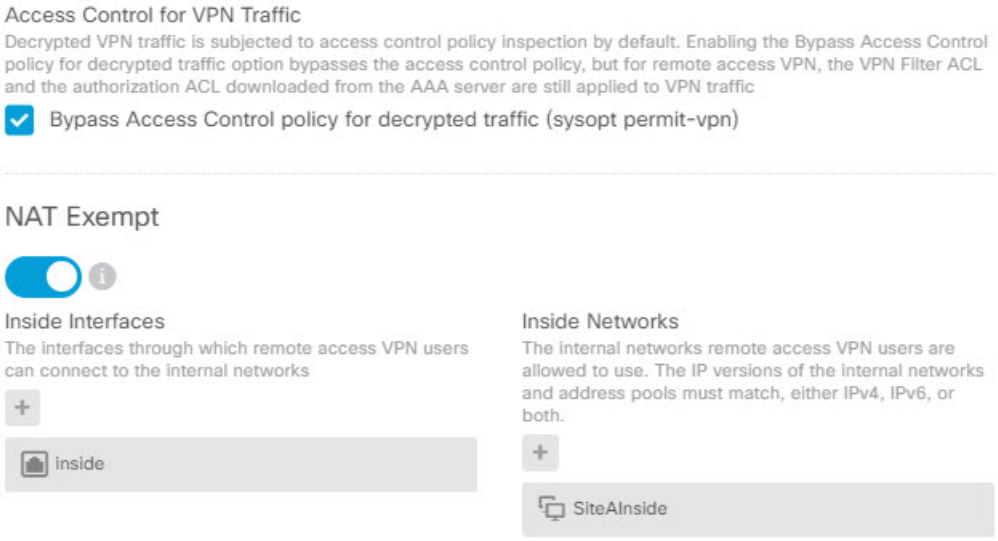
e) [次へ（Next）] をクリックし、適切なグループポリシーを選択します。

選択したポリシーに関する要約情報を確認します。DNS サーバーが設定されていることを確認します。設定されていない場合は、ここでポリシーを編集して、DNS を設定します。

f) [次へ（Next）] をクリックし、[グローバル設定（Global Settings）] で [復号されたトラフィックでアクセスコントロールポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択し、[NAT免除（NAT Exempt）] オプションを設定します。

[NAT免除（NAT Exempt）] では、次のオプションを設定する必要があります。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

- [内部インターフェイス（Inside Interfaces）]：[内部（inside）] インターフェイスを選択します。これらは、内部ネットワークのリモートユーザーがアクセスするインターフェイスです。これらのインターフェイスには NAT ルールが作成されます。
- [内部ネットワーク（Inside Networks）]：SiteAInside ネットワーク オブジェクトを選択します。これらは、内部ネットワークのリモートユーザーがアクセスするオブジェクトを表すネットワーク オブジェクトです。



g) サポートするプラットフォームの セキュアクライアント パッケージをアップロードします。

h) [次へ（Next）] をクリックして、設定を確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順（Instructions）] をクリックして、セキュアクライアント ソフトウェアをインストールし、VPN接続を完了できることをテストするためにエンドユーザーが最初に行う必要がある内容を確認します。[コピー（Copy）]をクリックして、それらの手順をクリップボードにコピーし、テキスト ファイルまたは電子メールに貼り付けます。

i) [終了（Finish）] をクリックします。

ステップ 7 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

ステップ 8 [今すぐ展開（Deploy Now）] ボタンをクリックして、導入が正常に完了するまで待ちます。

これで、サイト A のデバイスが RA VPN の接続を承認できるようになりました。外部ユーザーに セキュアクライアント クライアントをインストールさせて、VPN 接続を完了させます。

接続を確認するには、デバイス CLI にログインし、**show vpn-sessiondb anyconnect** コマンドを使用してセッション情報を表示します。

グループによって RA VPN アクセスを制御する方法

リモートアクセス VPN 接続プロファイルを、グループポリシーに基づいて内部リソースへの差分アクセスを提供するように設定することができます。たとえば、従業員に無制限のアクセスを提供し、請負業者には単一の内部ネットワーク以外へのアクセスを提供したくない場合

は、グループポリシーを使用して、適切にアクセスを制限するための異なる ACL を定義できます。

次の例は、192.168.2.0/24 内部サブネットにのみアクセスする必要がある請負業者の RA VPN 接続の設定方法を示しています。通常の従業員の場合、VPNに対してトラフィックフィルタが定義されていないデフォルトグループポリシーを使用できます。これらのユーザーに制限を適用する場合は、デフォルトグループポリシーを編集して、次のように構築された ACL を適用することができます。

始める前に

次の手順では、請負業者に使用するアイデンティティソースがすでに作成されていると仮定します。これは、通常の従業員に使用するものとは異なるソースである可能性があります。アイデンティティソースはアクセスの制限に厳密に関連するものではないため、この例からは省略します。

また、この例では、「inside2」インターフェイスが 192.168.2.0/24 サブネットを IP アドレス 192.168.2.1 でホストするように設定されていると想定します（サブネット上のその他のアドレスも許容されます）。

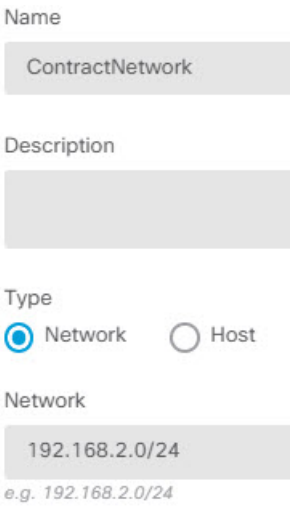
手順

ステップ 1 RA VPN トラフィックを制限するため、拡張アクセスコントロールリスト（ACL）を設定します。

まず、ターゲット 192.168.2.0/24 を定義するネットワークオブジェクトを設定し、次にアクセスリストを定義するスマート CLI オブジェクトを作成する必要があります。ACL の最後には暗黙の「deny」があるため、サブネットへのアクセスを許可することだけが必要となります。サブネット外の IP アドレスへのトラフィックは拒否されます。この例は、IPv4 のみに適用されます。また、特定のサブネットへの IPv6 アクセスを制限するためのオブジェクトも設定できます。ネットワークオブジェクトを作成し、同じ ACL に IPv6 ベースの ACE を追加するだけです。

a) **[オブジェクト（Objects）]** > **[ネットワーク（Networks）]** を選択し、必要なオブジェクトを作成します。

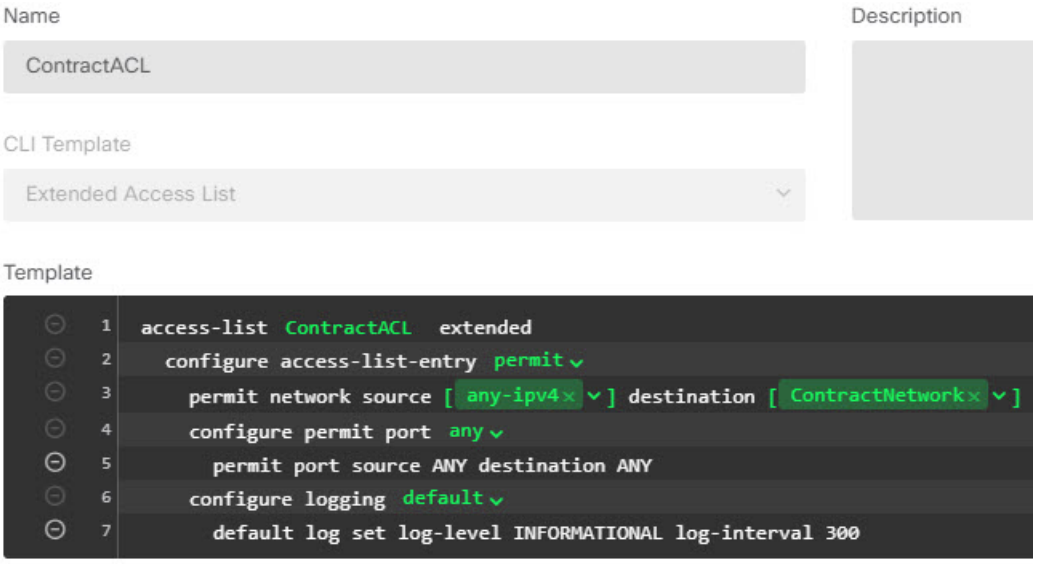
たとえば、オブジェクトにContractNetwork という名前を付けます。オブジェクトは、次のようになります。



b) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** > **[スマートCLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。
c) [+] をクリックして新しいオブジェクトを作成します。
d) ACL の名前を入力します。**ContractACL** などを入力します。
e) [CLIテンプレート（CLI Template）] の場合は、[拡張アクセスリスト（Extended Access List）] を選択します。
f) [テンプレート（Template）] 本文で次のように設定します。

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = ContractNetwork object
- configure permit port = any
- configure logging = default

ACE は次のようになります。



g) [OK] をクリックします。

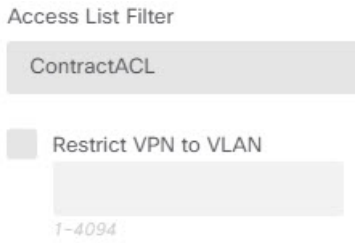
この ACL は、次に変更を展開するときに設定されます。別のポリシーでオブジェクトを使用して強制的に展開する必要はありません。

ステップ 2 ACL を使用するグループポリシーを作成します。

最低限、グループポリシーの DNS サーバーを設定する必要もあります。必要に応じて他のオプションを設定できます。次の手順は、この使用例に関連する 1 つの設定に重点を置いています。

a) **[デバイス（Device）] > [RA VPN] > [グループポリシー（Group Policies）]** を選択します。
b) [+] をクリックして新しいグループポリシーを作成します。
c) [全般（General）] ページで、ポリシーの名前（**ContractGroup** など）を入力します。
d) 目次で [トラフィックフィルタ（Traffic Filters）] をクリックします。
e) [アクセスリストフィルタ（Access List Filter）] の場合は、ContractACL オブジェクトを選択します。

この例では、VLAN オプションは空のままにします。別の方法として、フィルタリング用の VLAN を設定し、その VLAN にサブインターフェイスを設定することも可能です。



f) [OK] をクリックして、グループ ポリシーを保存します。

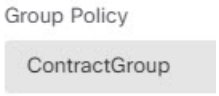
ステップ 3 コントラクタの接続プロファイルを設定します。

a) [RA VPN] ページで、目次の [接続プロファイル（Connection Profiles）] をクリックします。
b) 新しい接続プロファイルを作成するには、[+] をクリックします。
c) ウィザードのステップ 1 を完了し、[次へ（Next）] をクリックします。

プロファイルの名前（Contractors など）を入力します。

残りのオプションを通常どおりに設定します。これには、請負業者の適切な認証ソースの選択、アドレスプールの定義が含まれます。

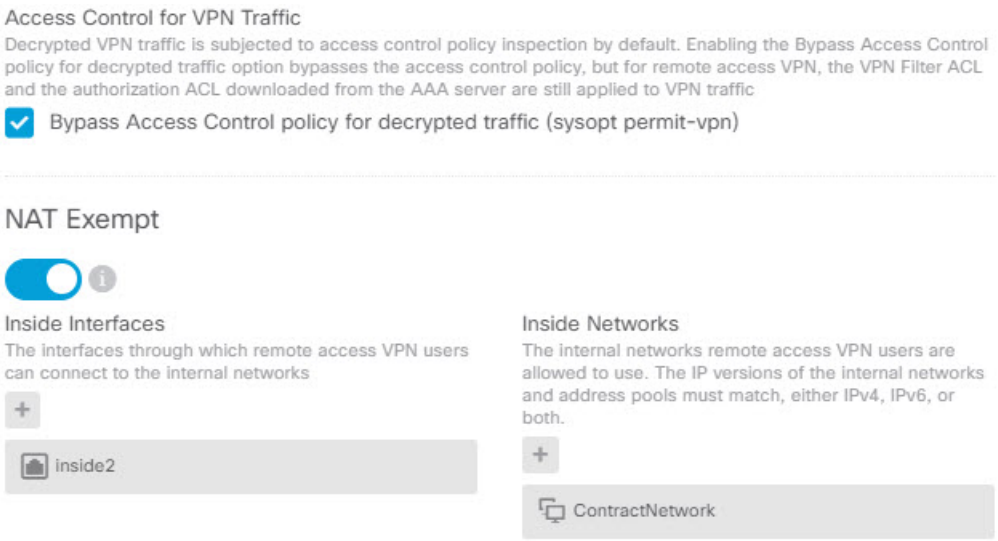
d) 請負業者用に設定されているグループポリシーを選択し、[次へ（Next）] をクリックします。



e) グローバル設定で、[復号されたトラフィックでアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択し、[NAT免除（NAT Exempt）] オプションを設定します。

[NAT免除（NAT Exempt）] では、次のオプションを設定する必要があります。他に定義済みの接続プロファイルがある場合、既存の設定に追加する必要があります。これは、その設定がすべての接続プロファイルに適用されるためです。

- [内部インターフェイス（Inside Interfaces）]：**inside2** インターフェイスを選択します。これらは、内部ネットワークのリモートユーザーがアクセスするインターフェイスです。これらのインターフェイスには NAT ルールが作成されます。
- [内部ネットワーク（Inside Networks）]：ContractNetwork ネットワーク オブジェクトを選択します。これらは、内部ネットワークのリモートユーザーがアクセスするオブジェクトを表すネットワーク オブジェクトです。



f) サポートするプラットフォームの セキュアクライアント パッケージをアップロードします。

g) [次へ（Next）] をクリックして、設定を確認します。

最初に、サマリーが正しいことを確認します。

次に、[手順（Instructions）] をクリックして、セキュアクライアント ソフトウェアをインストールし、VPN接続を完了できることをテストするためにエンドユーザーが最初に行う必要がある内容を確認します。[コピー（Copy）]をクリックして、それらの手順をクリップボードにコピーし、テキスト ファイルまたは電子メールに貼り付けます。

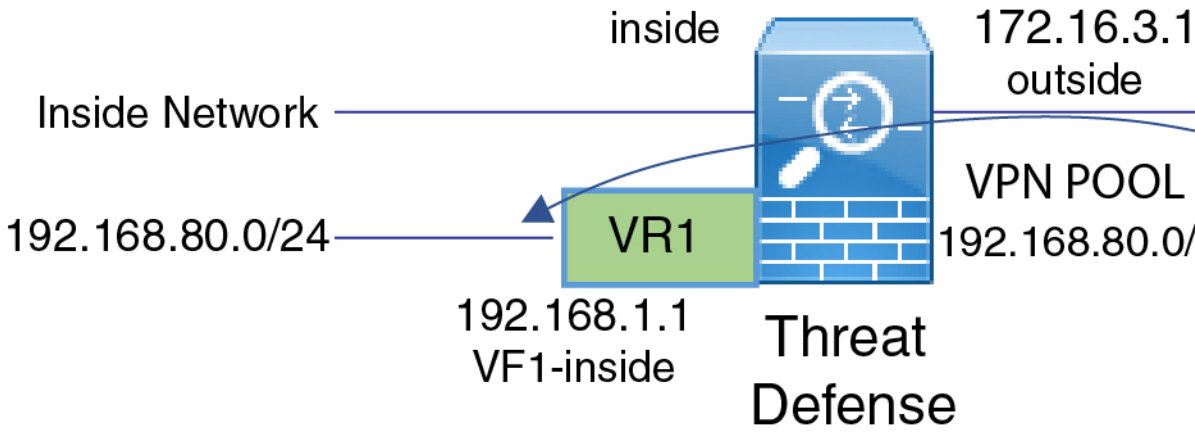
h) [終了（Finish）] をクリックします。

異なる仮想ルータの内部ネットワークへの RA VPN アクセスを可能にする方法

1 つのデバイスに複数の仮想ルータを設定する場合には、グローバル仮想ルータで RA VPN を設定する必要があります。カスタム仮想ルータに割り当てられているインターフェイスに RA VPN を設定することはできません。

仮想ルータのルーティングテーブルはそれぞれ異なるため、RA VPN ユーザーが別の仮想ルータの一部であるネットワークにアクセスする必要がある場合には、スタティックルートを作成する必要があります。

次の例を考えてみます。RA VPN ユーザーが 172.16.3.1 の外部インターフェイスに接続するとします。このユーザーには 192.168.80.0/24 のプールに含まれる IP アドレスが割り当てられます。その結果、このユーザーは、グローバル仮想ルータに接続されている内部ネットワークにアクセスできるようになります。ただし、仮想ルータ VR1 の一部である 192.168.1.0/24 ネットワークに到達することはできません。VR1 ネットワークと RA VPN ユーザー間のトラフィックフローを許可するには、双方向のスタティックルートを設定する必要があります。



始める前に

この例では、すでにRA VPNを設定し、仮想ルータを定義し、インターフェイスを設定して適切な仮想ルータに割り当てていることを前提としています。

手順

ステップ 1 グローバル仮想ルータから VR1 へのルートリークを設定します。

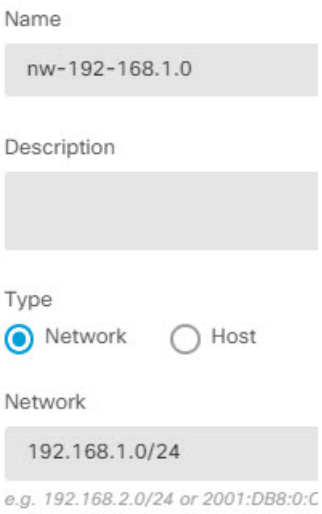
このルートにより、VPN プール内の IP アドレスが割り当てられた セキュアクライアントは、VR1 仮想ルータの 192.168.1.0/24 ネットワークにアクセスできるようになります。

a) **[デバイス（Device）]** > **[ルーティング（Routing）]** > **[設定の表示（View Configuration）]** の順に選択します。

b) グローバル仮想ルータの表示アイコン（）をクリックします。

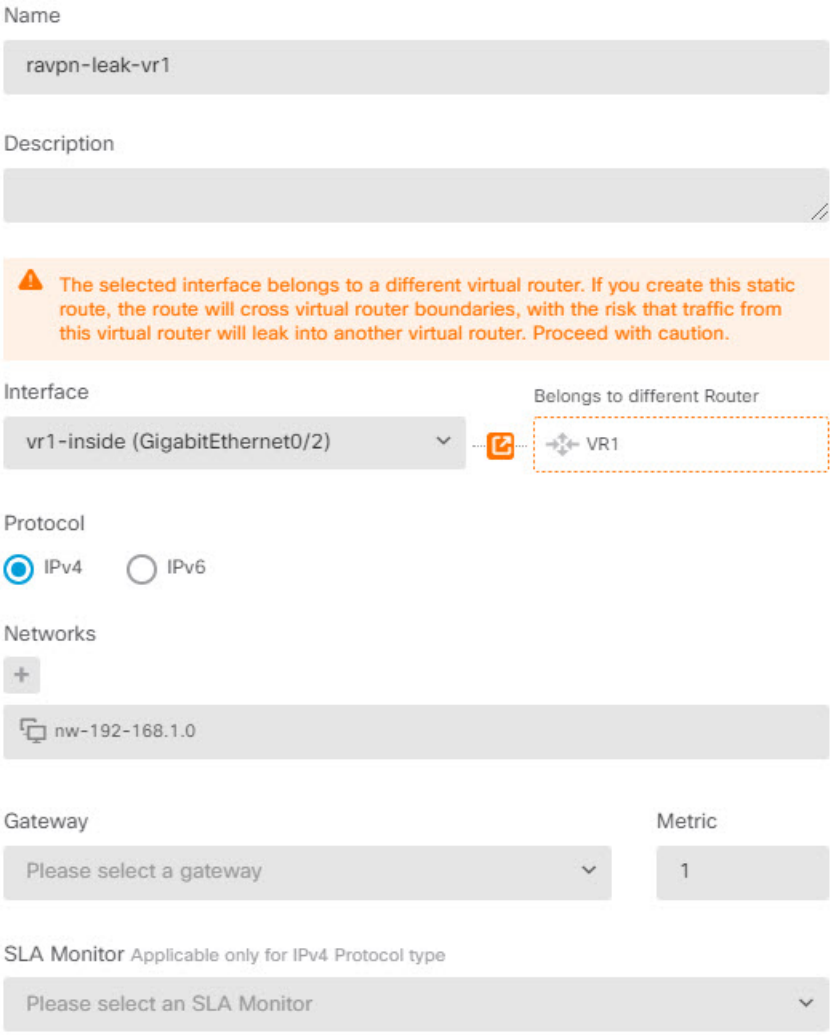
c) グローバルルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：任意の名前（**ravpn-leak-vr1** など）を付けることができます。
- [インターフェイス（Interface）]：**vr1-inside** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]：192.168.1.0/24 ネットワークを定義するオブジェクトを選択します。必要な場合には、[新しいネットワークの作成（Create New Network）] をクリックしてオブジェクトを作成します。



- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



d) [OK] をクリック

ステップ 2 VR1 からグローバル仮想ルータへのルートリークを設定します。

このルートにより、192.168.1.0/24 ネットワーク上のエンドポイントは、VPN プール内の IP アドレスが割り当てられた セキュアクライアントへの接続を開始できます。

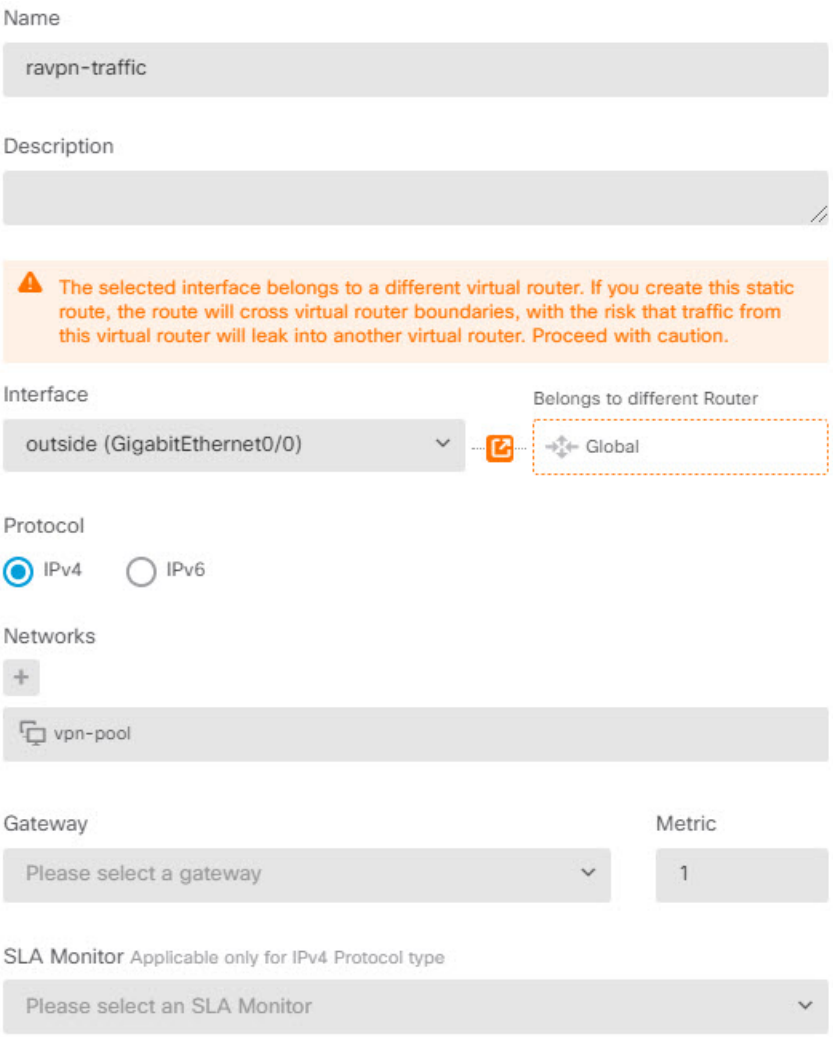
a) 仮想ルータのドロップダウンリストから [VR1] を選択して、VR1 設定に切り替えます。

b) VR1 ルータの [スタティックルーティング（Static Routing）] タブで、[+] をクリックしてルートを設定します。

- [名前（Name）]：任意の名前（**ravpn-traffic** など）を付けることができます。
- [インターフェイス（Interface）]：**outside** を選択します。
- [プロトコル（Protocol）]：**IPv4** を選択します。
- [ネットワーク（Networks）]：VPN プール用に作成したオブジェクト（**vpn-pool など**）を選択します。

- [ゲートウェイ（Gateway）]：この項目は空白のままにします。別の仮想ルータにルートをリークする場合は、ゲートウェイアドレスを選択しません。

次のようなダイアログが表示されるはずです。



c) [OK] をクリック

次のタスク

RA VPN アドレスプールとカスタム仮想ルータの IP アドレスの間に重複がある場合には、IP アドレスに対してスタティック NAT ルールを使用し、適切なルーティングを有効にする必要があります。とはいえ、単に重複しないようにRA VPNアドレスプールを変更する方がはるかに簡単です。

セキュアクライアント のアイコンとロゴをカスタマイズする方法

Windows および Linux クライアントマシン上の セキュアクライアント アプリケーションのアイコンとロゴをカスタマイズできます。アイコンの名前は事前定義されており、アップロードする画像のファイルタイプとサイズには特定の制限があります。

独自の実行可能ファイルを展開して GUI をカスタマイズする場合は、任意のファイル名を使用できますが、この例では、完全にカスタマイズされたフレームワークを展開せずに、アイコンとロゴを置き換えるだけであることを前提としています。

置き換えることができる画像はいくつかあり、それらのファイル名はプラットフォームによって異なります。カスタマイズオプション、ファイル名、タイプ、およびサイズの詳細については、『*Cisco Secure Client Administrator Guide*』の セキュアクライアントおよびインストーラのカスタマイズとローカライズに関する章を参照してください。たとえば、4.8 クライアントに関する章は次の場所にあります。

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

始める前に

この例では、Windows クライアントの次の画像を置き換えます。画像のサイズが最大サイズと異なる場合、自動的に最大サイズに変更され、必要に応じて画像が拡大されます。

- app_logo.png

  このアプリケーションロゴ画像はアプリケーションアイコンであり、最大サイズは 128 X 128 ピクセルです。

- company_logo.png

  この企業ロゴ画像は、トレイフライアウトと [詳細（Advanced）] ダイアログの左上隅に表示されます。最大サイズは 97 X 58 ピクセルです。

- company_logo_alt.png

  この代替企業ロゴ画像は、[バージョン情報（About）] ダイアログの右下隅に表示されます。最大サイズは 97 X 58 ピクセルです。

これらのファイルをアップロードするには、Threat Defense デバイスがアクセスできるサーバーにファイルを配置する必要があります。TFTP、FTP、HTTP、HTTPS、または SCP サーバーを使用できます。これらのファイルから画像を取得するための URL には、サーバーのセットアップで必要なパスとユーザー名/パスワードを含めることができます。この例では、TFTP を使用します。

手順

ステップ 1 カスタマイズされたアイコンとロゴを使用する必要がある、RA VPN ヘッドエンドとして機能している各 Threat Defense デバイスに画像ファイルをアップロードします。

a) SSH クライアントを使用してデバイス CLI にログインします。

b) CLI で、**system support diagnostic-cli** コマンドを入力して、診断 CLI モードを開始します。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

（注） メッセージに示されているように、診断 CLI を終了して通常の Threat Defense CLI モードに戻るには、**Ctrl + A キーを押してから D キーを押す**必要があります。

c) コマンドプロンプトに注意してください。通常の CLI では > だけが表示されますが、診断 CLI のユーザー EXEC モードではホスト名と > が表示されます。この例では、ftdv1> です。特権 EXEC モードを開始する必要があります。このモードでは、ftdv1# のように、# が終了文字として使用されます。プロンプトにすでに # が表示されている場合は、この手順をスキップしてください。それ以外の場合は、enable コマンドを入力し、パスワードプロンプトではパスワードを入力せずに単に Enter キーを押します。

```
ftdv1> enable
Password:
ftdv1#
```

d) **copy** コマンドを使用して、ホスティングサーバーから Threat Defense デバイスの disk0 に各ファイルをコピーします。それらのファイルは disk0:/anyconnect-images/ などのサブディレクトリに配置できます。**mkdir** コマンドを使用して新しいフォルダを作成できます。

たとえば、TFTP サーバーの IP アドレスが 10.7.0.80 であり、新しいディレクトリを作成する場合、コマンドは次のようになります。最初の例の後は **copy** コマンドへの応答が省略されていることに注意してください。

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

ステップ 2 診断 CLI で **import webvpn** コマンドを使用して、セキュアクライアント に、それ自体のクライアントマシンへのインストール時にこれらの画像をダウンロードするように指示します。

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

このコマンドはWindows用です。Linuxでは、クライアントに応じて、**win**キーワードを**linux**または**linux-64**に置き換えます。

たとえば、前の手順でアップロードしたファイルをインポートする場合、引き続き診断CLIを使用していると想定すると、次のようになります。

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

ステップ3 設定を確認します。

- インポートしたファイルを確認するには、診断CLIの特権EXECモードで**show import webvpn AnyConnect-customization**コマンドを使用します。
- 画像がクライアントにダウンロードされたことは、ユーザーがクライアントを実行したときに画像が表示されることで確認できます。Windowsクライアントで次のフォルダを確認することもできます。ここで、%PROGRAMFILES%は、通常、c:\Program Filesに置き換えられます。

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

次のタスク

デフォルトの画像に戻す場合は、カスタマイズしたイメージごとに**revert webvpn**コマンドを（診断CLIの特権EXECモードで）使用します。コマンドは、次のとおりです。

revert webvpn AnyConnect-customization type resource platform win name *filename*

import webvpnの場合と同様に、当該のクライアントプラットフォームをカスタマイズしている場合は**win**を**linux**または**linux-64**に置き換え、インポートした画像ファイル名ごとに個別にコマンドを発行してください。次に例を示します。

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

第 VII 部

システム管理

第 26 章

システム設定

ここでは、[システム設定（System Settings）] ページでグループ化されているさまざまなシステム設定の設定方法について説明します。設定は、システムの機能全体を網羅しています。

管理アクセスの設定

管理アクセスとは、設定およびモニター目的で 脅威に対する防御 デバイスにログインする機能のことです。次の項目を設定できます。

- ユーザーアクセス認証に使用するアイデンティティソースを特定するための AAA。ローカルユーザーデータベースまたは外部AAAサーバーを使用することができます。管理ユーザーの管理の詳細については、Device Manager および Threat Defense ユーザーアクセスの管理 （999 ページ）を参照してください。
- 管理インターフェイスおよびデータ インターフェイスへのアクセス制御。これらのインターフェイスには個別のアクセス リストがあります。どの IP アドレスが HTTPS（Device

Manager で使用）および SSH（CLI で使用）で許可されるかを決定できます。管理アクセス リストの設定 （924 ページ）を参照してください。

- Device Manager に接続するためにユーザーが受け入れる必要がある管理 Web サーバー証明書。Web ブラウザで信頼される証明書をアップロードすることにより、ユーザーが不明な証明書を信頼するように求められるのを回避できます。Threat Defense Web サーバー証明書の設定 （927 ページ） を参照してください。

管理アクセス リストの設定

デフォルトでは、任意の IP アドレスから、デバイスの管理アドレス上の Device Manager Web または CLI インターフェイスにアクセスできます。システム アクセスは、ユーザ名/パスワードのみで保護されています。ただし、特定の IP アドレスまたはサブネットのみからの接続を許可するようアクセス リストを設定し、さらにレベルの高い保護を提供できます。

また、データインターフェイスを開いて、Device Manager または SSH から CLI への接続を許可することもできます。これにより、管理アドレスを使用せずにデバイスを管理できます。たとえば、外部インターフェイスへの管理アクセスを許可し、デバイスをリモートで設定できます。ユーザ名/パスワードにより、不要な接続から保護します。デフォルトでは、データインターフェイスへの HTTPS 管理アクセスは内部インターフェイスで有効になっていますが、外部インターフェイスでは無効になっています。デフォルトの「内部」ブリッジグループが設定されている Firepower 1010 の場合、この設定は、ブリッジグループに含まれる任意のデータインターフェイスを使用して Device Manager をブリッジグループ IP アドレス（デフォルトは 192.168.95.1）に接続できることを意味します。管理接続は、デバイスに入るインターフェイス上でのみ開くことができます。

注意 特定のアドレスへのアクセスを制限すると、システムから簡単にロックアウトできます。現在使用している IP アドレスへのアクセスを削除し、「任意」のアドレスへのエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。アクセス リストを設定する場合は、特に注意してください。

始める前に

同じ TCP ポートの同じインターフェイスでは、Device Manager アクセス（HTTPS アクセス）とリモートアクセス SSL VPN の両方を設定できません。たとえば、外部インターフェイスにリモート アクセス SSL VPN を設定する場合、ポート 443 で HTTPS 接続用の外部インターフェイスも開くことはできません。同じインターフェイスで両方の機能を設定する場合は、競合を回避するために、必ず、これらのサービスの少なくとも 1 つの HTTPS ポートを変更してください。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[System Settings]** > **[Management Access]** の順にリンクをクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で **[管理アクセス（Management Access）]** をクリックします。

このページで AAA を設定して、外部 AAA サーバで定義されたユーザの管理アクセスを許可することもできます。詳細は、Device Manager および Threat Defense ユーザーアクセスの管理（999 ページ）を参照してください。

ステップ 2 管理アドレスのルールを作成するには、以下の手順に従います。

a) [管理インターフェイス（Management Interface）] タブを選択します。

ルールのリストは、指定されたポートへのアクセスが許可されるアドレスを定義します。Device Manager （HTTPS Web インターフェイス）の場合は 443、SSH CLI の場合は 22 です。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

（注） ルールを削除するには、ルールの [ごみ箱（trash can）] アイコン（  ）をクリックします。あるプロトコルのルールをすべて削除した場合、そのプロトコルを使用して該当インターフェイスのデバイスにアクセスすることはできなくなります。

b) [+] をクリックし、次のオプションを入力します。

- [プロトコル（Protocol）]：ルールが HTTPS（ポート 443）または SSH（ポート 22）用かを選択します。
- [IP アドレス（IP Address）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

c) [OK] をクリックします。

ステップ 3 データインターフェイスへのルールを作成するには、以下の手順に従います。

a) [データインターフェイス（Data Interfaces）] タブを選択します。

ルールのリストは、インターフェイス上の指定されたポートへのアクセスが許可されるアドレスを定義します。Device Manager （HTTPS Web インターフェイス）の場合は 443、SSH CLI の場合は 22 です。

ルールは番号付きリストではありません。IP アドレスが要求されたポートの任意のルールと一致する場合、そのユーザはデバイスへのログイン試行が許可されます。

（注） ルールを削除するには、ルールの[ごみ箱（trash can）]アイコン（）をクリックします。あるプロトコルのルールをすべて削除した場合、そのプロトコルを使用して該当インターフェイスのデバイスにアクセスすることはできなくなります。

b) [+] をクリックし、次のオプションを入力します。

- [インターフェイス（Interface）]：管理アクセスを許可するインターフェイスを選択します。
- [プロトコル（Protocols）]：ルールが HTTPS（ポート 443）または SSH（ポート 22）、またはその両方用かを選択します。外部インターフェイスがリモート アクセス VPN 接続プロファイルで使用されている場合、その外部インターフェイスに HTTPS ルールを設定することはできません。
- [許可されたネットワーク（Allowed Networks）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワーク オブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

c) （任意）HTTPS データポート番号を変更する場合は、番号をクリックし、新しいポートを入力します。データインターフェイスでの管理アクセス用の HTTPS ポートの設定 （926 ページ）を参照してください。

d) [OK] をクリックします。

データインターフェイスでの管理アクセス用の HTTPS ポートの設定

デフォルトでは、Device Manager または Threat Defense API のいずれかで管理のためにデバイスにアクセスする場合、ポート TCP/443 を経由します。データインターフェイスの管理アクセスポートは変更できます。

ポートを変更すると、ユーザは、システムにアクセスするための URL にカスタムポートを含める必要があります。たとえば、データインターフェイスが ftd.example.com であり、ポートを 4443 に変更した場合、ユーザは URL を https://ftd.example.com:4443 に変更する必要があります。

すべてのデータインターフェイスで同じポートが使用されます。インターフェイスごとに異なるポートを設定することはできません。

（注） 管理インターフェイスの管理アクセスポートは変更できません。管理インターフェイスでは常にポート 443 が使用されます。

手順

ステップ 1 [Device] をクリックしてから、**[System Settings]** > **[Management Access]** リンクの順にクリックします。

[System Settings] ページがすでに表示されている場合は、目次で [Management Access] をクリックします。

ステップ 2 [Data Interfaces] タブをクリックします。

ステップ 3 [HTTPS Data Port] 番号をクリックします。

ステップ 4 [Data Interfaces Setting] ダイアログボックスで [HTTPS Data Port] を、使用するポートに変更します。

次の番号は指定できません。

- 22：このポートは SSH 接続に使用されます。
- リモートアクセス VPN に使用するポート（管理アクセスも許可されているインターフェイス用に設定されている場合）：リモートアクセス VPN はデフォルトではポート 443 を使用しますが、カスタムポートを設定できます。
- アイデンティティポリシーでアクティブ認証に使用するポート：デフォルトは 885 です。

ステップ 5 [OK] をクリックします。

Threat Defense Web サーバー証明書の設定

Web インターフェイスにログインするときに、システムはデジタル証明書を使用して HTTPS で通信を保護します。デフォルトの証明書はブラウザで信頼されていないため、Untrusted Authority という警告が表示され、証明書を信頼するかどうかを確認されます。ユーザーは証明書を Trusted Root Certificate ストアに保存することもできますが、その代わりにブラウザが信頼するように設定されている新しい証明書をアップロードすることもできます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンクの順にクリックします。

[System Settings] ページがすでに表示されている場合は、目次で [Management Access] をクリックします。

ステップ 2 [管理Webサーバ（Management Web Server）] タブをクリックします。

ステップ 3 [Webサーバ証明書（Web Server Certificate）] で、Device Manager への HTTPS 接続をセキュリティ保護するために使用する内部証明書を選択します。

証明書をアップロードまたは作成していない場合、リストの下部にある [内部証明書の新規作成（Create New Internal Certificate）] リンクをクリックして作成します。

デフォルトは、事前に定義された DefaultWebserverCertificate オブジェクトです。

ステップ 4 証明書が自己署名されていない場合は、完全な信頼チェーン内のすべての中間証明書とルート証明書を信頼チェーンリストに追加します。

チェーンには最大 10 個の証明書を追加できます。[+] をクリックして各中間証明書を追加し、最後にルート証明書を追加します。[保存（Save）] をクリックし（Webサーバの再起動を警告するダイアログで [続行（Proceed）] をクリックすると）、証明書がない場合は、欠落しているチェーン内の次の証明書の共通名を含むエラーメッセージが表示されます。チェーンに含まれていない証明書を追加した場合も、エラーが表示されます。これらのメッセージを慎重に調べて、追加または削除する必要がある証明書を特定してください。

ここから証明書をアップロードするには、[+] をクリックした後に、[新規信頼CA証明書の作成（Create New Trusted CA Certificate）] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

変更はすぐに適用され、システムは Web サーバーを再起動します。設定を展開する必要はありません。

数分待って再起動が完了してから、ブラウザを更新します。

システム ロギングの設定

Threat Defense デバイスのシステム ロギング（syslog）を有効にすることができます。情報をロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。syslog は、アクセス制御、侵入防御、およびファイルとマルウェアのロギングを含む診断ロギングおよび接続関連ロギングのために有効にすることができます。

診断ロギングは、デバイスとシステムの正常性に関連するイベントと、接続とは関係のないネットワーク設定に関する syslog メッセージを提供します。個々のアクセス コントロール ルール内に接続ロギングを設定します。

診断ロギングでは、データプレーン上で実行されている機能、つまり **show running-config** コマンドで表示できる CLI 設定で定義されている機能に関するメッセージが生成されます。これには、ルーティング、VPN、データ インターフェイス、DHCP サーバ、NAT などの機能が含まれます。

これらのメッセージの詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html にある『*Cisco Threat Defense Syslog Messages*』を参照してください。

次のトピックでは、さまざまな出力場所に対するの診断メッセージやファイル/マルウェア メッセージのロギングを設定する方法について説明します。

シビラティ（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。

表 *16 : 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。
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 および Threat Defense は、重大度 0（緊急）の syslog メッセージを生成しません。

リモート syslog サーバーのロギングの設定

syslog のメッセージを外部 syslog サーバーに送信するようにシステムを設定できます。これはシステムロギングの最適なオプションです。外部サーバーを使用すると、メッセージを保持するためのスペースを確保し、サーバーの施設を使用してメッセージを表示、分析、およびアーカイブできます。

さらに、アクセス制御ルールでトラフィックにファイルポリシーを適用してファイルへのアクセスまたはマルウェア、あるいはその両方を制御する場合、外部syslogサーバーにファイルイベントメッセージを送信するようにシステムを設定できます。syslog サーバーを設定しない場合、イベントは Device Manager イベントビューアのみに表示されます。

次の手順では、診断（データ）ロギングとファイル/マルウェアロギング用に Syslog をイネーブルにする方法について説明します。次のイベント用に外部ロギングを設定することもできます。

- 接続イベント。個々のアクセス制御ルール、SSL復号ルール、またはセキュリティインテリジェンス ポリシー設定で Syslog サーバーを選択します。
- 侵入イベントの場合は、侵入ポリシーの設定で syslog サーバーを選択します。

始める前に

ファイル/マルウェアイベントの syslog 設定は、IPS およびマルウェア防御ライセンスを必要とするファイルまたはマルウェアのポリシーを適用する場合にのみ該当します。

さらに、ポリシーを適用するアクセス制御ルールで、**[ファイルイベント（File Events）]**>**[ファイルのロギング（Log Files）]** オプションが選択されていることを確認する必要があります。そうでない場合、syslog でもイベントビューアでもイベントはまったく生成されません。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]**>**[ログ設定（Logging Settings）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）] をクリックします。

ステップ 2 [リモートサーバー（Remote Server）] の下の [データロギング（Data Logging）] スライダを「オン」にして、データプレーンで生成された診断メッセージの外部syslogサーバーへのロギングを有効にします。その後、次のオプションを設定します。

- [Syslogサーバー（Syslog Server）]：[+] をクリックし、1 つまたは複数の syslog サーバーオブジェクトを選択して、[OK] をクリックします。オブジェクトが存在しない場合は、[Syslog サーバーの追加（Add Syslog Server）] リンクをクリックして作成します。詳細については、「Syslog サーバーの設定 （175 ページ）」を参照してください。
- [FXOSシャーシsyslogのフィルタリングの重大度レベル（Severity Level for Filtering FXOS Chassis Syslogs）]：FXOS を使用する特定のデバイス モデルの、基本の FXOS プラットフォームによって生成される syslog メッセージの重大度レベル。このオプションは、デバイスに関連している場合にのみ表示されます。重大度のレベルを選択します。このレベル以上のメッセージが syslog サーバーに送信されます。
- [メッセージフィルタリング（Message Filtering）]：Threat Defense のオペレーティングシステム用に生成されたメッセージを制御するには、次のオプションのいずれかを選択します。
  - [すべてのイベントのフィルタリングの重大度レベル（Severity Level for Filtering All Events）]：重大度レベルを選択します。このレベル以上のメッセージが syslog サーバーに送信されます。
  - [カスタムロギングフィルタ（Custom Logging Filter）]：関心のあるメッセージのみを取得するために追加のメッセージフィルタリングを行う場合、生成させたいメッセージを定義するイベントリストフィルタを選択します。このフィルタが存在しない場合は、[新しいイベントリストフィルタの作成（Create New Event List Filter）] をクリッ

クして作成します。詳細については、「イベント リスト フィルタの設定 （932 ページ）」を参照してください。

ステップ 3 ファイルおよびマルウェアのイベントの外部syslogサーバーへのロギングを有効にするには、[ファイル/マルウェア（File/Malware）] スライダを「オン」にします。次に、ファイル/マルウェアロギングのオプションを設定します。

- [Syslogサーバー（Syslog Server）]：syslog サーバー オブジェクトを選択します。オブジェクトが存在しない場合は、[Syslogサーバーの追加（Add Syslog Server）] リンクをクリックして作成します。
- [重大度レベルのログ（Log at Severity Level）]：ファイル/マルウェア イベントに割り当てる重大度レベルを選択します。すべてのファイル/マルウェアイベントが同じ重大度で生成されるため、フィルタリングは実行されません。選択したレベルに関係なく、すべてのイベントが表示されます。これは、メッセージの [シビラティ（重大度）（severity）] フィールドに表示されるレベルになります（つまり、FTD-x-<message_ID>のx）。ファイルイベントはメッセージ ID 430004 であり、マルウェアイベントは 430005 です。

ステップ 4 [保存（Save）] をクリックします。

内部バッファへのロギングの設定

システムを設定して、内部ロギングバッファに syslog メッセージを保存できます。このバッファの内容を表示するには、CLI または CLI コンソールで **show logging** コマンドを使用します。

新しいメッセージは、バッファの最後に追加されます。バッファの空きがなくなると、システムはバッファをクリアしてから、メッセージの追加を続行します。ログバッファに空きがなくなると、システムは最も古いメッセージを削除して、バッファに新しいメッセージ用の領域を確保します。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[ログ設定（Logging Settings）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）] をクリックします。

ステップ 2 ロギングの宛先としてバッファを有効にするには、[内部バッファ（Internal Buffer）] スライダを「オン」にします。

ステップ 3 内部バッファロギングのオプションの設定。

- [すべてのイベントのフィルタリングの重大度レベル（Severity Level for Filtering All Events）]：重大度レベルを選択します。このレベル以上のメッセージが内部バッファに送信されます。
- [カスタムロギングフィルタ（Custom Logging Filter）]：（オプション）関心のあるメッセージのみを取得するために追加のメッセージフィルタリングを行う場合、生成するメッセージを定義するイベント リスト フィルタを選択します。このフィルタが存在しない場合は、[新しいイベントリストフィルタの作成（Create New Event List Filter）] をクリックして作成します。詳細については、「イベントリストフィルタの設定（932ページ）」を参照してください。
- [バッファサイズ（Buffer Size）]：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。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。指定できる範囲は 4096 ～ 52428800 です。

ステップ 4 [保存（Save）] をクリックします。

コンソールへのロギングの設定

コンソールにメッセージを送信するようにシステムを設定できます。コンソールポートの CLI にログインしたときにこれらのメッセージが表示されます。さらに、**show console-output** コマンドを使用することで、他のインターフェイス（管理アドレスを含む）に対する SSH セッションでもこれらのログが表示されます。さらに、メイン CLI から **system support diagnostic-cli** と入力すると、診断 CLI でリアルタイムでこれらのメッセージを表示できます。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[ログ設定（Logging Settings）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [ロギングの設定（Logging Settings）] をクリックします。

ステップ 2 ロギングの宛先としてコンソールを有効にするには、[コンソールフィルタ（Console Filter）] スライダを「オン」にします。

ステップ 3 **重大度**のレベルを選択します。このレベル以上のメッセージがコンソールに送信されます。

ステップ 4 [保存（Save）] をクリックします。

イベント リスト フィルタの設定

[イベントリストフィルタ（event list filter）] は、宛先に送信されるメッセージを制御するためにロギング宛先に適用できるカスタムフィルタです。通常は、シビラティ（重大度）のみに基

づいて宛先へのメッセージをフィルタ処理しますが、カスタムフィルタを使用すると、イベントクラス、シビラティ（重大度）、およびメッセージ識別子（ID）の組み合わせに基づいて、送信するメッセージを微調整できます。

シビラティ（重大度）レベル単独でのメッセージの制限では目的を十分に果たせない場合は、フィルタを使用します。

次の手順では、[オブジェクト（Objects）]ページでフィルタを設定する方法について説明します。フィルタを使用できるロギング宛先の設定時にフィルタを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から **[イベントリストフィルタ（Event List Filters）]** を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 フィルタのプロパティを設定します。

- [名前（Name）]：フィルタ オブジェクトの名前。
- [説明（Description）]：（オプション）オブジェクトの説明。
- [重大度とログクラス（Severity and Log Class）]：メッセージクラスでフィルタリングする場合は、[+] をクリックしてクラス フィルタの重大度レベルを選択し、[OK] をクリックします。次に、シビラティ（重大度）レベル内のドロップダウン矢印をクリックして、そのシビラティ（重大度）レベルでフィルタ処理する 1 つ以上のクラスを選択し、[OK] をクリックします。

  システムは、そのシビラティ（重大度）レベル以上のメッセージがある場合にのみ、指定されたメッセージクラスの syslog メッセージを送信します。各シビラティ（重大度）レベルには、最大で 1 つの行を追加できます。

  特定の重大度レベルですべてのクラスをフィルタリングする場合は、重大度リストを空のままにし、その代わりに、ロギング宛先を有効にするときにそのロギング宛先のグローバル重大度レベルを選択します。
- [Syslog範囲/メッセージID（Syslog Range/Message ID）]：syslog メッセージ ID でフィルタリングする場合は、単独のメッセージ ID、またはメッセージを生成する ID 番号の範囲を入力します。開始番号と終了番号は、100000-200000 のようにハイフンで区切ります。ID は 6 桁の数字です。特定のメッセージ ID および関連するメッセージについては、https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html の『*Cisco Threat Defense Syslog Messages*』を参照してください。

ステップ 4 [保存（**Save**）] をクリックします。

これで、[カスタムフィルタリング（custom filtering）] オプションでこのオブジェクトを選択して、そのオブジェクトを許可する宛先をロギングできます。**[デバイス（Device）] > [システム設定（System Settings）] > [ロギング設定（Logging Settings）]** に移動します。

DHCP の設定

DHCP サーバは、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。インターフェイス上の DHCP サーバーを設定して、接続されたネットワーク上の DHCP クライアントに設定パラメータを提供するか、またはインターフェイス上の DHCP リレーを有効にして、ネットワーク内の別のデバイスで動作している外部 DHCP サーバーに要求を転送できます。

これらの機能は相互に排他的です。いずれか一方のみ設定でき、両方は設定できません。

DHCP サーバの設定

DHCP サーバは、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。接続されたネットワークで DHCP クライアントに構成パラメータを提供するように、インターフェイスで DHCP サーバを設定できます。

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 サーバは、BOOTP 要求をサポートしていません。

（注） すでに DHCP サーバが動作しているネットワークで DHCP サーバを設定しないでください。2 つのサーバが競合するため、結果は予測不可能になります。

始める前に

DHCP クライアントは、サーバが有効になっているインターフェイスと同じネットワークに属している必要があります。つまり、スイッチがあるとしても、サーバとクライアントの間にルータを介在させることはできません。

複数のネットワークをサポートする必要があり、各インターフェイスで DHCP サーバを設定したくない場合は、代わりに DHCP リレーを設定して、一つのネットワークから別のネットワークに存在する DHCP サーバに DHCP 要求を転送できます。この場合、DHCP サーバはネットワーク内の別のデバイス上に存在する必要があります。一つのインターフェイスで DHCP サーバを設定し、同じデバイスの別のインターフェイスで DHCP リレーを設定することはできません。DHCP リレーを使用する場合は、DHCP サーバが管理する各ネットワークアドレス空間のアドレスプールを DHCP サーバに設定してください。

DHCP リレーを設定する方法については、DHCP リレーの設定 （937 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[DHCP サーバー/リレー（DHCP Server / Relay）]** リンクをクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、目次の [DHCPサーバー（DHCP Server）] **[DHCP]** > **[DHCPサーバー（DHCP Server）]** をクリックします。

ページには 2 つのタブがあります。当初、[設定（Configuration）] タブには、グローバル パラメータが表示されます。

[DHCPサーバ（DHCP Servers）] タブには、DHCP サーバを設定したインターフェイスと、サーバが有効にされているかどうか、そしてサーバのアドレス プールが表示されます。

ステップ 2 [設定（Configuration）] タブで、自動設定およびグローバル設定を設定します。

DHCP 自動設定では、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、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

a) 自動設定を利用する場合、**[自動設定を有効にする（Enable Auto Configuration）]** > **[オン（On）]** をクリックしてから（スライダは右側に移動）、DHCP を介してアドレスを取得するインターフェイスを [次のインターフェイスから取得（From Interface）] で選択します。

仮想ルータを設定する場合、DHCP サーバの自動設定は、グローバル仮想ルータのインターフェイスのみで使用できます。自動設定は、ユーザ定義の仮想ルータに割り当てられているインターフェイスではサポートされていません。

b) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、次のグローバル オプションを設定します。これらの設定は、DHCP サーバをホストするすべてのインターフェイスで DHCP クライアントに送信されます。

- [プライマリ WINS IPアドレス（Primary WINS IP Address）]、[セカンダリ WINS IPアドレス（Secondary WINS IP Address）]：Windows インターネット ネーム サービス（WINS）サーバ クライアントのアドレスは、NetBIOS の名前解決に使用されます。
- [プライマリ DNS IPアドレス（Primary DNS IP Address）]、[セカンダリ DNS IPアドレス（Secondary DNS IP Address）]：クライアントがドメイン名の解決に使用するドメイン ネーム システム（DNS）サーバのアドレス。OpenDNS パブリック DNS サーバを設定するには、[OpenDNSを使用する（Use OpenDNS）] をクリックします。ボタンをクリックすると、適切な IP アドレスがフィールドにロードされます。

c) [保存（Save）] をクリックします。

ステップ 3 [DHCPサーバ（DHCP Servers）] タブをクリックし、サーバを設定します。

a) 次のいずれかを実行します。

- まだリストされていないインターフェイスの DHCP サーバを設定するには、[+] をクリックします。
- 既存の DHCP サーバを編集するには、そのサーバの編集アイコン（）をクリックします。

サーバを削除するには、サーバのごみ箱アイコン（）をクリックします。

b) サーバ プロパティを設定します。

- [DHCPサーバを有効にする（Enable DHCP Server）]：サーバを有効にするかどうかを決定します。サーバを設定できますが、使用する準備が整うまでサーバは無効にしておきます。
- [インターフェイス（Interface）]：クライアントに DHCP アドレスを提供するインターフェイスを選択します。インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバを実行する場合、インターフェイス アドレスの取得に DHCP を使用することはできません。ブリッジ グループの場合、 メンバー インターフェイスではなく、ブリッジ仮想インターフェイス（BVI）で DHCP サーバを設定します。そうすると、サーバはすべてのメンバーインターフェイスで有効になります。

  この画面で Management インターフェイス上に DHCP サーバーを設定することはできません。その代わりに、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページで、管理インターフェイス上に DHCP サーバーを設定します。
- [アドレスプール（Address Pool）]：アドレスを要求するクライアントにサーバが提供できる IP アドレスの最小から最大までの範囲。プールの開始アドレスと終了アドレスをハイフンで区切って指定します。たとえば、 10.100.10.12-10.100.10.250 のように指定します。

  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体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。

  アドレスプールのサイズは、脅威に対する防御デバイス上のプールあたり 256 アドレスに制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、脅威に対する防御インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

c) [OK] をクリックします。

DHCP リレーの設定

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、脅威に対する防御 デバイス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脅威に対する防御デバイスのインターフェイスを、別のインターフェイスを介して利用可能な DHCP サーバに DHCP 要求を転送するように設定できます。

そのため、DHCP サーバをホストしていないサブネット上のクライアントでも、別のサブネットに存在する DHCP サーバから IP アドレスリースを取得できます。

始める前に

- 追加するサブネットごとに、アドレスプールを使用して DHCP サーバを設定します。たとえば、アドレスが 192.168.1.1/24 のインターフェイスで DHCP リレークライアントを有効にする場合、192.168.1.0/24 ネットワーク上のクライアントをサポートするには、DHCP サーバが 192.168.1.0/24 サブネットの IP アドレス（192.168.1.2 ～ 192.168.1.254 など）を提供できる必要があります。
- DHCP サーバごとに、サーバの IP アドレスを指定して、ホスト ネットワーク オブジェクトを作成します。
- **[DHCP]** > **[DHCPサーバ（DHCP Servers）]** ページで、すべてのサーバが削除または無効化されていることを確認します。いずれかのインターフェイスで DHCP リレーが有効になっている場合は、どのインターフェイスでも（異なるインターフェイスであっても）DHCP サーバをホストできません。
- インターフェイスに関する制限：インターフェイスには、サーバまたはエージェントのいずれかに使用される名前が必要です。また、次の点に注意してください。
  - インターフェイスをルーティング ECMP トラフィックゾーンのメンバーにすることはできません。
  - インターフェイスは DHCP を使用してアドレスを取得できません。
  - DHCP サーバと DHCP リレーの両方を、物理インターフェイス、サブインターフェイス、VLAN インターフェイス、および EtherChannel で設定できます（それらのメンバーでは設定できない）。
  - 仮想トンネルインターフェイス（VTI）で DHCP リレーサーバを設定することもできます。
  - どちらのサービスも、管理インターフェイス、またはブリッジグループとそのメンバーをサポートしません。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[DHCPサーバ/リレー（DHCP Server / Relay）]** リンクをクリックして、目次の **[DHCP]** > **[DHCPリレー（DHCP Relay）]** をクリックします。

[システム設定（System Settings）] ページをすでに開いている場合は、目次の **[DHCP]** > **[DHCPリレー（DHCP Relay）]** をクリックします。

ステップ 2 （任意）必要に応じて、[IPv4リレータイムアウト（IPv4 Relay Timeout）] と [IPv6リレータイムアウト（IPv6 Relay Timeout）] の設定を調整します。

これらのタイムアウトにより、特定の IP バージョンの DHCP リレー アドレス ネゴシエーションで許可される秒数が設定されます。デフォルトは 60 秒（1 分）ですが、1 ー 3600 秒の範囲で異なるタイムアウトを設定できます。サブネットと DHCP サーバの間に大きな遅延がある場合は、タイムアウトを長くすることが適切である可能性があります。

ステップ 3 **DHCP リレーサーバ**を設定します。

DHCP リレーサーバは、DHCP リレー要求を処理するネットワーク内の DHCP サーバです。これらの DHCP サーバは、ネットワーク内の設定しているデバイスとは異なるデバイス上に存在します。

a) [+] をクリックし、DHCP サーバの IP アドレスを持つホストネットワークオブジェクトを選択して、[OK] をクリックします。

オブジェクトがまだ存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。追加した DHCP サーバを使用する必要がなくなった場合は、サーバのエントリの右側にある [X] をクリックして削除します。

b) 追加した DHCP サーバのエントリをクリックし、その DHCP サーバに到達できるインターフェイスを選択します。

ステップ 4 DHCP リレーエージェントを設定します。

DHCP リレーエージェントはインターフェイス上で動作します。これらは、ネットワークセグメント上のクライアントからの DHCP 要求を DHCP サーバに転送してから、応答をクライアントに返します。

a) [+] をクリックし、DHCP リレーエージェントを実行するインターフェイスを選択して、[OK] をクリックします。

インターフェイスで DHCP リレーエージェントを実行する必要がなくなった場合は、サーバのエントリの右側にある [X] をクリックして削除します。必要に応じて、テーブルからインターフェイスを削除せず、単にすべての DHCP リレーサービスを無効にすることができます。

b) 追加したインターフェイスエントリをクリックし、エージェントが提供する DHCP サービスを選択して、[OK] をクリックします。

- [IPv4 を有効にする（Enable IPv4）]：IPv4 アドレス要求を DHCP サーバに転送します。このオプションを選択しない場合、IPv4 アドレス要求は無視され、クライアントは IPv4 アドレスを取得できません。
- [ルート設定（Set Route）]（IPv4 のみ）：DHCP サーバーから送信されるパケットにある最初のデフォルトルータアドレスを、DHCP リレーエージェントを実行している脅威に対する防御デバイス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 サーバで異なるルータが指定されている場合でも、脅威に対する防御デバイス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、DHCP リレーエージェントは、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 を有効にする（Enable IPv6）]：IPv6 アドレス要求を DHCP サーバに転送します。このオプションを選択しない場合、IPv6 アドレス要求は無視され、クライアントは IPv6 アドレスを取得できません。

ステップ 5 [保存（Save）] をクリックします。

ダイナミック DNS（DDNS）の設定

Web 更新方式を使用してダイナミック ドメイン ネーム システム（DDNS）の変更をダイナミック DNS サービスに送信するようにシステムを設定できます。これらのサービスは、完全修飾ドメイン名（FQDN）に関連付けられた新しい IP アドレスを使用するように DNS サーバを更新します。これにより、ユーザがホスト名を使用してシステムにアクセスしようとしたときに、DNS によって名前が正しい IP アドレスに解決されます。

DDNS を使用すると、システムのインターフェイスに定義された FQDN が常に正しい IP アドレスに解決されるようになります。これは、DHCP を使用してインターフェイスのアドレスを取得するように設定する場合に特に重要です。また、スタティック IP アドレスに使用しても効果的です。DNS サーバに正しいアドレスが保持され、スタティックアドレスを変更した場合に簡単に更新できるようになります。

選択した DDNS サービスプロバイダーのグループを使用するように DDNS を設定できるほか、カスタムオプションを使用すると Web 更新をサポートする他の DDNS プロバイダーに更新を送信できます。インターフェイスに指定する FQDN をこれらのサービスプロバイダーに登録する必要があります。

（注） Device Manager を使用して設定できるのは Web 更新の DDNS のみです。IETF RFC 2136 で定義されている方式の DDNS は設定できません。

始める前に

プロバイダーの証明書を検証する信頼できる CA 証明書が必要です。この証明書がシステムにないと、DDNS 接続は成功しません。証明書はサービスプロバイダーのサイトからダウンロードできます。適切な証明書がアップロードされて展開されていることを確認してください。また、アップロードした証明書の [検証の使用（Validation Usage）] が SSL サーバーを含むように設定されていることを確認します。「信頼できる CA 証明書のアップロード（188 ページ）」を参照してください。

手順

ステップ 1 [Device] をクリックし、**[System Settings]** > **[DDNS Service]** リンクをクリックします。

[System Settings] ページをすでに開いている場合、目次の [DDNS Service] をクリックします。

このページには、サービスプロバイダー、インターフェイス、インターフェイスの完全修飾ドメイン名（FQDN）、DNS サーバーで FQDN の IP アドレスの変更を更新する頻度など、DDNS 更新方式のリストが表示されます。エントリの [ステータスの表示（Show Status）] リンクをクリックすると、エントリが正しく機能しているかどうかを確認できます。

ステップ 2 次のいずれかを実行します。

- 新しいダイナミック DNS 更新方式を作成するには、[+] または [Create DDNS Service] ボタンをクリックします。
- 既存のダイナミック DNS 更新方式を編集するには、その方式の編集アイコン（  ）をクリックします。

方式を削除するには、その方式のごみ箱アイコン（  ）をクリックします。

ステップ 3 ダイナミック DNS サービスのプロパティを設定します。

- [Name]：サービスの名前。
- [Web Type Update]：DDNS サービスプロバイダーでサポートされる内容に基づいて、更新するアドレスのタイプを選択します。デフォルトは [All Addresses] で、IPv4 と IPv6 の両方のすべてのアドレスが更新されます。代わりに [IPv4 Address]、[IPv4 and One IPv6 Address]、[One IPv6 Address]、または [All IPv6 Addresses] を選択すると、該当するアドレスを更新できます。

  IPv6 アドレスについては、次の点に注意してください。

  - 更新されるのはグローバルアドレスのみです。リンクローカルアドレスは更新されません。
  - Device Manager では各インターフェイスに設定できる IPv6 アドレスは 1 つだけであるため、1 つの IPv6 アドレスのみが更新されます。
- [Service Provider]：ダイナミック DNS 更新を受信して処理するサービスプロバイダーを選択します。次のサービスプロバイダーを使用できます。

- [No-IP]：No-IP DDNS サービスプロバイダー（https://www.noip.com/）。
- [Dynamic DNS]：Oracle Dynamic DNS サービスプロバイダー（https://account.dyn.com/）。
- [Google]：Google Domains サービスプロバイダー（https://domains.google.com）。
- [Custom URL]：その他の DDNS サービスプロバイダー。選択したプロバイダーに必要な URL（ユーザ名とパスワードを含む）を [Web URL] フィールドに入力する必要があります。DDNS サービスは、https://help.dyn.com/remote-access-api/ で説明されている標準に従う必要があります。

- [Username] と [Password]（[Custom URL] 以外の方式）：ダイナミック DNS 更新を送信するときに使用するユーザ名とパスワード（サービスプロバイダーのプラットフォームで定義）。

  注：

  - ユーザ名にスペースや@および:を含めることはできません。これらの文字はデリミタとして使用されます。
  - パスワードにスペースや @ を含めることはできません。この文字はデリミタとして使用されます。最初の : から @ までの間にある : は、パスワードの一部と見なされます。

- [Web URL]（[Custom URL] 方式）：サービスプロバイダーとしてカスタム URL を選択した場合、ダイナミック DNS サービスの URL を入力します。URL は次の形式にする必要があり、511 文字までに制限されます。

  http(s)://username:password@provider-domain/xyz?hostname=<h> &myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- [Interfaces and Fully-Qualified Domain Name]：このサービスプロバイダーで DNS レコードを更新するインターフェイスを選択し、各インターフェイスの完全修飾ドメイン名を入力します。たとえば、interface.example.com のようになります。インターフェイスには次の制限があります。
  - 名前付きの物理インターフェイスとサブインターフェイスのみを選択できます。
  - 管理、BVI/EtherChannel またはそのメンバー、VLAN、仮想トンネルインターフェイス（VTI）のタイプのインターフェイスは選択できません。
  - 各インターフェイスは 1 つの DDNS 更新方式でのみ選択できます。同じ DDNS 更新オブジェクトでサービスプロバイダーを使用するすべてのインターフェイスを選択できます。

- [Update Interval]：ダイナミック DNS 更新を送信する頻度。デフォルトは [On Change] で、インターフェイスの IP アドレスが変更されるたびに更新が送信されます。ほかに、[Hourly]、[Daily]、または [Monthly] を選択できます。更新を毎日送信する場合は時刻を設定し、毎月送信する場合は時刻と日付を設定します。

ステップ 4 [OK] をクリックします。

DNS の設定

ドメインネームシステム（DNS）サーバーは、IPアドレスのホスト名の解決に使用されます。初期システムセットアップ時にDNSサーバを設定します。それにより、これらのサーバがデータインターフェイスと管理インターフェイスに適用されます。セットアップ後に変更することが可能です。また、データ インターフェイスと管理インターフェイスに個別のサーバ セットを使用できます。

少なくとも、管理インターフェイスの DNS を設定する必要があります。FQDN ベースのアクセス制御ルールを使用する場合や、**ping** などの CLI コマンドでホスト名を使用する場合は、データインターフェイスの DNS も設定する必要があります。

DNS の設定は、DNS グループを設定し、インターフェイスで DNS を設定するという 2 手順のプロセスです。

ここでは、このプロセスについて詳しく説明します。

DNS グループの設定

DNS グループは、DNS サーバーおよび関連付けられているいくつかの属性のリストを定義します。管理インターフェイスとデータ インターフェイスで別々に DNS を設定できます。www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するのには、DNS サーバーが必要です。

デバイス セットアップ ウィザードが完了した後、次のシステム定義 DNS グループの一方または両方を使用できます。

- CiscoUmbrellaDNSServerGroup：このグループには、Cisco Umbrella と使用できる DNS サーバの IP アドレスが含まれています。初期セットアップ時にこれらのサーバを選択した場合、これが唯一のシステム定義グループになります。このグループの名前またはサーバリストを変更することはできませんが、他のプロパティは編集できます。
- CustomDNSServerGroup：デバイス セットアップ時に Umbrella サーバを選択していない場合、システムはサーバリストを使用してこのグループを作成します。このグループのすべてのプロパティを編集できます。

手順

ステップ 1 [オブジェクト（Objects）] を選択して、目次から [DNSグループ（DNS Groups）] を選択します。

ステップ 2 次のいずれかを実行します。

- グループを作成するには、[グループの追加（Add Group）] ボタン（）をクリックします。
- グループを編集するには、そのグループの [編集（edit）] アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 次のプロパティを設定します。

- [名前（Name）]：DNS サーバ グループの名前。DefaultDNS という名前は予約済みで使用できません。
- [DNS IPアドレス（DNS IP Addresses）]：DNS サーバの IP アドレスを入力します。複数のサーバを設定するには、[別のDNS IPアドレスを追加（Add Another DNS IP Address）] をクリックします。サーバー アドレスを削除する場合は、アドレスの [削除（delete）] アイコン（）をクリックします。

  リストは優先順です。リストの最初のサーバが常に使用されます。後続のサーバは、上位のサーバから応答が受信されない場合にのみ使用されます。最大 6 台のサーバを設定できます。ただし、6 台のサーバはデータ インターフェイスでのみサポートされます。管理インターフェイスでは、最初の 3 台のサーバのみが使用されます。
- [ドメイン検索名（Domain Search Name）]：ネットワークのドメイン名（example.com など）を入力します。このドメインは、完全修飾されていないホスト名（たとえば、serverA.example.com ではなく serverA）に追加されます。名前は、データ インターフェイスのグループを使用するために 63 文字以下にする必要があります。
- [再試行（Retries）]：システムが応答を受信しない場合に DNS サーバーのリストを再試行する回数（0 ～ 10 の範囲）。デフォルトは 2 です。この設定は、データ インターフェイスのみで使用される DNS グループに適用されます。
- [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。システム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 2 倍になります。この設定は、データ インターフェイスのみで使用される DNS グループに適用されます。

ステップ 4 [OK] をクリックします。

データおよび管理トラフィック用の DNS の設定

ドメイン ネーム システム（DNS）サーバーは、IP アドレスのホスト名の解決に使用されます。2 つの DNS サーバー設定があり、異なるタイプのトラフィック（データトラフィックと特別な管理トラフィック）に適用されます。データトラフィックには、アクセスコントロールルールやリモートアクセス VPN など、DNS ルックアップが必要な FQDN を使用するサービスが含ま

れます。特別な管理トラフィックには、スマートライセンスやデータベースの更新など、管理インターフェイスで発生するトラフィックが含まれます。

CLI セットアップウィザードを使用する場合、システムの初期設定で管理 DNS サーバーを設定します。Device Manager セットアップウィザードでデータおよび管理 DNS サーバーを設定することもできます。次の手順を使用して、DNS サーバーのデフォルトを変更できます。

configure network dns servers および **configure network dns searchdomains** コマンドを使用して、CLI で管理 DNS の設定を変更することもできます。データ インターフェイスおよび管理インターフェイスが同じ DNS グループを使用していて、そのグループが更新され次の展開段階にある場合、データ インターフェイスにも変更が適用されます。

DNS サーバー通信の正しいインターフェイスを決定するために、Threat Defense はルーティングルックアップを使用しますが、どのルーティングテーブルが使用されるかは、DNS をイネーブルにするインターフェイスによって異なります。詳細については、以下のインターフェイス設定を参照してください。

DNS 解決に関する問題が発生した場合は、次を参照してください。

- DNS の一般的な問題のトラブルシューティング （946 ページ）
- 管理インターフェイスの DNS のトラブルシューティング （1014 ページ）

始める前に

- DNS サーバグループを作成していることを確認します。この説明については、DNS グループの設定 （942 ページ） を参照してください。
- Threat Defense に、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあることを確認します。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）] > [DNSサーバー（DNS Server）]** リンクをクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、コンテンツテーブルの [DNSサーバー（DNS Server）] をクリックします。

ステップ 2 データインターフェイスの DNS を設定します。

a) すべてのインターフェイスまたは特定のインターフェイスで DNS ルックアップを有効にします。これらの選択は、使用されるルーティングテーブルにも影響します。

インターフェイスで DNS ルックアップを有効にすることは、ルックアップの送信元インターフェイスを指定することとは異なるので注意してください。デバイスは、常にルートルックアップを使用して送信元インターフェイスを決定します。

- [すべて（ANY）]（どのインターフェースも選択しない）：すべてのインターフェイスで、DNSルックアップを有効にします。デバイスはデータルーティングテーブルのみ。
- [Managementインターフェイスまたは管理専用インターフェイス以外の選択したインターフェイス（Interfaces selected but not the Diagnostic interface or a management）]：指定したインターフェイスでDNSルックアップを有効にします。デバイスはデータルーティングテーブルのみチェックします。
- [選択したインターフェイスとManagementインターフェイスまたは管理専用インターフェイス（Interfaces selected plus the Diagnostic interface or a management-only interface）]：指定したインターフェイスで DNS ルックアップを有効にします。デバイスはデータルーティングテーブルをチェックし、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックします。
- [選択されたManagementインターフェイスまたは管理専用インターフェイス（Only the Diagnostic interface or a management-only interface selected）]：Managementインターフェイスまたは管理専用インターフェイスで DNS ルックアップを有効にします。デバイスは管理専用ルーティングテーブルのみチェックします。

b) データ インターフェイスで使用するサーバを定義する [DNSグループ（DNS Group）] を選択します。グループが存在していない場合は、[DNSグループの新規作成（Create New DNS Group）]をクリックし、すぐに作成します。データインターフェイスでルックアップしないようにするには、[なし（None）] を選択します。

c) （オプション）アクセス制御ルールで FQDN ネットワーク オブジェクトを使用する場合は、[FQDN DNS設定（FQDN DNS Settings）] を設定します。

これらのオプションは、FQDN オブジェクトのみを解決する場合に使用されます。その他のタイプの DNS 解決では無視されます。

- [ポーリング時間（Poll Time）]：FQDN ネットワーク オブジェクトを IP アドレスに解決するために使用するポーリング サイクルの時間（分単位）。FQDN オブジェクトは、アクセス コントロール ポリシーで使用されてい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定されます。また、DNSエントリの存続可能時間（TTL）の値を使用しても、IP アドレス解決を更新するタイミングを決定できます。したがって、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可能性があります。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。
- [有効期限（Expiry）]：DNS エントリの期限が切れる（DNS サーバから取得した TTL が経過する）分数。この分数が経過すると、エントリは DNS ルックアップ テーブルから削除されます。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。

d) [保存（Save）] をクリックします。設定を展開して、デバイスに変更を適用する必要もあります。

ステップ 3 管理インターフェイスの DNS を設定します。

a) 管理インターフェイスで使用するサーバーを定義する [DNS グループ（DNS Group）] を選択します。グループが存在していない場合は、[DNSグループの新規作成（Create New DNS Group）] をクリックし、すぐに作成します。

b) [保存（Save）] をクリックします。管理DNSサーバーを更新するには、変更を展開する必要があります。

DNS の一般的な問題のトラブルシューティング

管理インターフェイスおよびデータインターフェイスに個別に DNS サーバを設定する必要があります。一部の機能では、両方ではなくどちらか片方のタイプのインターフェイスで名前解決を行います。所定の機能では、用途に応じて異なる解決方法を使用することもあります。

たとえば、**ping** *hostname* コマンドと**ping interface** *interface_name hostname* コマンドはデータインターフェイス DNS サーバを使用して名前解決を行い、**ping system** *hostname* コマンドは管理インターフェイスDNSサーバを使用します。これにより、特定のインターフェイスおよびルーティング テーブルを介した接続をテストできます。

ホスト名ルックアップに関する問題をトラブルシューティングする場合は、このことに留意してください。

管理インターフェイスの DNS をトラブルシューティングする場合は、管理インターフェイスの DNS のトラブルシューティング （1014 ページ）も参照してください。

名前解決しない場合

単純に名前解決が実行されない場合のトラブルシューティングに関するヒントは、次のとおりです。

- 管理インターフェイスとデータ インターフェイスの両方に DNS サーバを設定していることを確認します。データ インターフェイスでは、インターフェイスに [任意（Any）] を使用します。一部のインターフェイスで DNS を許可しない場合にのみ、インターフェイスを明示的に指定します。
- Managementインターフェイスまたは管理専用インターフェイスManagementインターフェイスを使用する場合は、そのインターフェイスのみが選択されていることを確認します。
- 各 DNS サーバの IP アドレスに ping を実行して、到達可能であることを確認します。**system** キーワードおよび **interface** キーワードを使用して、特定のインターフェイスをテストします。ping が失敗した場合は、スタティック ルートとゲートウェイを確認します。サーバのスタティック ルートを追加する必要がある場合があります。
- ping が成功して名前解決が失敗する場合は、アクセス制御ルールを確認します。サーバから到達可能なインターフェイスの DNS トラフィック（UDP/53）を許可していることを確

認します。このトラフィックは、システムと DNS サーバの間にあるデバイスによってブロックされる可能性もあるため、別の DNS サーバを使用する必要がある場合があります。

- ping が機能する場合は適切なルートが存在し、アクセス制御ルールに問題はありません。DNS サーバに FQDN のマッピングが存在しない可能性を考えます。別のサーバを使用する必要がある場合があります。

名前解決が正しくない場合

名前解決は実行されるが名前の IP アドレスが最新のものではない場合、キャッシュに問題がある可能性があります。この問題は、アクセス制御ルールで使用される FQDN ネットワーク オブジェクトなどのデータ インターフェイス ベースの機能にのみ影響します。

システムには、以前のルックアップで取得した DNS 情報のローカル キャッシュが存在します。新しいルックアップが要求されると、システムは最初にローカル キャッシュを調べます。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、DNS サーバに DNS クエリが送信されます。外部 DNS サーバ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。

各ルックアップには DNS サーバによって定義される存続可能時間値が設定されており、キャッシュからのルックアップは自動的に期限切れになります。また、システムはアクセス制御ルールで使用される FQDN の値を定期的に更新します。この更新は、少なくともポーリング間隔（デフォルトでは 4 時間ごと）で実行されますが、エントリの存続可能時間値に基づいて、より頻繁に実行できます。

show dns-hosts コマンドおよび **show dns** コマンドを使用して、ローカルキャッシュを確認します。FQDN の IP アドレスが正しくない場合は、**dns update** [**host** *hostname*] コマンドを使用して情報を強制的に更新できます。ホストを指定せずにコマンドを使用すると、すべてのホスト名が更新されます。

clear dns[**host** *fqdn*] コマンドおよび **clear dns-hosts cache** コマンドを使用して、キャッシュ情報を削除できます。

デバイスのホスト名の設定

デバイス ホスト名を変更できます。

また、CLI で **configure network hostname** コマンドを使用してホスト名を変更できます。

⚠

注意 ホスト名を使用してシステムに接続しているときにホスト名を変更すると、変更はただちに適用されるため、変更を保存するときに Device Manager へのアクセスが失われます。デバイスに接続し直す必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[ホスト名（Hostname）]** リンクの順にクリックします。

すでにシステム設定ページを開いている場合、目次の [ホスト名（Hostname）] をクリックします。

ステップ 2 新しいホスト名を入力します。

ステップ 3 [保存（Save）] をクリックします。

ホスト名の変更は、いくつかのシステムプロセスにすぐに適用されます。ただし、すべてのシステムプロセスで同じ名前が使用されるため、更新を完了するには変更を展開する必要があります。

Network Time Protocol（NTP）の設定

システムの時刻を定義するには、Network Time Protocol（NTP）サーバーを設定する必要があります。NTP サーバーはシステムの初期設定時に設定しますが、次の手順を使用して変更できます。NTP 通信に関する問題が発生した場合は、NTP のトラブルシューティング （1013 ページ）を参照してください。

Threat Defense デバイスは NTPv4 をサポートします。

（注） Firepower 4100/9300 の場合は、Device Manager を介して NTP を設定しません。FXOS で NTP を設定してください。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[タイムサービス（Time Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに表示している場合は、目次で [タイムサービス（Time Services）] をクリックします。

ステップ 2 [NTPタイムサーバー（NTP Time Server）] で、独自のタイム サーバーとシスコのタイム サーバーのどちらを使用するか選択します。

- **[デフォルトNTPサーバー（Default NTP Servers）]**：このオプションを選択すると、NTP に使用するサーバー名がサーバー リストに表示されます。

- **[ユーザー定義NTPサーバー（User-Defined NTP Servers）]**：このオプションを選択する場合は、使用する NTP サーバーの完全修飾ドメイン名か IPv4 または IPv6 アドレスを入力します。例、ntp1.example.com または 10.100.10.10。NTP サーバは最大 3 つまで追加できます。

ステップ 3 [保存（Save）] をクリックします。

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。

Threat Defense 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。Threat Defense 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。Threat Defense 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ときは、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 ドメインを設定した後、1 つの特定のドメインに PTP クロックを使用するように各非 PTP デバイスを設定できます。

始める前に

デバイスが使用する PTP クロックに設定されているドメイン番号を確認します。また、システムがドメイン内の PTP クロックに到達できるインターフェイスを決定します。

以下に、PTP の設定に関するガイドラインを示します。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- 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。
- 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、ルーテッド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 データ インターフェイスでサポートされます。管理インターフェイス、サブインターフェイス、Etherchannel、ブリッジ仮想インターフェイス（BVI）、またはその他の仮想インターフェイスではサポートされません。
- 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。PTP トラフィックは UDP 宛先ポート 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、このトラフィックを許可するアクセスコントロールルールはすべて動作します。
- ルーティングされたインターフェイス間で PTP パケットが転送される場合は、マルチキャストルーティングを有効にするとともに、各インターフェイスが 224.0.1.129 IGMP マルチキャストグループに参加する必要があります。同じブリッジグループ内のインターフェイス間で PTP パケットが転送される場合は、マルチキャストルーティングを有効にして IGMP グループを設定する必要はありません。

手順

ステップ 1 PTP クロック側インターフェイスの設定を確認します。

デフォルト設定では、すべてのインターフェイスが同じブリッジグループに配置されますが、ブリッジグループからインターフェイスを削除できます。マルチキャスト IGMP グループの場合とは異なる方法で設定する必要があるため、インターフェイスがルーテッドなのかブリッジグループメンバーなのかを決定することが重要です。

次の手順では、ブリッジグループに含まれているインターフェイスの確認方法について説明します。PTP 用に設定するインターフェイスがブリッジ グループ メンバーかどうかを確認します。

a) FDM で、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** の [すべてのインターフェイスを表示（View All Interfaces）] をクリックします。
b) リストでインターフェイスを検索し、[モード（Mode）]列を確認します。BridgeGroupMember はブリッジグループの一部であることを意味します。それ以外の場合はルーテッドです。

ステップ 2 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[タイムサービス（Time Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに表示している場合は、目次で [タイムサービス（Time Services）] をクリックします。

ステップ 3 PTP の設定を行います。

- [ドメイン番号（Domain Number）]: 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（0 ～ 255）。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。
- [クロックモード（Clock Mode）] : [エンドツーエンドトランスペアレント（End To End Transparent）] を選択します。デバイスを PTP トランスペアレントクロックとしてのみ動作させることができます。

  [転送（Forward）] を選択することもできますが、これは PTP を設定しない場合と基本的に同じです。ドメイン番号は無視されます。PTP パケットは、マルチキャストトラフィックのルーティングテーブルに基づいてデバイスを通過します。これは、デフォルトの PTP 設定です。

- [インターフェイス（Interface）]：システムがネットワーク内の PTP クロックに接続できるインターフェイスをすべて選択します。PTPは、これらのインターフェイスでのみ有効になります。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 選択したインターフェイスのいずれかがルーテッドモードである場合、つまりブリッジグループメンバーではない場合は、FlexConfig を使用してマルチキャストルーティングを有効にし、ルーテッドインターフェイスを正しい IGMP グループに参加させる必要があります。

選択したすべてのインターフェイスがブリッジグループメンバーである場合は、この手順を完了しないでください。ブリッジグループメンバーでIGMPを設定しようとすると、展開に失敗します。

a) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

b) 詳細設定の目次で **[FlexConfig]** > **[FlexConfig オブジェクト（FlexConfig Objects）]** をクリックします。

c) マルチキャストルーティングを有効にし、ルーテッドインターフェイスの IGMP 参加を設定するために、必要なオブジェクトを作成します。

次に、オブジェクトの基本テンプレートを示します。この例では、GigabitEthernet1/2 は、PTP を有効にするルーテッドインターフェイスの 1 つです。必要に応じてインターフェイスのハードウェア名を変更します。また、複数のルーテッドインターフェイスがある場合は、追加のインターフェイスごとに **interface** コマンドと **igmp** コマンドを繰り返します。

コマンド **igmp** では、224.0.1.129 IGMP グループに参加します。これは、ネットワークアドレスに関係なく、すべてのインターフェイスの正しい IP アドレスです。

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

ルーテッドインターフェイスのネゲートテンプレートは、次のようになります。

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) 目次の [FlexConfigポリシー（FlexConfig Policy）] をクリックして、FlexConfig ポリシーにこのオブジェクトを追加し、[保存（Save）] をクリックします。

プレビューに、オブジェクトからの期待されるコマンドが表示されていることを確認します。

次のタスク

変更を展開した後に、PTP の設定を確認できます。Device Manager CLI コンソール、または SSH またはコンソールセッションから、さまざまな **show ptp** コマンドを発行します。たとえ

ば、GigabitEthernet1/2 のみでドメイン 10 の PTP を設定している場合、出力は次のようになります。

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

管理接続用 HTTP プロキシの設定

システムとインターネットの間に直接接続がない場合は、管理インターフェイスの HTTP プロキシを設定できます。システムは、Device Manager への接続やデータベース更新をダウンロードするためのシステムからシスコへの接続など、すべての管理接続にプロキシを使用します。

また、Threat Defense CLI で **configure network http-proxy** コマンドを使用して、HTTP プロキシを設定することもできます。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[HTTPプロキシ（HTTP Proxy）]** リンクをクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、目次の [HTTPプロキシ（HTTP Proxy）] をクリックします。

ステップ 2 トグルをクリックしてプロキシを有効にしてから、プロキシ設定を指定します。

- [HTTPプロキシ（HTTP proxy）]：プロキシサーバーの IP アドレス。
- [Port（ポート）]：HTTP接続をリッスンするためにプロキシサーバーに設定するポート番号。
- [プロキシ認証を使用（Use Proxy Authentication）]：プロキシ接続に認証を要求するようサーバーが設定されている場合は、このオプションを選択します。このオプションを選択した場合は、プロキシサーバーにログインできるアカウントの[ユーザー名（Username）]と [パスワード（Password）] も入力します。

ステップ 3 [保存（Save）] をクリックし、変更を確定します。

変更はすぐに適用されます。展開ジョブは必要ありません。

システムの管理接続完了方法を変更しようとしているため、Device Manager への接続が失われます。変更が完了するまで数分待って、ブラウザウィンドウを更新してからもう一度ログインしてください。

クラウド サービスの設定

クラウドサービスに登録すると、CDO、Cisco Threat Response、Cisco Success Network など、さまざまなクラウドベースのアプリケーションを使用できます。

クラウドに登録すると、ページには登録ステータスとテナンシーのタイプ、およびデバイス登録で使用されたアカウント名が表示されます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

デバイスが登録されていない場合、このページに Cisco Cloud に登録するための登録方法が表示されます。クラウドに登録すると、個々のクラウドサービスを有効または無効にできます。

ステップ 2 （評価モードのとき、またはクラウドサービスからの登録解除後に）Cisco Cloud に登録するには、次のいずれかのオプションを選択します。

- [セキュリティ/CDOアカウント（Security/CDO Account）]：次のいずれかの方法を使用できます。
  - [Cisco Defense Orchestratorのテナンシーへの自動登録（Auto-enroll with Tenancy from Cisco Defense Orchestrator）]（Firepower 1000、2100、Cisco Secure Firewall 3100 のみ）。登録キーを取得する代わりに、自動登録を使用できます。最初に CDO に移動し、デ

バイスのシリアル番号を使用してデバイスを追加します。次に、Device Manager でこのチェックボックスをオンにして登録を開始します。デバイスのシャーシまたは梱包明細からシリアル番号を取得します。FXOS の場合は、FXOS CLI に移動して **show chassis detail** コマンドを実行することにより、シリアル番号（SN）というラベルが付いた正しいシリアル番号が表示されます。Threat Defense コマンドの **show serial-number** では異なるシリアル番号が表示されることに注意してください。これは CDO 登録には推奨されません。この方式は、CDO のレガシー デバイス マネージャ モードだけでなく、CDO のクラウド提供型 Management Center でも機能します。

（注） デバイスマネージャモードは、このモードを使用して Threat Defense をすでに管理している既存のユーザーのみが使用できます。

- CDO またはその他のセキュリティアカウントにログインし、登録キーを生成します。このページに戻り、[クラウドサービスのリージョン（Cloud Services Region）] を選択して、[登録キー（Registration Key）] に貼り付けます。この方式は、CDO のレガシー デバイス マネージャ モードでのみ機能します。CDO のクラウド提供型の管理センターについては、Device Manager から Management Center、または CDO への切り替え（960 ページ）を参照してください。

（注） デバイスマネージャモードは、このモードを使用して Threat Defense をすでに管理している既存のユーザーのみが使用できます。

この時点で、**Cisco Defense Orchestrator** と **Cisco Success Network** を有効にすることもできます。これらはデフォルトで有効になっています。

- [スマートライセンス（Smart License）]：（CDO を使用しない場合のみ）リンクをクリックして [スマートライセンシング（Smart Licensing）] ページに移動し、CSSM に登録します。CSSM に登録すると、デバイスがクラウドサービスにも登録されます。

（注） クラウドサービスから登録解除した場合、スマートライセンスの登録アプローチではいくつかの追加手順が必要です。この場合、[クラウドサービスのリージョン（Cloud Services Region）] を選択してから [登録（Register）] をクリックします。開示内容を読み、[承認（Accept）] をクリックします。

ステップ 3 クラウドサービスに登録したら、必要に応じて機能を有効または無効にできます。次のトピックを参照してください。

- CDO の有効化または無効化（レガシー デバイス マネージャ モード） （955 ページ）
- Cisco Success Network への接続 （955 ページ）
- Cisco Cloud へのイベントの送信 （957 ページ）
- クラウドサービスの登録解除 （958 ページ）

CDO の有効化または無効化（レガシー デバイス マネージャ モード）

（注） このセクションは、クラウド提供型の管理センターではなく、CDO のレガシー デバイス マネージャ モードにのみ適用されます。

クラウド サービスの設定 （953 ページ） の推奨に従い、CDO の登録キーを使用してクラウド サービスに登録した場合、デバイスはすでに CDO に登録されています。その後、必要に応じて接続を無効にしたり、再度有効にしたりできます。

デバイスがスマートライセンスを使用してクラウドサービスに登録されている場合、CDO を有効にすると問題が発生します。デバイスは CDO インベントリに表示されません。最初にクラウドサービスからデバイスの登録を解除しておくことを強くお勧めします。歯車（⚙）ドロップダウンリストから [クラウドサービスの登録解除（Unregister Cloud Services）] を選択します。登録解除後、「クラウドサービスの設定 （953ページ）」で説明されているとおりに、CDO から登録トークンを取得し、トークンとセキュリティアカウントを使用して再登録します。

クラウド管理の仕組みの詳細については、CDO ポータル（http://www.cisco.com/go/cdo）を参照するか、共に作業しているリセラーまたはパートナーにお問い合わせください。

始める前に

高可用性を設定する予定の場合、高可用性グループで使用する両方のデバイスを登録する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 必要に応じて、CDO 機能の [有効化（Enable）]/[無効化（Disable）] ボタンをクリックして設定を変更します。

Cisco Success Network への接続

デバイスを登録するときに、Cisco Success Network への接続を有効にするかどうかを決めます。デバイスの登録 （107 ページ） を参照してください。

Cisco Success Network を有効にすると、テクニカル サポートを提供するために不可欠な使用状況の情報と統計情報がシスコに提供されます。またこの情報により、シスコは製品を向上さ

せ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。

接続を有効にすると、デバイスが Cisco Cloud へのセキュアな接続を確立し、シスコから提供されているテクニカルサポートサービス、クラウド管理および監視サービスなどの追加サービスに参加できるようになります。お使いのデバイスは、いつでもこのセキュアな接続を確立して維持できます。クラウドから完全に切断する方法については、クラウドサービスの登録解除（958 ページ）を参照してください。

デバイスを登録した後で Cisco Success Network の設定を変更できます。

（注） システムがシスコにデータを送信する際に、タスク リストにテレメトリ ジョブが表示されます。

始める前に

Cisco Success Network を有効にするには、デバイスをクラウドに登録する必要があります。デバイスを登録するには、（[スマートライセンス（Smart Licensing）] ページで）Cisco Smart Software Manager にデバイスを登録し、登録中に [Cisco Success Network] オプションを選択するか、または登録キーを入力して CDO に登録します（CDO のレガシーデバイス マネージャ モードのみ）。

（注） 高可用性グループのアクティブ装置で Cisco Success Network を有効にする場合、スタンバイ装置での接続も有効にします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 必要に応じて Cisco Success Network 機能の [有効化（Enable）]/[無効化（Disable）] コントロールをクリックして設定を変更します。

[サンプルデータ（sample data）] リンクをクリックするとシスコに送信される情報の種類を確認できます。

接続を有効にする場合、情報開示を読み、[同意（Accept）] をクリックします。

Cisco Cloud へのイベントの送信

Cisco Cloud サーバーにイベントを送信できます。このサーバーから、各種のシスコ クラウド サービスがイベントにアクセスできます。次に、クラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。

クラウドツールは、送信したイベントを使用するかどうかを決定します。ツールのマニュアルを参照するかイベントデータを調べ、未使用のイベントをクラウドに送信して帯域幅とストレージ領域の両方を無駄にしていないことを確認します。ツールは同じソースからイベントを取り込むため、最も制限の厳しいツールだけでなく、使用するすべてのツールを選択する必要があります。次に例を示します。

- CDO のセキュリティ分析およびロギングツールは、すべての接続イベントを使用できます。
- Threat Response は優先順位の高い接続イベントのみを使用するため、すべての接続イベントをクラウドに送信する必要がありません。またこれは、セキュリティインテリジェンスの優先順位の高いイベントのみを使用します。

始める前に

このサービスを有効にするには、事前にクラウドサービスにデバイスを登録する必要があります。

米国地域では https://visibility.amp.cisco.com/ で、EU 地域では https://visibility.eu.amp.cisco.com で、APJC 地域では https://visibility.apjc.amp.cisco.com で、Threat Response に接続できます。アプリケーションの使い方と利点についての動画は、YouTube でご視聴いただけます（http://cs.co/CTRvideos）。詳細については、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html にある『*Cisco Secure Firewall Threat Defense and SecureX Threat Response Integration guide*』を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 必要に応じて **[Cisco Cloudにイベントを送信（Send Events to the Cisco Cloud）]** オプションの [有効化（Enable）]/[無効化（Disable）] コントロールをクリックして設定を変更します。

ステップ 3 サービスを有効にすると、クラウドに送信するイベントを選択するように求められます。後で、選択したイベントのリストの横にある [編集（Edit）] をクリックして、これらの選択を変更できます。送信するイベントのタイプを選択し、[OK] をクリックします。

- [ファイル/マルウェア（File/Malware）]：任意のアクセスコントロールルールで適用した任意のファイルポリシー用。

- [侵入（Intrusion）]：任意のアクセスコントロールルールで適用した任意の侵入ポリシー用。
- [接続（Connection）]：ロギングを有効にしたアクセスコントロールルール用。このオプションを選択すると、すべての接続イベントを送信するか、優先度の高い接続イベントのみを送信するかを選択することも可能です。優先度の高い接続イベントとは、侵入、ファイル、またはマルウェアイベントをトリガーする接続、またはセキュリティインテリジェンス ブロッキング ポリシーに一致する接続に関連するイベントです。

クラウドサービスの登録解除

クラウドサービスを使用しなくなった場合は、クラウドからそのデバイスの登録を解除できます。デバイスをサービスから削除する場合、またはサービスの使用を停止する場合、登録を解除する必要があります。クラウドサービスのリージョンを変更する必要がある場合は、登録を解除してから、再登録時に新しいリージョンを選択します。

この手順を使用してクラウドから登録を解除しても、スマートライセンシングの登録には影響しません。

手順

ステップ 1 [デバイス（Device）]をクリックしてから、**[システム設定（System Settings）]**>**[クラウドサービス（Cloud Services）]** リンクの順にクリックします。

[システム設定（System Settings）] ページがすでに表示されている場合は、目次で [クラウドサービス（Cloud Services）] をクリックします。

ステップ 2 歯車（⚙）のドロップダウンリストから、[クラウドサービスの登録解除（Unregister Cloud Services）] を選択します。

ステップ 3 警告を確認してから、[登録解除（Unregister）] をクリックします。

有効にしたクラウドサービスは自動的に無効になり、それらを再度有効にすることはできなくなります。ただし、クラウドに登録するためのコントロールが表示されるため、再登録は可能です。

Web 分析の有効化と無効化

Web分析を有効にすると、ページのヒット数に基づいて匿名の製品使用情報をシスコに提供できます。情報には、表示したページ、ページで費やした時間、ブラウザのバージョン、製品バージョン、デバイスのホスト名などが含まれます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブ データは送信されません。

Web 分析はデフォルトで有効になっています。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）]** > **[Web分析（Web Analytics）]** リンクをクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、目次の [Web分析（Web Analytics）] をクリックします。

ステップ 2 必要に応じて [Web分析（Web Analytics）] 機能の [有効化（Enable）]/[無効化（Disable）] コントロールをクリックして設定を変更します。

URL フィルタリングの設定

システムは Cisco Collective Security Intelligence（csi）（Cisco Talos Intelligence Group（Talos））から URL カテゴリおよびレピュテーションデータベースを取得します。これらの設定により、データベースの更新とシステムが不明なカテゴリまたはレピュテーションの URL を処理する方法が制御されます。これらの設定を行うには、URL フィルタリングライセンスを有効にする必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[URLフィルタリングの設定（URL Filtering Preferences）]** リンクの順にクリックします。

[システム設定（System Settings）] ページをすでに開いている場合、目次の [クラウドの基本設定（Cloud Preferences）] と [URLフィルタリングの基本設定（Filtering Preferences）] をクリックします。

ステップ 2 次のオプションを設定します。

- [自動更新の有効化（Enable Automatic Updates）]：カテゴリとレピュテーションを含む更新された URL データをチェックしてダウンロードすることをシステムに許可します。データは通常 1 日に 1 回更新されますが、システムは 30 分ごとに更新をチェックします。デフォルトでは、更新が有効になっています。このオプションを選択解除した状態でカテゴリとレピュテーションのフィルタリングを使用している場合、このオプションを周期的に有効にして新しい URL データを取得してください。
- [URLクエリソース（URL Query Source）]：URL のカテゴリとレピュテーションを取得するためにクエリを実行するソース。
  - [ローカルデータベースのみ（Local Database Only）]：ローカル URL フィルタリングデータベースでのみカテゴリとレピュテーションを検索します。一致するものがない

場合、URLはレピュテーションなしの未分類になります。この方式は、特にローエンドシステムにおいてストレージが限られているためにURLフィルタリングデータベースが小さい場合には、限定的なものになる可能性があります。

- [ローカルデータベースおよびCisco Cloud（Local Database and Cisco Cloud）]：これは推奨されるオプションです。ローカルデータベースに一致するものがない場合、更新されたカテゴリ/レピュテーション情報に関して Cisco Cloud に対するクエリが実行されます。規定された時間内に応答が受信された場合は、それが照合に使用されます。それ以外の場合、および一致するものがない場合、URLはレピュテーションなしの未分類になります。
- [Cisco Cloudのみ（Cisco Cloud Only）]：カテゴリおよびレピュテーション情報に関して、常に、Cisco Cloud に対するクエリが実行されます。ローカル URL データベースは使用されません。

- [URL存続可能時間（URL Time to Live）]（[未知のURL用Cisco CSIのクエリ（Query Cisco CSI for Unknown URLs）]を選択している場合にのみ利用可能）：指定された URL のカテゴリおよびレピュテーション ルックアップ値を保持する時間。存続可能時間が経過すると、次に試行される URL のアクセスが新規のカテゴリ/レピュテーション ルックアップになります。時間が短いほどURLフィルタリングが正確になり、時間が長いほど未知のURLに対するパフォーマンスが向上します。TTL は 2、4、8、12、24、または 48 時間、1 週間、または [使用しない（Never）]（デフォルト）に設定できます。

ステップ 3 必要に応じて、**URL のカテゴリを確認**できます。

特定の URL のカテゴリとレピュテーションを確認できます。[確認するURL（URL to Check）] ボックスに URL を入力し、[移動（Go）] をクリックします。結果を表示するには、外部の Webサイトに移動します。分類に同意しない場合は、[URLカテゴリの異議を送信する（Submit a URL Category Dispute）] リンクをクリックしてお知らせください。

ステップ 4 [保存（Save）] をクリックします。

Device Manager から Management Center、または CDO への切り替え

Device Manager から切り替える場合は、Threat Defense デバイスを Management Center または CDO に接続するように設定して管理できます。

（注） CDOは、クラウド提供型の管理センターを使用してThreat Defense デバイスを管理できます。CDOの簡素化されたデバイスマネージャ機能は、このモードでThreat Defense をすでに管理している既存のユーザーのみが使用できます。この手順は、クラウド提供型の管理センターにのみ適用されます。

Device Manager を使用して Management Center/CDO セットアップを実行すると、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、管理のために Management Center/CDO に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。Management Center/CDO の初期設定に Threat Defense CLI を使用する場合、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス設定は保持されません）。

Management Center/CDO に切り替えると、Device Manager を使用して Threat Defense デバイスを管理できなくなります。

始める前に

ファイアウォールが高可用性用に設定されている場合は、まず、Device Manager （可能な場合）または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから高可用性を中断することをお勧めします

手順

ステップ 1 Cisco Smart Software Manager にファイアウォールを登録した場合は、マネージャを切り替える前に登録を解除する必要があります。デバイスの登録解除（111ページ）を参照してください。

ファイアウォールを登録解除すると、基本ライセンスとすべての機能ライセンスが解放されます。ファイアウォールを登録解除しないと、それらのライセンスはCisco Smart Software Managerのファイアウォールに割り当てられたままになります。

ステップ 2 （必要に応じて）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の設定 （300ページ）を参照してください。

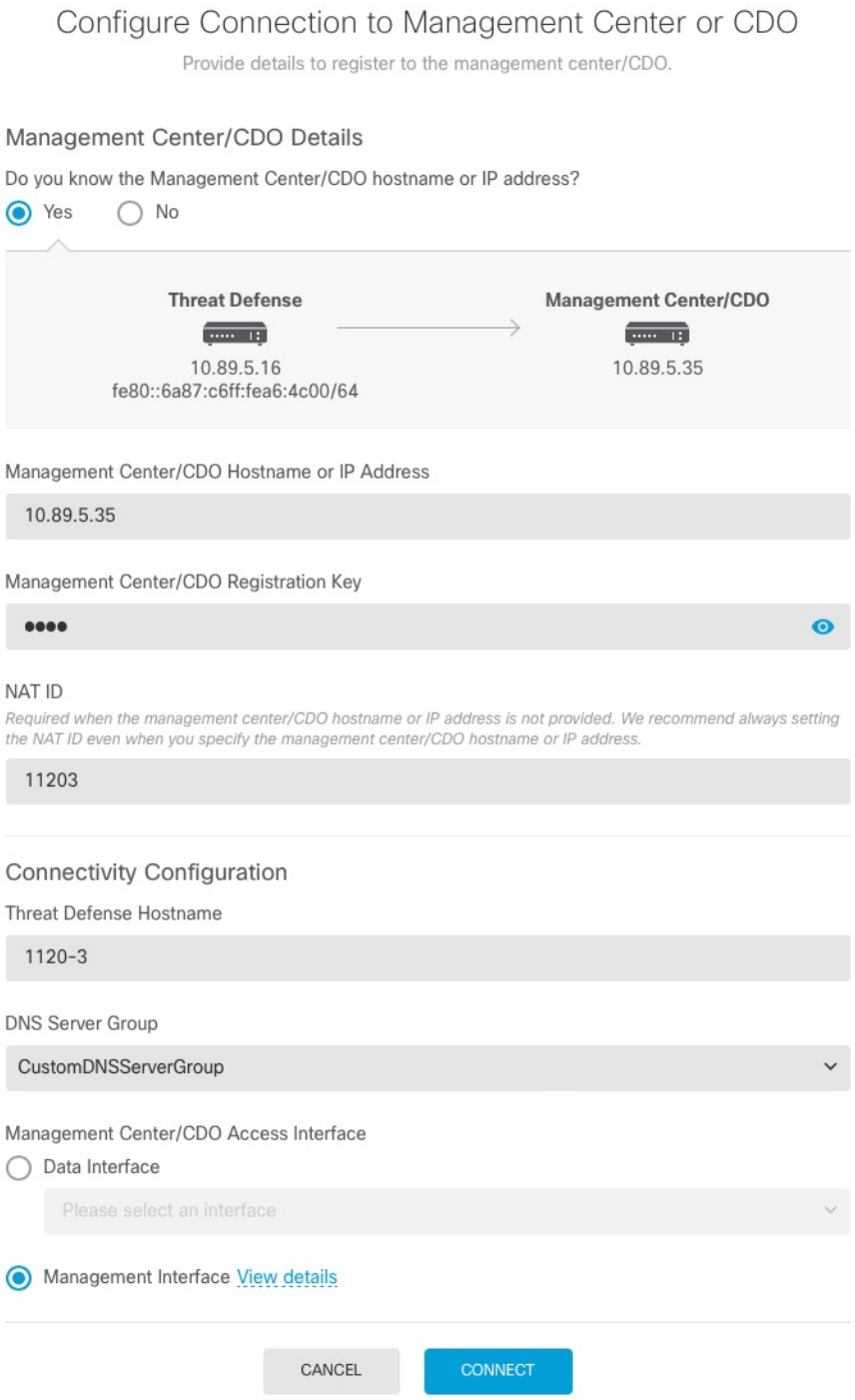
マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Device Manager 接続に管理インターフェイスを使用していた場合は、Device Manager に再接続する必要があります。

- マネージャアクセス用のデータインターフェイス：管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCPからゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

ステップ 3 **[デバイス（Device）] > [システム設定（Device System Settings）] > [中央管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Management Center/CDO の管理を設定します。

ステップ 4 **[Management Center/CDOの詳細（Management Center/CDO Details）]** を設定します。

図 *52 : Management Center/CDO* の詳細



a) **[Management Center/CDOのホスト名またはIPアドレスを知っていますか（Do you know the FMC hostname or IP address）]** で、IP アドレスまたはホスト名を使用して Management Center/CDO に到達できる場合は [はい（Yes）] をクリックし、Management Center/CDO が NAT の背後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ（No）] をクリックします。

双方向の TLS-1.3 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Management Center/CDO または Threat Defense デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。

c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するときに Management Center/CDO でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center/CDO に登録する複数のデバイスに使用できます。

d) [NAT ID] を指定します。

この ID は、Management Center/CDO でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center/CDO に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 5 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

Management Center/CDO アクセスインターフェイスのアクセスにデータインターフェイスを使用する場合、この FQDN がこのインターフェイスに使用されます。

b) [DNSサーバーグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

Management Center/CDO アクセスインターフェイスにデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同じ DNS サーバーグループを選択する可能性があります。

Management Center/CDO では、この Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center/CDO に Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense デバイスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center/CDO と Threat Defense デバイスを同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center/CDO で保持されます。

Management Center/CDO アクセスインターフェイスに管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを構成します。

c) **Management Center/CDO アクセスインターフェイス**については、任意の構成済みインターフェイスを選択してください。

管理インターフェイスは、Threat Defense デバイスを Management Center/CDO に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

ステップ 6 （任意）外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center/CDO に接続する前にデフォルトルートを手動で設定する必要があります。スタティックルートの設定の詳細については、「スタティック ルートの設定 （396 ページ）」を参照してください。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意のゲートウェイとして設定する必要があります。管理インターフェイスの設定 （300 ページ）を参照してください。

ステップ 7 （任意） データインターフェイスを選択した場合は、[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、 IP アドレスが変更された場合に Management Center/CDO が完全修飾ドメイン名（FQDN）で Threat Defense デバイスに到達できるようにします。[デバイス（Device）] > [システム設定（System Settings）] > [DDNSサービス（DDNS Service）] を参照して DDNS を設定します。

Management Center/CDO に Threat Defense デバイスを追加する前に DDNS を設定すると、Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加し、Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。 Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

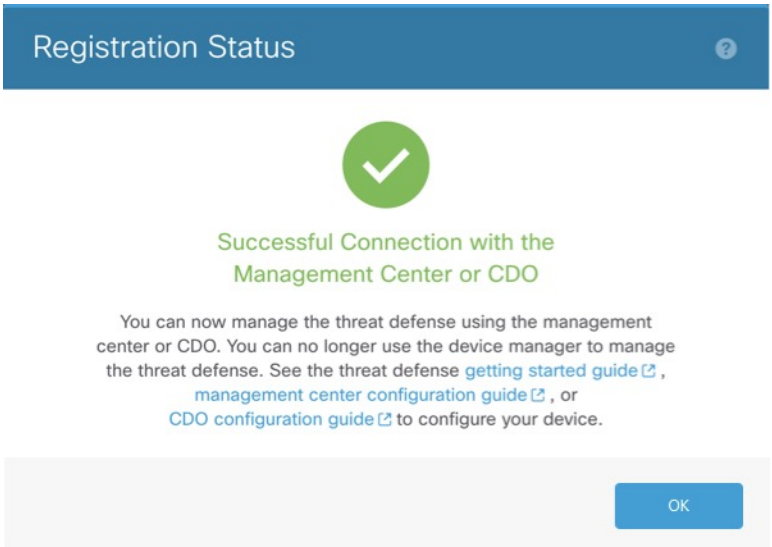
マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

ステップ 8 [接続（Connect）] をクリックします。**[登録ステータス（Registration Status）]** ダイアログボックスには、Management Center/CDO への切り替えに関する現在のステータスが表示されます。**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップの後、Management Center/CDO に移動してファイアウォールを追加します。

Management Center/CDO への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] のステップの後に Device Manager に接続したままにする場合、その後 **[Management CenterまたはCDOとの正常接続（Successful Connection with Management Center or CDO）]** ダイアログボックスが表示され、Device Manager から切断されます。

図 *53* : 正常接続



Management Center または CDO から Device Manager に切り替える

代わりにDevice Managerを使用するように、オンプレミスまたはクラウド提供型のManagement Centerによって現在管理されている Threat Defense デバイスを設定できます。

ソフトウェアを再インストールすることなく、Management CenterからDevice Managerに切り替えることができます。Management CenterからDevice Managerに切り替える前に、Device Managerがすべての設定要件を満たしていることを確認します。Device Manager から Management Centerに切り替える場合は、Device Manager から Management Center、または CDO への切り替え（960 ページ） を参照してください。

注意 Device Manager に切り替えると、デバイスの設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は維持されます。

手順

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] ページからファイアウォールを削除します。

ステップ 2 SSH またはコンソールポートを使用して、Threat Defense CLI に接続します。SSH の場合、管理 IP アドレスへの接続を開き、admin ユーザー名（または管理者権限を持つ他のユーザー）で Threat Defense CLI にログインします。

（Firepower モデル）コンソールポートはデフォルトで FXOS CLI になります。**connect ftd** コマンドを使用して、Threat Defense CLI に接続します。SSH セッションは Threat Defense CLI に直接接続します。

管理 IP アドレスに接続できない場合は、次のいずれかを実行します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理 IP アドレスとゲートウェイが設定されていることを確認します。**configure network ipv4/ipv6 manual** コマンドを使用します。

ステップ 3 現在リモート管理モードになっていることを確認します。

show managers

例：

```
> show managers
Type                       : Manager
Host                       : 10.89.5.35
Display name               : 10.89.5.35
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
```

ステップ 4 リモート マネージャを削除すると、マネージャなしのモードになります。

configure manager delete *uuid*

リモート管理からローカル管理に直接移行することはできません。複数のマネージャが定義されている場合は、識別子（UUID とも呼ばれます。**show managers** コマンドを参照）を指定する必要があります。各マネージャ エントリを個別に削除します。

例：

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 5 ローカル マネージャを設定します。

configure manager local

これで、Web ブラウザで **https://***management-IP-address* にアクセスしてローカル マネージャを開くことができるようになりました。

例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

TLS/SSL 暗号設定の設定

SSL 暗号設定は、デバイスへの TLS/SSL 接続に許可される TLS バージョンと暗号化暗号スイートを制御します。具体的には、これらの設定は、リモートアクセス VPN 接続を確立するときにクライアントが使用できる暗号を制御します。

通常、設定する暗号スイートには、使用可能な複数の暗号化暗号スイートが必要です。システムは、クライアントと Threat Defense デバイスの両方がサポートする最高の TLS バージョンを決定し、その TLS バージョンと互換性のある両方をサポートする暗号スイートを選択します。システムは、両方のエンドポイントでサポートされている最も強力な TLS バージョンと暗号スイートを選択して、許可する暗号の中で最も安全な接続を確保します。

始める前に

デフォルトでは、システムは DefaultSSLCipher オブジェクトを使用して、許可される暗号スイートを定義します。このオブジェクトに含まれる暗号は、スマート ライセンス アカウントが輸出規制機能に対して有効になっているかどうかによって異なります。このデフォルトでは、できるだけ多くのクライアントが接続を完了できるように、低セキュリティ レベルが設定されます。デフォルトの Diffie-Hellman グループもあります。これらの設定は、デフォルトが要件に適合しない場合にのみ設定する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[システム設定（System Settings）] > [SSL設定（SSL Settings）]** リンクの順にクリックします。

ステップ 2 次のオプションを設定します。

- [暗号（Ciphers）]：許可されるTLSバージョンと暗号化アルゴリズムを定義するSSL暗号オブジェクトを選択します。DefaultSSLCipher オブジェクトでは、低セキュリティレベルが設定されます。このオブジェクトをCiscoRecommendedCipher、または独自のカスタム暗号オブジェクトに置き換えて、より高い要件を実装します。理想的には、すべておよび許可する TLS バージョンと暗号のみを含む単一のオブジェクトを作成します。

  オブジェクトを今すぐ作成する必要がある場合は、リストの下部にある [新しい暗号の作成（Create New Cipher）] をクリックします。

- [一時的なDiffie-Hellmanグループ（Ephemeral Diffie-Hellman Group）]：一時的な暗号化アルゴリズムに使用する DH グループ。DH グループの説明については、使用する Diffie-Hellman 係数グループの決定 （783 ページ）を参照してください。デフォルトは 14 です。

- [楕円曲線DHグループ（Elliptical Curve DH Group）]：楕円曲線暗号化アルゴリズムに使用する DH グループ。デフォルトは 19 です。

ステップ 3 [保存（Save）] をクリックします。

TLS/SSL 暗号オブジェクトの設定

SSL 暗号オブジェクトでは、Threat Defense デバイスへの SSL 接続を確立するときに使用できるセキュリティレベル、TLS/DTLS プロトコルバージョン、および暗号化アルゴリズムの組み合わせを定義します。ボックスへのSSL接続を確立するユーザーのセキュリティ要件を定義するには、**[デバイス（Device）] > [システム設定（System Settings）] > [SSL設定（SSL Settings）]** で次のオブジェクトを使用します。

選択できる TLS のバージョンと暗号は、スマート ライセンス アカウントによって制御されます。輸出コンプライアンス要件を満たしている場合は、オプションの任意の組み合わせを選択できます。ライセンスが輸出要件に準拠していない場合は、TLSv1.0 および DES-CDC-SHA に制限されます。これらは最も低いセキュリティオプションです。評価モードは非準拠モードと見なされるため、システムのライセンスを取得するまではオプションが制限されます。

システムには、事前定義されたオブジェクトがいくつか含まれています。事前定義されたオブジェクトがセキュリティ要件に適合しない場合にのみ、新しいオブジェクトを作成する必要があります。オブジェクトは次のとおりです。

- DefaultSSLCipher：これは低セキュリティレベルのグループです。これは、できるだけ多くのクライアントがシステムへの接続を完了できるようにするために、SSL設定で使用さ

れるデフォルトです。システムでサポートされるすべてのプロトコルバージョンと暗号が含まれます。

- CiscoRecommendedCipher：これは、最も安全な暗号と TLS バージョンのみを含む、高セキュリティレベルのグループです。このグループは最高のセキュリティを提供しますが、各クライアントが一致する暗号を使用できるようにする必要があります。暗号の不一致の問題によって、一部のクライアントが接続を完了できない可能性が高くなります。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [SSL暗号（SSL Ciphers）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 次のオプションを設定します。

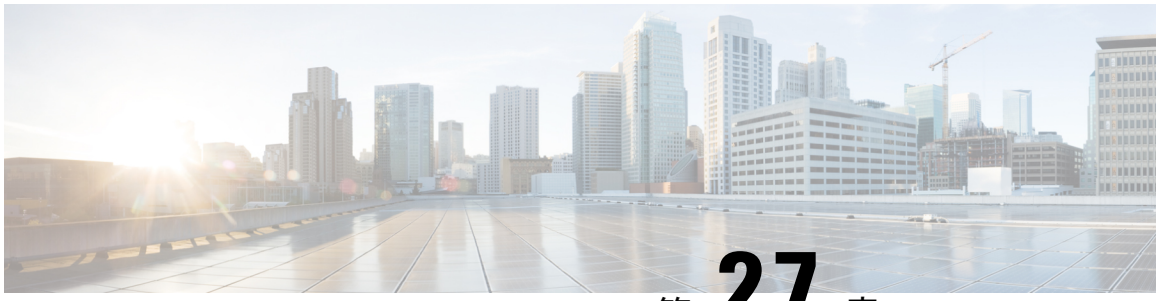
- [セキュリティレベル（Security Level）]：オブジェクトの相対的なセキュリティレベル。セキュリティレベルを選択した後にプロトコルバージョンまたは暗号スイートリストを編集すると、オブジェクトによって提供される実際のセキュリティレベルが選択したセキュリティレベルと一致しない場合があることに注意してください。次のいずれかを実行します。
  - [すべて（All）]：低セキュリティから高セキュリティまで、すべての TLS レベルと暗号スイートをオブジェクトに含めます。
  - [低（Low）]：すべての TLS バージョンと暗号が含まれます。この場合、ユーザーは最も安全性の低い暗号で接続を完了できます。非輸出準拠ライセンスの場合は、TLSv1.0 および DES-CBC-SHA が含まれます。
  - [中（Medium）]：すべての TLS バージョンが含まれますが、一部の比較的安全でない暗号は削除されます。このオプションと [低（Low）] および [すべて（All）] オプションの違いはごくわずかです。このオプションは、非輸出準拠ライセンスでは使用できません。
  - [高（High）]：最新の DTLS および TLS バージョンのみ、およびこれらのバージョンで動作する暗号を許可します。このオプションは、現在使用可能な最も安全な暗号に接続を制限します。このオプションは、非輸出準拠ライセンスでは使用できません。
  - [カスタム（Custom）]：TLS バージョンと暗号を個別に選択する場合は、このオプションを選択します。選択するオプションによって、定義するセキュリティ暗号化設定の高低が決まります。カスタムオブジェクトにはデフォルトはありませんが、[カ

スタム（Custom）] を選択する前に別のレベルを選択した場合は、前に表示されたオプションが選択したままになります。

- [プロトコルバージョン（Protocol Versions）]：クライアントが Threat Defense デバイスへの TLS/SSL 接続を確立するときに使用できる TLS/DTLS バージョン。カスタムオブジェクトの場合は、サポートするバージョンを選択します。他のセキュリティレベルの場合は、リストを編集しないことが理想的ですが、必要に応じてバージョンを追加または削除できます。
- [使用可能な暗号スイート（Applicable Cipher Suites）]：クライアントが使用できる暗号化アルゴリズム。新しいスイートを追加する場合は [+] をクリックします。スイートを削除する場合はそのスイートの [x] をクリックします。

  選択したプロトコルバージョンによって、このリストで使用可能なスイートが制御されます。プロトコルバージョンを変更すると、選択したバージョンで動作しなくなった選択済みのスイートにフラグが付けられます。それらのスイートは削除するか、必要なプロトコルバージョンを再度追加する必要があります。

ステップ 5 [OK] をクリックします。



第 27 章

システム管理

ここでは、システムデータベースの更新やシステムのバックアップおよび復元などの、システム管理タスクの実行方法について説明します。

ソフトウェア アップデートのインストール

システム データベースとシステム ソフトウェアの更新プログラムをインストールできます。ここでは、これらの更新プログラムのインストール方法について説明します。

システム データベースおよびフィードの更新

システムは、複数のデータベースおよびセキュリティ インテリジェンス フィードを使用して高度なサービスを提供します。シスコでは、セキュリティ ポリシーで最新の情報が使用されるよう、これらのデータベースおよびフィードに対する更新を提供しています。

システム データベースおよびフィードの更新の概要

Threat Defense は次のデータベースおよびフィードを使用して高度なサービスを提供します。

侵入ルール

新たな脆弱性が既知になると、Cisco Talos Intelligence Group（Talos） はユーザーがインポート可能な侵入ルールの更新をリリースします。それらの更新は、侵入ルール、プリプロセッサ ルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルールカテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。

侵入ルールの更新によって行われた変更を有効にするには、設定を再展開する必要があります。

侵入ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに実行してください。低速ネットワークでは、更新の試行が失敗し、再試行が必要になることがあります。

位置情報データベース（GeoDB）

シスコの地理位置情報データベース（GeoDB）は、ルーティング可能な IP アドレスに関連する地理情報データ（国、都市、緯度と経度など）のデータベースです。

GeoDB の更新には、検出されたルーティング可能な IP アドレスにシステムが関連付けることが可能な物理的な場所に関する更新情報が含まれています。位置情報データは、アクセス コントロール ルールとして使用できます。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30 ～ 40 分かかります。GeoDB の更新は他のシステムの機能（実行中の地理情報の収集など）を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

脆弱性データベース（VDB）

シスコの脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。ファイアウォールシステムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。Cisco Talos Intelligence Group（Talos） では、VDB の定期的な更新を配布しています。

脆弱性のマッピングを更新するのにかかる時間は、ネットワーク マップ内のホストの数によって異なります。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、更新されたアプリケーション ディテクタとオペレーティング システム フィンガープリントを有効にするために、設定を再展開する必要があります。

Cisco Talos Intelligence Group（Talos） セキュリティ インテリジェンスのフィード

Talos は、セキュリティ インテリジェンス ポリシーで使用するため定期的に更新されるインテリジェンスフィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。これらのフィードには、既知の脅威のアドレスや URL が含まれています。システムによって

フィードが更新される場合、再展開する必要はありません。後続の接続の評価には新しい一覧が使用されます。

URL カテゴリ/レピュテーション データベース

システムは、Cisco Collective Security Intelligence（CSI）から URL カテゴリとレピュテーションデータベースを取得します。カテゴリとレピュテーションに関してフィルタリングする URL フィルタリング アクセス制御ルールを設定すると、要求された URL がデータベースと照合されます。**[システム設定（System Settings）]** > **[URLフィルタリングの設定（URL Filtering Preferences）]** でデータベースの更新といくつかのその他の URL フィルタリング設定を設定できます。URL カテゴリ/レピュテーション データベースの更新は、他のシステム データベースの更新を管理する方法では管理できません。

システム データベースの更新

必要に応じて、手動でシステムデータベースの更新を取得して適用できます。更新はシスコサポートサイトから取得されます。そのため、システムの管理アドレスからインターネットへのパスが必要です。

または、インターネットから更新パッケージを取得して、ワークステーションからアップロードできます。この方法は、主に、シスコから更新を取得するためのインターネットへのパスがないエアギャップネットワークを対象としています。software.cisco.com のシステム ソフトウェア アップグレードをダウンロードするのと同じフォルダから更新をダウンロードします。

（注） 2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。Device Manager は IP パッケージの情報を使用しません。また、これまでに使用したこともありません。この分割により、ローカルで管理された Threat Defense 展開においてディスク容量が大幅に節約されます。シスコからご自身で GeoDB を入手する場合は、古いオールインワンパッケージと同じファイル名を持つ国コードパッケージ（Cisco_GEODB_Update-*date-build*）を入手してください。

またデータベースの更新を取得して適用するよう、定期的なスケジュールを設定することもできます。これらの更新はサイズが大きい場合があるため、ネットワークアクティビティが少ない時間帯にスケジュールしてください。

（注） データベース更新が進行中の場合、ユーザーインターフェイスのアクションへの応答が遅くなる場合があります。

始める前に

保留中の変更に対して潜在的な影響を与えることを避けるため、これらのデータベースを手動で更新する前に、デバイスに設定を展開します。

VDB および URL カテゴリを更新すると、アプリケーションまたはカテゴリが削除される可能性があることに注意してください。変更を展開する前に、これらの廃止された項目を使用しているアクセス制御ルールまたは SSL 復号ルールを更新する必要があります。

手順

ステップ 1 [デバイス（Device）]をクリックしてから、[更新（Updates）]のサマリーで[設定の表示（View Configuration）] をクリックします。

これによって、[更新（Updates）]ページが開きます。このページの情報には、各データベースの現在のバージョン、および各データベースの最終更新日時が表示されます。

ステップ 2 データベースを手動で更新するには、そのデータベースのセクションで次のいずれかのオプションをクリックします。

- [クラウドから更新（Update From Cloud）]：Device Manager が更新パッケージをシスコから取得するようにします。これは最も簡単で信頼性の高い方法ですが、使用するにはインターネットへのパスが必要です。
- **（下矢印）** > ***[オプション（option）]***：ワークステーションまたはワークステーションに接続されているドライブから更新パッケージを選択します。オプションは次のいずれかです。
  - [ファイルの選択（Select File）]：VDB または地理位置情報パッケージを選択します。
  - [新しいバージョンに更新（Update to Newer Version）]：現在インストールされている侵入ルールパッケージよりも新しいパッケージを選択します。
  - [古いバージョンにダウングレード（Downgrade to Older Version）]：現在インストールされている侵入ルールパッケージよりも古いパッケージを選択します。

ルールおよび VDB の更新では、アクティブにするための設定の展開が必要です。クラウドから更新する場合、今すぐ展開するかどうかを尋ねられるので、[はい（Yes）] をクリックします。[いいえ（No）]をクリックする場合は、都合の良いときにできるだけ早く展開ジョブを開始してください。

独自のファイルをアップロードする場合は、必ず手動で変更を展開する必要があります。

（注） 侵入ルールパッケージを手動でアップロードする場合は、必ず Snort のバージョンに適したパッケージタイプ（Snort 2 の場合は SRU、Snort 3 の場合は LSP）をアップロードしてください。非アクティブなバージョンの Snort 用のパッケージもアップロードできますが、バージョンを切り替えるまでアクティブになりません。Snort のバージョンの切り替えについては、Snort 2 と Snort 3 の切り替え （647 ページ）を参照してください。

ステップ 3 （オプション）定期的なデータベース更新スケジュールを設定するには、次の手順に従います。

a) 目的のデータベースのセクションで[設定（Configure）]リンクをクリックします。すでにスケジュールが設定されている場合、[編集（Edit）] をクリックします。

データベースの更新スケジュールは独立しています。スケジュールは別途定義する必要があります。

b) 更新開始時刻を設定します。

- 更新の頻度（日次、週次、または月次）。
- 週次または月次の場合、更新が必要な曜日または日付。
- 更新を開始する時刻。指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

c) ルールまたは VDB の更新では、データベースが更新されるたびにシステムが設定を展開するようにする場合は、[更新の自動展開（Automatically Deploy the Update）]チェックボックスをオンにします。

更新は、展開されるまでは有効になりません。自動展開では、まだ展開されていないその他の設定変更も展開されます。

d) [保存（Save）] をクリックします。

（注） 定期的なスケジュールを削除する場合、[編集（Edit）] リンクをクリックしてスケジューリング ダイアログボックスを開き、[削除（Remove）] ボタンをクリックします。

Cisco Security Intelligence フィードの更新

Cisco Talos Intelligence Group（Talos）は、定期的に更新されるセキュリティ インテリジェンス フィードへのアクセスを提供します。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。システムによってフィードが更新される場合、再展開する必要はありません。後続の接続の評価には新しい一覧が使用されます。

システムがフィードをインターネットから更新するタイミングを厳密に制御したい場合は、そのフィードの自動更新を無効にできます。ただし、自動更新を行えば、最新の関連するデータであることが確実になります。

手順

ステップ 1 [デバイス（Device）]をクリックしてから、[更新（Updates）]のサマリーで[設定の表示（View Configuration）] をクリックします。

これによって、[更新（Updates）]ページが開きます。ページには、[セキュリティインテリジェンスフィード（Security Intelligence Feeds）] の現在のバージョン、およびフィードの最終更新日時が表示されます。

ステップ 2 フィードを手動で更新するには、[セキュリティインテリジェンスフィード（Security Intelligence Feeds）] グループで [今すぐ更新（Update Now）] をクリックします。

ハイ アベイラビリティ グループ内の 1 台の装置のフィードを手動で更新する場合は、その他の装置のフィードも手動で更新して一貫性を確保する必要があります。

ステップ 3 （オプション）定期的な更新の頻度を設定するには：

a) [シスコのフィード（Cisco Feeds）] セクションにある [設定（Configure）] リンクをクリックします。すでにスケジュールが設定されている場合、[編集（Edit）]をクリックします。

b) 希望する頻度を選択します。

デフォルトは [毎時（Hourly）] です。[毎日（Daily）] 更新（時刻を指定）または [毎週（Weekly）] 更新（曜日と時刻を指定）を設定することもできます。 指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

[削除（Delete）] をクリックして、自動更新されないようにします。

c) [OK] をクリックします。

のアップグレードThreat Defense

この手順を使用して、スタンドアロンの Threat Defense デバイスをアップグレードします。FXOS を更新する必要がある場合は、それを最初に実行します。高可用性脅威防御をアップグレードするには、ハイアベイラビリティ Threat Defense のアップグレード （270 ページ）を参照してください。

⚠

注意 アップグレード中にトラフィックがドロップされます。システムが非アクティブまたは無反応に見えても、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。失敗した（または進行中）のメジャーおよびメンテナンスアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。問題が解消されない場合は、Cisco TAC にお問い合わせください。

アップグレード中に発生する可能性のあるこれらの問題およびその他の問題の詳細については、Threat Defense のアップグレードのトラブルシューティング （981 ページ）を参照してください。

始める前に

事前アップグレードのチェックリストを完了します。正常に展開され、通信が確立されていることを確認します。

ヒント　アップグレード前のチェックリストには、計画（Cisco Secure Firewall Threat Defense リリースノートを読むことから開始）、バックアップの作成、アップグレードパッケージの取得、および関連するアップグレード（Firepower 4100/9300 の FXOS など）の実行が含まれます。また、必要な構成変更のチェック、準備状況のチェック、ディスク容量のチェック、実行中のタスクとスケジュールされたタスクの両方のチェックも含まれます。アップグレード手順の詳細については、アップグレード前のチェックリストを含め、お使いのバージョンの『Device Manager 用 Cisco Secure Firewall Threat Defense アップグレードガイド』を参照してください。

手順

ステップ 1　[デバイス（Device）] を選択し、[更新（Updates）] パネルの [設定の表示（View Configuration）] をクリックします。
[システムアップグレード（System Upgrade）] パネルには、現在実行中のソフトウェアバージョン、およびすでにアップロードされたアップグレードパッケージが表示されます。

ステップ 2　アップグレードパッケージをアップロードします。

アップロードできるパッケージは 1 つだけです。新しいパッケージをアップロードすると、古いパッケージが置き換えられます。ターゲットバージョンとデバイスモデルに適したパッケージがあることを確認してください。[参照（Browse）] または **[ファイルの置き換え（Replace File）]** をクリックしてアップロードを開始します。

アップロードが完了すると、確認ダイアログボックスが表示されます。[OK] をクリックする前に、必要に応じて [すぐにアップグレードを実行（Run Upgrade Immediately）] を選択して、ロールバックオプションを選択し、今すぐアップグレードします。今すぐアップグレードする場合は、アップグレード前のチェックリストをできるだけ多く完了することが特に重要です（次のステップを参照）。

ステップ 3　準備状況チェックを含む、アップグレード前の最終チェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。準備状況チェックを手動で実行しない場合、アップグレードの開始時に実行されます。準備状況チェックに失敗すると、アップグレードはキャンセルされます。詳細については、アップグレード準備状況チェックの実行 （978 ページ）を参照してください。

ステップ 4　**[今すぐアップグレード（Upgrade Now）]** をクリックしてアップグレードを開始します。

a)　ロールバックオプションを選択します。

[アップグレードに失敗すると自動的にキャンセルされ、前のバージョンにロールバックする（Automatically cancel on upgrade failure and roll back to the previous version）] を選択できます。オプションを有効にすると、メジャーまたはメンテナンスアップグレードが失敗し

た場合、デバイスは自動的にアップグレード前の状態に戻ります。失敗したアップグレードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。

b) [続行（Continue）] をクリックして、アップグレードしてデバイスを再起動します。

自動的にログオフされ、デバイスが再起動するまでアップグレードを監視できるステータスページに移動します。また、このページには、進行中のインストールをキャンセルするオプションが含まれています。自動ロールバックを無効にしてアップグレードが失敗した場合は、アップグレードを手動でキャンセルするか、再試行できます。

アップグレード中にトラフィックがドロップされます。ISA 3000 の場合にのみ、電源障害に対するハードウェアバイパスを設定すると、トラフィックはアップグレード中にドロップされますが、デバイスのアップグレード後の再起動完了時に検査なしでトラフィックが渡されます。

ステップ 5 可能なときに再度ログインし、アップグレードが成功したことを確認します。

[デバイスの概要（Device Summary）] ページには、現在実行中のソフトウェアのバージョンが表示されます。

ステップ 6 アップグレード後のタスクを完了します。

a) システムデータベースを更新します。侵入ルール、VDB、GeoDB の自動更新が設定されていない場合は、ここで更新します。
b) アップグレード後に必要な構成変更が他にもあれば、実行します。
c) 展開します。

アップグレード準備状況チェックの実行

アップグレードパッケージがインストールされる前に、準備状況チェックが実行されて、システムに有効なアップグレードであるか確認されます。また、他にもアップグレードの成功を妨げる可能性のある項目がないかチェックされます。準備状況チェックに失敗した場合は、インストールを再試行する前に問題を修正する必要があります。チェックに失敗した場合、次回インストールを試みると、チェック失敗についてのプロンプトが表示され、強制的にインストールを実行するオプションが与えられます。

次の手順の説明に従って、アップグレードを開始する前に手動で準備状況チェックを実行することもできます。

始める前に

チェックするアップグレードパッケージをアップロードします。

手順

ステップ 1 [デバイス（Device）] をクリックし、[更新サマリー（Updates summary）] の [設定の表示（View Configuration）] をクリックします。

[システムアップグレード（System Upgrade）] セクションには、現在実行中のソフトウェアバージョン、およびすでにアップロードされた更新が表示されます。

ステップ 2 [Readiness Check] セクションを確認します。

- アップグレードチェックがまだ実行されていない場合は、[Run Upgrade Readiness Check] リンクをクリックします。チェックの進行状況がこの領域に表示されます。プロセスの完了には、20 秒程度かかります。
- アップグレードチェックがすでに実行されている場合、このセクションにはチェックが成功か失敗かが示されます。チェックに失敗した場合は、[See Details] をクリックして、準備状況チェックの詳細を表示します。問題を修正した後、チェックを再度実行します。

ステップ 3 準備状況チェックに失敗した場合は、アップグレードパッケージをインストールする前に問題を解決する必要があります。詳細情報には、指摘された問題の修正方法に関するヘルプが含まれています。失敗したスクリプトについては、[Show Recovery Message] リンクをクリックすると情報が表示されます。

一般的な問題のいくつかを以下に示します。

- FXOS バージョンに互換性がない：FXOS アップグレードを個別にインストールする Firepower 4100/9300 などのシステムでは、現行の Threat Defense ソフトウェアバージョンとは異なる FXOS の最小バージョンが必要になる場合があります。この場合、Threat Defense ソフトウェアをアップグレードする前に、まず FXOS をアップグレードする必要があります。
- デバイスモデルがサポートされていない：アップグレードパッケージは、サポートされていないデバイスにはインストールできません。誤ったパッケージをアップロードしたか、デバイスが旧モデルのため、新しい Threat Defense ソフトウェアバージョンではサポートされていない可能性があります。デバイスの互換性を確認し、サポートされているパッケージがあればアップロードしてください。
- ディスク容量が不十分：十分な空き容量がない場合は、システムバックアップなどの不要なファイルを削除してください。作成したファイルのみを削除します。

アップグレードのモニタリング Threat Defense

Threat Defense のアップグレードを開始すると、自動的にログオフされ、アップグレードの進捗を監視できるステータスページに移動します。また、このページには、進行中のインストールをキャンセルするオプションが含まれています。自動ロールバックを無効にしてアップグ

レードが失敗した場合は、このページから、アップグレードを手動でキャンセルするか、再試行できます。

デバイスに SSH で接続し、CLI（**show upgrade status**）を使用することもできます。ログエントリが生成されたときにそれらを表示するには **continuous** キーワードを追加します。また、詳細情報を表示するには **detail** キーワードを追加します。両方のキーワードを追加して、継続的な詳細情報を取得します

アップグレードが完了した後は、デバイスがリブートすると、ステータスページと CLI にアクセスできなくなります。

Threat Defense のアップグレードのキャンセルまたは再試行

アップグレードステータスのページまたは CLI を使用して、失敗した（または進行中）のメジャーおよびメンテナンスアップグレードを手動でキャンセルし、失敗したアップグレードを再試行することができます。

- アップグレードステータスのページ：進行中のアップグレードをキャンセルするには、[アップグレードのキャンセル（Cancel Upgrade）] をクリックします。アップグレードが失敗した場合は、[アップグレードのキャンセル（Cancel Upgrade）] をクリックしてジョブを停止し、アップグレード前のデバイスの状態に戻すことができます。また、[続行（Continue）] をクリックしてアップグレードを再試行することができます。
- CLI：進行中のアップグレードをキャンセルするには、**upgrade cancel** を使用します。アップグレードが失敗した場合は、**upgrade cancel** を使用してジョブを停止し、アップグレード前のデバイスの状態に戻すことができます。また、**upgrade retry** を使用してアップグレードを再試行することができます。

（注） デフォルトでは、Threat Defense はアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。高可用性の展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

これらのオプションは、パッチではサポートされていません。正常なアップグレードを元に戻す方法については、Threat Defense の復元 （980 ページ）を参照してください。

Threat Defense の復元

メジャーアップグレードまたはメンテナンスアップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元が可能です。Threat Defense を復元すると、ソフトウェアは、最後のメジャーアップグレードまたはメンテナンスアップグレードの直前の状態に戻ります。アップグレード後の設定変更は保持されません。パッチ適用後に復元すると、

パッチも必然的に削除されます。個々のパッチまたはホットフィックスを元に戻すことはできないので注意してください。

次の手順では、Device Manager から復元する方法について説明します。Device Manager にアクセスできない場合は、 **upgrade revert** コマンドを使用して SSH セッションの Threat Defense コマンドラインから復元できます。**show upgrade revert-info** コマンドを使用すると、システムがどのバージョンに戻るのかを確認できます。

始める前に

ユニットがハイアベイラビリティペアの一部である場合は、両方のユニットを元に戻す必要があります。理想的には、フェールオーバーの問題なしに設定を復元できるように、両方のユニットで復元を同時に開始します。両方のユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを開始します。復元時にトラフィックが中断されることに注意してください。そのため、可能であれば、これを業務時間外に実行してください。

Firepower 4100/9300 シャーシの場合、Firepower のメジャーバージョンには特別に認定および推奨されている付随の Threat Defense バージョンがあります。これは、Threat Defense ソフトウェアを復元した後に、推奨されていない（新しすぎる）バージョンの FXOS を実行している可能性があることを意味します。新しいバージョンの FXOS は旧バージョンの Threat Defense と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS をダウングレードすることはできないため、このような状況下で推奨の組み合わせを稼働するには、デバイスの再イメージ化が必要になります。

手順

ステップ 1 [Device] を選択し、次に [Updates summary] の [View Configuration] をクリックします。

ステップ 2 [System Upgrade] セクションで、[Revert Upgrade] リンクをクリックします。

現在のバージョンと復元されるバージョンを示す確認ダイアログボックスが表示されます。復元できるバージョンがない場合、[Revert Upgrade] リンクは表示されません。

ステップ 3 ターゲットバージョンが許容できるバージョンである場合（かつ使用可能な場合）、[Revert] をクリックします。

復元後、デバイスを Smart Software Manager に再登録する必要があります。

Threat Defense のアップグレードのトラブルシューティング

以下の問題は、スタンドアロンまたはハイアベイラビリティペアのデバイスをアップグレードするときに発生する可能性があります。ハイアベイラビリティのアップグレードに固有の問題をトラブルシューティングするには、ハイアベイラビリティ Threat Defense のアップグレードのトラブルシューティング （273 ページ）を参照してください。

アップグレードパッケージのエラー。

適切なアップグレードパッケージを見つけるには、使用しているモデルを シスコ サポートおよびダウンロード サイト で選択または検索し、適切なバージョンのソフトウェアのダウンロードページを参照します。使用可能なアップグレードパッケージは、インストールパッケージ、ホットフィックス、およびその他の該当するダウンロードとともに表示されます。アップグレードパッケージのファイル名には、プラットフォーム、パッケージタイプ（アップグレード、パッチ、ホットフィックス）、ソフトウェアバージョン、およびビルドが反映されています。

バージョン 6.2.1 以降のアップグレードパッケージは署名されており、ファイル名の最後は .sh.REL.tar です。署名付きのアップグレードパッケージは解凍しないでください。 アップグレードパッケージの名前を変更したり、電子メールで転送したりしないでください。

アップグレード中にデバイスにまったく到達できない。

デバイスは、アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止します。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。

アップグレード中にデバイスが非アクティブまたは無反応に見える。

進行中のメジャーおよびメンテナンスアップグレードは手動でキャンセルできます。Threat Defense のアップグレードのキャンセルまたは再試行（980 ページ）を参照してください。デバイスが応答しない場合、またはアップグレードをキャンセルできない場合は、Cisco TAC にお問い合わせください。

注意 システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウン「しない」でください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

アップグレードは成功したが、システムが予期どおりに機能しない。

まず、キャッシュされた情報が更新されていることを確認します。単にブラウザウィンドウを更新して再度ログインするのではなく、URL から「余分な」パスを削除し、ホームページに再接続します（たとえば、http://threat-defense.example.com/）。

引き続き問題が発生し、以前のメジャーリリースまたはメンテナンスリリースに戻す必要がある場合は、復元できる場合があります。Threat Defense の復元（980 ページ）を参照してください。復元できない場合は、イメージを再作成する必要があります。

アップグレードが失敗する。

メジャーアップグレードまたはメンテナンスアップグレードを開始する場合は、[アップグレードに失敗すると自動的にキャンセルされる...（Automatically cancel on upgrade failure...）]（自動キャンセル）オプションを使用して、次のように、アップグレードが失敗した場合の動作を選択します。

- [自動キャンセルが有効（Auto-cancel enabled）]（デフォルト）：アップグレードが失敗すると、アップグレードがキャンセルされ、デバイスは自動的にアップグレード前の状態に復元されます。問題を修正し、後で再試行してください。
- [自動キャンセルが無効（Auto-cancel disabled）]：アップグレードが失敗した場合、デバイスはそのままになります。問題を修正してすぐに再試行するか、手動でアップグレードをキャンセルして後で再試行してください。

詳細については、Threat Defense のアップグレードのキャンセルまたは再試行 （980 ページ）を参照してください。再試行またはキャンセルできない場合、または問題が解消されない場合は、Cisco TAC にお問い合わせください。

デバイスの再イメージ化

デバイスを再イメージ化すると、デバイス設定が消去され、新しいソフトウェアイメージがインストールされます。再イメージ化の目的は、工場出荷時のデフォルト設定でクリーンインストールすることです。

次の場合に、デバイスを再イメージ化します。

- ASA ソフトウェアから Threat Defense ソフトウェアにシステムを変換する場合。ASA イメージを実行しているデバイスを Threat Defense イメージを実行しているデバイスにアップグレードすることはできません。
- デバイスが正しく機能せず、設定の修正ですべての試行が失敗した場合。

デバイスの再イメージ化の詳細については、ご使用のデバイスモデルの『*Reimage the Cisco ASA or Threat Defense Device*』または *Threat Defense* のクイックスタートガイドを参照してください。これらのガイドは、http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html で入手できます。

システムのバックアップと復元

システム設定をバックアップしておくことで、将来的に設定ミスや物理的な災害が生じて設定が破損したとしても、デバイスを復元することができます。

代替のデバイスにバックアップを復元できるのは、どちらのデバイスも同じモデルで、（同時リリースだけでなく、ビルド番号を含む）同じバージョンのソフトウェアを実行している場合のみです。アプライアンス間で設定をコピーするためにバックアップおよび復元プロセスを使用しないでください。バックアップファイルには、この方法で共有することができないようにアプライアンスを一意に特定する情報が含まれます。

（注） バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワーク セグメント上の別のデバイスに設定を復元することもできます。バックアップにはライセンス情報やクラウド登録情報も含まれていないため、復元時に存在するライセンスやクラウド登録の状態はすべて保持されます。

バックアップには設定だけが含まれ、システム ソフトウェアは含まれません。デバイスを完全に再イメージ化する必要がある場合、ソフトウェアを再インストールしてからバックアップをアップロードして、設定を回復する必要があります。

バックアップ中は設定データベースがロックされます。バックアップの間はポリシー、ダッシュボードなどを表示できますが、設定を変更することはできません。復元を行っている間、システムは完全に使用できません。

「バックアップと復元」ページの表は、バックアップのファイル名、作成日時、ファイル サイズを含む、システムで使用できる既存のすべてのバックアップ コピーを示します。バックアップのタイプ（手動、スケジュール、繰り返し）は、システムに指示したバックアップ コピーの作成方法に基づいています。

ヒント バックアップ コピーはシステム自体に作成されます。ディザスタ リカバリのために必要なバックアップ コピーを確保するため、バックアップ コピーは手動でダウンロードし、安全なサーバーに保存する必要があります。システムは、デバイス上に最大3つのバックアップコピーを保持します。新しいバックアップによって、最も古いバックアップが置き換えられます。

次に、バックアップの管理と復元操作について説明します。

システムの即時バックアップ

希望する場合はいつでもバックアップを開始できます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[バックアップと復元（Backup and Restore）] のサマリーで [設定の表示（View Configuration）] をクリックします。

これにより、[バックアップおよび復元（Backup and Restore）] ページが開きます。使用可能なすべての既存のバックアップ コピーが表にリストされています。

ステップ 2 **[手動バックアップ（Manual Backup）] > [今すぐバックアップ（Back Up Now）]** をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

今すぐではなく、将来のある時刻にバックアップする場合は、代わりに [スケジュール（Schedule）] をクリックできます。

ステップ 4 （任意）[Encrypt File] オプションを選択して、バックアップファイルを暗号化します。

このオプションを選択した場合は、バックアップファイルの復元に必要な [Password]（および [Confirm Password]）を入力する必要があります。

ステップ 5 （ISA 3000 のみ）[バックアップファイルの場所（Location of Backup Files）] を選択します。

[ローカルハードディスク（Local Hard Disk）] または [SDカード（SD Card）] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。

ステップ 6 [今すぐバックアップ（Back Up Now）] をクリックします。

システムがバックアップ プロセスを開始します。バックアップが完了すると、バックアップファイルが表に表示されます。必要に応じて、バックアップ コピーをシステムにダウンロードして、他の場所に保存できます。

バックアップが開始されたら、[バックアップと復元（Backup and Restore）] ページを閉じてもかまいません。ただし、システムの動作が遅くなる可能性があるため、バックアップを完了するために作業を一時停止することを検討してください。

また、一部または全部のバックアップ中に、システムによってコンフィギュレーションデータベースのロックが取得され、それが原因でバックアップ プロセス中に変更を加えることができなくなる場合があります。

スケジュールされた時間でのシステムのバックアップ

システムを将来の特定の日時にバックアップするために、スケジュールバックアップを設定できます。スケジュールバックアップは、1 回だけ実行されます。定期的にバックアップを作成するようにバックアップ スケジュールを作成するには、スケジュールバックアップではなく、繰り返しバックアップを設定します。

（注） 将来のバックアップのスケジュールを削除するには、スケジュールを編集して、[削除（Remove）] をクリックします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[バックアップと復元（Backup and Restore）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 **[スケジュールバックアップ（Scheduled Backup）] > [バックアップをスケジュール（Schedule a Backup）]** をクリックします。

すでにスケジュール バックアップがある場合は、**[スケジュールバックアップ（Scheduled Backup）]** > **[編集（Edit）]** をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 バックアップの日時を入力します。

ステップ 5 （任意）[Encrypt File] オプションを選択して、バックアップファイルを暗号化します。

このオプションを選択した場合は、バックアップファイルの復元に必要な [Password]（および [Confirm Password]）を入力する必要があります。

ステップ 6 （ISA 3000 のみ）[バックアップファイルの場所（Location of Backup Files）] を選択します。

[ローカルハードディスク（Local Hard Disk）] または [SDカード（SD Card）] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。

ステップ 7 [スケジュール（Schedule）] をクリックします。

選択した日時に達すると、システムがバックアップされます。完了すると、バックアップ コピーがバックアップの表に一覧されます。

定期的なバックアップ スケジュールの設定

定期的なバックアップを設定し、システムを定期的にバックアップできます。たとえば、毎週金曜日の真夜中にバックアップをとることもできます。定期的なバックアップ スケジュールにより、常に最新のバックアップ セットを保持できます。

（注） 定期的なスケジュールを削除する場合、スケジュールを編集し、[削除（Delete）] をクリックします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[バックアップと復元（Backup and Restore）] のサマリーで [設定の表示（View Configuration）] をクリックします。

ステップ 2 **[定期バックアップ（Recurring Backup）]** > **[設定（Configure）]** をクリックします。

すでに定期バックアップを設定している場合は、**[定期バックアップ（Recurring Backup）]** > **[編集（Edit）]** をクリックします。

ステップ 3 バックアップの名前を入力し、任意で説明を入力します。

ステップ 4 [頻度（Frequency）] と関連スケジュールを選択します。

- [日次（Daily）]：時刻を選択します。バックアップは毎日、スケジュールされた時刻に取得されます。
- [週次（Weekly）]：曜日と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、毎週月曜日、水曜日、金曜日の 23 時（午後 11 時）にバックアップをスケジュールすることもできます。
- [月次（Monthly）]：日付と時刻を選択します。バックアップは選択した日付のスケジュールされた時刻に取得されます。たとえば、1 日、15 日、28 日の 23 時（午後 11 時）にバックアップをスケジュールすることもできます。

指定された時刻はサマータイムのため調整され、当該地域で時刻が調整されるたびに 1 時間、前または後に移動します。年間を通して正確な時刻を保持するには、時刻の変更の際にスケジュールを編集する必要があります。

ステップ 5 （任意）[Encrypt File] オプションを選択して、バックアップファイルを暗号化します。

このオプションを選択した場合は、バックアップファイルの復元に必要な [Password]（および [Confirm Password]）を入力する必要があります。

ステップ 6 （ISA 3000 のみ）[バックアップファイルの場所（Location of Backup Files）] を選択します。

[ローカルハードディスク（Local Hard Disk）] または [SDカード（SD Card）] にバックアップを作成できます。SD カードを使用する利点は、カードを使用して設定を交換デバイスに回復できることです。

ステップ 7 [保存（Save）] をクリックします。

選択した日付と時刻になると、バックアップが取得されます。完了すると、バックアップ コピーがバックアップ テーブルにリストされます。

定期的なスケジュールを変更または削除するまで、バックアップを取得し続けます。

バックアップの復元

デバイスでバックアップを取得したときに実行されていたものと同じソフトウェア バージョン（ビルド番号を含む）が実行されている限り、バックアップを復元できます。代替のデバイスにバックアップを復元できるのは、どちらのデバイスも同じモデルで、同じバージョンのソフトウェア（ビルド番号を含む）を実行している場合のみです。

ただし、このデバイスがハイアベイラビリティペアの一部である場合、バックアップは復元できません。まず、**[デバイス（Device）]** > **[ハイ アベイラビリティ（High Availability）]** ページから HA を無効化することで、バックアップを復元できます。バックアップに HA の設定が含まれている場合、デバイスは HA グループに再度参加します。両方のユニットで同じバックアップを復元しないでください（両方のユニットがアクティブになってしまうため）。代わりに、まず、アクティブにする装置でバックアップを復元し、その後に、別のユニットで同等のバックアップを復元してください。

復元するバックアップ コピーがまだデバイスに存在しない場合、復元する前にまずバックアップをアップロードする必要があります。

復元している間、システムはまったく使用できません。

（注） バックアップには管理 IP アドレスの設定は含まれません。したがって、バックアップ ファイルを復元しても、管理アドレスがバックアップ コピーにより置き換えられることはありません。これにより、アドレスに対する変更はすべて保持され、また異なるネットワーク セグメント上の別のデバイスに設定を復元することもできます。バックアップにはライセンス情報やクラウド登録情報も含まれていないため、復元時に存在するライセンスやクラウド登録の状態はすべて保持されます。

始める前に

別のシステムでバックアップを復元する場合（デバイスを交換するときなど）、ベストプラクティスは、最初にデバイスを登録し、バックアップファイルで設定された機能に必要なオプションのライセンスを有効にすることです。バックアップファイルにはライセンス情報やクラウドサービス情報が含まれていないため、復元前に行ったライセンスの変更やクラウドの登録は保持されます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[バックアップと復元（Backup and Restore）] のサマリーで [設定の表示（View Configuration）] をクリックします。

これにより、[バックアップおよび復元（Backup and Restore）] ページが開きます。使用可能なすべての既存のバックアップ コピーが表にリストされています。

ステップ 2 復元しようとするバックアップ コピーが、使用可能なバックアップのリストにない場合、**[アップロード（Upload）]** > **[検索（Browse）]** をクリックし、バックアップ コピーをアップロードします。

ステップ 3 ファイルの [復元（restore）] アイコン（  ）をクリックします。

復元するかどうかの確認が求められます。デフォルトでは、復元後にバックアップ コピーは削除されますが、これを保持するには、復元を続行する前に、[復元後にバックアップを削除しない（Do not remove the backup after restoring）] を選択します。

バックアップファイルが暗号化されている場合は、ファイルを開いて復号するために必要な [パスワード（Password）] を入力する必要があります。

復元が完了すると、システムは再起動します。

（注） システムが再起動後、脆弱性データベース（VDB）、地理位置情報、およびルールデータベースの更新が自動的にチェックされ、必要に応じてダウンロードされます。これらの更新は大規模な場合があるため、初回の試行が失敗する可能性があります。タスクリストを確認し、ダウンロードが失敗した場合はシステムデータベースの更新（973ページ）の説明に従って手動で更新をダウンロードしてください。またポリシーも再展開されます。更新が成功しないと、それ以降の展開はすべて失敗します。

ステップ 4 必要に応じて、**[デバイス（Device）]** > **[スマートライセンス（Smart License）]** > **[設定の表示（View Configuration）]** をクリックし、デバイスを再登録して、必要なオプションライセンスを再度有効にします。

バックアップにはライセンス情報やクラウド登録情報は含まれません。そのため、新しいシステムにバックアップを復元する場合（デバイスを交換するときなど）、システムが評価モードのときは、それを登録し、必要なすべてのライセンスを有効にする必要があります。復元前にデバイスを登録し、ライセンスを有効にした場合、追加の変更は必要ありません。

以前のバックアップを同じシステムに単に復元するだけの場合は、ライセンスやクラウド登録を変更する必要はありません。ただし、バックアップにはバックアップの作成後に無効にしたライセンスを必要とする機能が含まれている可能性があるため、必要なすべてのオプションライセンスが有効になっていることを確認してください。

ISA 3000 デバイスの交換

ISA 3000 の SD カードは、別の ISA 3000 デバイスとの間でやり取りできます。SD カード上にシステムバックアップを作成すれば、この機能を使用してデバイスを簡単に交換できます。その方法は、障害が発生したデバイスから SD カードを取り出して新しいデバイスに挿入するだけです。その後に、バックアップを使用して復元できます。

必要なバックアップを確実に用意するには、SD カードにバックアップを作成するバックアップ ジョブを設定します。

バックアップ ファイルの管理

新しいバックアップを作成すると、バックアップ ファイルがバックアップと復元ページに表示されます。バックアップ コピーは無期限に保たれません。デバイスのディスク領域の利用量が最大しきい値に達すると、新しいバックアップ コピー用の場所を空けるために、古いバックアップ コピーが削除されます。さらに、ホットフィックス以外のアップグレードをインストールすると、すべてのバックアップファイルが削除されます。したがって、定期的にバックアップ ファイルを管理し、最も保持したい特定のバックアップ コピーが削除されていないことを確認してください。

バックアップ コピーを管理するには、次の操作を行うことができます。

- ファイルを安全なストレージにダウンロード：バックアップ ファイルをワークステーションにダウンロードするには、ファイルの[ダウンロード（download）]アイコン（）をクリックします。その後、安全なファイル ストレージにファイルを移動できます。
- システムにバックアップ ファイルをアップロードする：デバイスで使用できなくなったバックアップ コピーを復元する場合は、**[アップロード（Upload）]** > **[ファイルの参照（Browse File）]** をクリックして、バックアップ コピーをワークステーションからアップロードします。その後、復元できます。

（注） アップロードされたファイルは、元のファイル名と一致するように名前が変更される場合があります。また、システムに 3 以上のバックアップコピーがすでに存在する場合、アップロードされたファイル用の場所を空けるために最も古いものは削除されます。古いソフトウェア バージョンによって作成されたファイルをアップロードすることはできません。

- バックアップを復元する：バックアップ コピーを復元するには、ファイルの [復元（restore）] アイコン（）をクリックします。復元の間システムは使用できなくなり、復元が完了するとリブートします。システムが稼働していて、動作中になってから設定を展開してください。
- バックアップ ファイルを削除する：特定のバックアップが必要でなくなったら、ファイルの削除アイコン（）をクリックします。削除の確認が求められます。削除すると、バックアップ ファイルを回復することはできません。

監査と変更管理

システム イベントやユーザが実行したアクションに関するステータス情報を表示できます。この情報は、システムを監査し、システムが適切に管理されていることを確認するために役立ちます。

監査ログを表示するには、**[デバイス（Device）]** > **[デバイス管理（Device Administration）]** > **[監査ログ（Audit Log）]** をクリックします。さらに、右上隅にある [タスクリスト（Task List）] アイコン ボタンまたは [展開（Deployment）] アイコン ボタンをクリックすると、システム管理情報を確認できます。

ここでは、システム監査および変更管理のいくつかの主要な概念とタスクについて説明します。

監査イベント

監査ログには、次のタイプのイベントを含めることができます。

[カスタムフィードの更新イベント（Custom Feed Update Event）]、[カスタムフィードの更新に失敗（Custom Feed Update Failed）]

これらのイベントは、カスタム セキュリティ インテリジェンス フィードの更新が正常に完了または失敗したことを示します。詳細には、更新を開始したユーザーと、更新されたフィードに関する情報が含まれます。

カスタムルールファイルのインポートの概要イベント

これらのイベントは、1 つ以上のカスタム侵入ルールを含むファイルをインポートしたことを示します。イベントには、追加、更新、および削除されたルールの数の概要と、インポートされたルールの詳細を示す差異ビューが含まれます。

Deployment Completed（展開完了）、Deployment Failed（展開失敗）：ジョブ名またはエンティティ名

これらのイベントは、正常に完了した展開ジョブまたは失敗した展開ジョブを示します。詳細には、ジョブを開始したユーザと、そのジョブエンティティに関する情報が含まれます。失敗したジョブには、その失敗に関連するエラー メッセージが含まれます。

詳細には[差異ビュー（Differences View）]タブもあります。このタブには、ジョブでデバイスに展開された変更が表示されます。これは、展開されたエンティティのすべてのエンティティ変更イベントの組み合わせです。

これらのイベントをフィルタリングするには、事前定義フィルタの[展開履歴（Deployment History）]をクリックします。これらのイベントのイベント タイプは Deployment Event（展開イベント）であり、完了したイベントまたは失敗したイベントのみをフィルタリングすることはできないことに注意してください。

イベント名には、ユーザー定義のジョブ名（定義している場合）または「User (*username*) Triggered Deployment（ユーザー（ユーザー名）トリガー イベント）」が含まれます。また、デバイス セットアップ ウィザードの実行時に発生する「Device Setup Automatic Deployment（デバイス セットアップ自動展開）」ジョブと「Device Setup Automatic Deployment (Final Step)（デバイスセットアップ自動展開（最終手順））」ジョブもあります。

Entity Created（エンティティ作成）、Entity Updated（エンティティ更新）、Entity Deleted（エンティティ削除）：エンティティ名（エンティティ型）

これらのイベントは、識別されたエンティティまたはオブジェクトに変更が加えられたことを示します。エンティティの詳細には、エンティティ名、タイプ、およびIDに加えて、変更を加えたユーザが含まれます。これらの項目に関してフィルタリングできます。詳細には[差異ビュー（Differences View）]タブもあります。このタブには、オブジェクトに加えられた変更が表示されます。

HA Action Event（HA アクション イベント）

これらのイベントは、高可用性設定でのアクション（ユーザが開始したアクションまたはシステムが開始したアクション）に関連したものです。HA Action Event はイベント タイプですが、イベント名は次のいずれかです。

- **HA Suspended**（HA 一時停止）：ユーザがシステムで HA を意図的に一時停止しました。
- **HA Resumed**（HA 再開）：ユーザがシステムで HA を意図的に再開しました。
- **HA Reset**（HA リセット）：ユーザがシステムで HA を意図的にリセットしました。
- **HA Failover: Unit Switched Modes**（HA フェールオーバー：ユニット モード切り替え）：ユーザーがモードを意図的に切り替えたか、ヘルスメトリック違反のためにシステムがフェールオーバーしました。このメッセージは、アクティブ ピアがスタンバイになったか、スタンバイ ピアがアクティブになったことを示します。

High Availability Sync Completed（高可用性同期完了）

アクティブユニットがスタンバイユニットと設定を同期しました。イベントには、同期バージョンと比較した前のバージョンの変更情報が含まれています。

Interface List Scanned（スキャンされたインターフェイスリスト）

このイベントは、インターフェイスインベントリの変更をスキャンしたことを示します。

Pending Changes Discarded（保留中の変更の破棄）

このイベントは、保留中のすべての変更をユーザが削除したことを示します。このイベントと以前の Deployment Completed イベントの間の Entity Created、Entity Updated、および Entity Deleted イベントで示されたすべての変更が削除され、影響を受けたオブジェクトの状態が、最後に展開されたバージョンに戻されています。

ルール更新イベント

Snort 3 を実行している場合、LSPUpdateServer エンティティからのこのイベントは、新しい侵入ルールパッケージがダウンロードされてインストールされたときに追加、削除、または変更された侵入ルールに関する詳細情報を示します。イベントは 100 のルールに制限されているため、100 を超えるルールが追加、削除、または変更された場合、イベントには完全な情報が含まれなくなります。このイベントは、Snort 2 の更新については表示されません。

Task Started（タスク開始）、Task Completed（タスク完了）、Task Failed（タスク失敗）

タスクイベントは、システムまたはユーザによって開始されたジョブの開始および終了を示します。これらの 2 つのイベントは、タスク リストで 1 つのタスクに統合されます。このタスク リストは、右上隅にある [タスクリスト（Task List）] ボタンをクリックすると表示されます。

タスクには、展開ジョブや手動（またはスケジュールされた）データベース更新などのアクションが含まれます。タスクリスト内の任意の項目は、監査ログの 2 つのタスクイベント、タスクの開始の表示、正常な完了または失敗のいずれかに対応します。

User Logged In（ユーザー ログイン）、User Logged Out（ユーザー ログアウト）：ユーザー名

これらのイベントは、Device Manager のユーザーログインおよびユーザーログアウトの時間と送信元 IP アドレスを示します。User Logged Out イベントは、アクティブ ログアウトと、アイドル時間を超過したための自動ログアウトの両方で発生します。

これらのイベントは、デバイスとの接続を確立している RA VPN ユーザに関するものではありません。また、デバイス CLI のログイン/ログアウトも含まれません。

監査ログの表示および分析

監査ログには、展開ジョブ、データベースの更新、Device Manager のログインとログアウトなど、システムが開始したイベントやユーザーが開始したイベントに関する情報が含まれています。

ログで確認できるイベントの種類の説明については、監査イベント（990 ページ）を参照してください。

手順

ステップ 1 [デバイス（Device）] をクリックし、**[デバイス管理（Device Administration）] > [設定の表示（View Configuration）]** リンクをクリックします。

ステップ 2 目次の [監査ログ（Audit Log）] をクリックします（未選択の場合）。

イベントは日付別にグループ分けされ、1 日の中では時間別にグループ分けされます。最新の日時がリストの一番上に表示されます。初めは、各イベントは折りたたまれているため、時間、イベント名、そのイベントを開始したユーザ、ユーザの送信元 IP アドレスのみ確認できます。ユーザと IP アドレスの「システム」は、デバイス自体がイベントを開始したことを意味しています。

次を実行できます。

- イベント名の横にある [>] をクリックしてイベントを開き、イベントの詳細を確認します。もう一度アイコンをクリックするとイベントが閉じます。多くのイベントには、イベント属性（イベントタイプ、ユーザ名、送信元 IP アドレスなど）の簡単なリストがあります。ただし、エンティティ イベントと展開イベントには次の 2 つのタブがあります。
  - [概要（Summary）]：基本的なイベント属性が示されます。
  - [差異ビュー（Differences View）]：既存の「展開済み」設定とイベントの一部として行われた変更との比較が示されます。展開ジョブの場合、このビューは長く、スクロールする必要がある場合があります。このタブには、展開ジョブの一部だったエンティティ イベントの変更のすべての差異が要約されます。
- [フィルタ（Filter）] フィールドの右にあるドロップダウン リストから別の時間範囲を選択します。デフォルトでは、過去 2 週間のイベントが表示されますが、過去 24 時間、7 日

間、月、または6ヵ月に変更できます。[カスタム（Custom）]をクリックし、開始および終了日時を入力して、正確な範囲を指定します。

- ログ内で任意のリンクをクリックして、該当項目の検索フィルタを追加します。リストが更新されて、該当項目を含むイベントだけが表示されます。単純に[フィルタ（Filter）]ボックスをクリックして、フィルタを直接作成することもできます。フィルタボックスの下には事前定義済みのフィルタがいくつかあり、クリックして関連するフィルタ条件をロードできます。イベントのフィルタリングの詳細については、監査ログのフィルタリング （994 ページ）を参照してください。
- ブラウザ ページをリロードして、ログを最新のイベントで更新します。

監査ログのフィルタリング

監査ログにフィルタを適用して、特定のタイプのメッセージだけが表示されるように絞り込むことができます。フィルタの各要素は、正確な完全一致です。たとえば、「User = admin」では **admin** という名前のユーザが開始したイベントだけが表示されます。

次の手法を単独または組み合わせて使用して、フィルタを作成できます。このリストは、フィルタ要素を追加するたびに自動的に更新されます。

事前定義のフィルタをクリック

[フィルタ（Filter）]フィールドの下には事前定義のフィルタがあります。リンクをクリックするだけでフィルタがロードされます。確認を求められます。すでにフィルタが適用されている場合は、追加されず、置き換えられます。

強調表示された項目をクリック

フィルタを作成する最も簡単な方法は、フィルタリングの基準となる値を含むログテーブルまたはイベント詳細情報内の項目をクリックすることです。項目をクリックすると、その値と要素の組み合わせに正しく定式化されている要素を使用して、[フィルタ（Filter）]フィールドが更新されます。ただし、この手法を使用するには、イベントの既存のリストに目的の値が含まれている必要があります。

項目に関するフィルタ要素を追加できる場合は、その項目にマウスカーソルを合わせると下線が引かれ、[クリックしてフィルタに追加（Click to Add to Filter）]コマンドが表示されます。

アトミック要素を選択

[フィルタ（Filter）]フィールドをクリックして、ドロップダウン リストから必要なアトミック要素を選択し、等号の後に照合値を入力してから Enter キーを押すことでフィルタを作成することもできます。次の要素に関するフィルタリングを実行できます。すべての要素がすべてのイベント タイプに関連するわけではないことに注意してください。

- [イベントタイプ（Event Type）]：これは、通常、イベント名と同じですが、異なる場合もあります（エンティティ名やユーザーのような可変修飾子はありません）。展

開イベントの場合、イベントタイプはDeployment Event（展開イベント）です。イベントタイプの説明については、監査イベント （990 ページ）を参照してください。

- [ユーザ（User）]：イベントを開始したユーザの名前。システム ユーザは SYSTEM（すべて大文字）です。
- [送信元IP（Source IP）]：ユーザーがイベントを開始した IP アドレス。システムが開始したイベントの送信元 IP アドレスは SYSTEM です。
- [エンティティID（Entity ID）]：エンティティまたはオブジェクトのUUID。これは、理解できない長い文字列（8e7021b4-2e1e-11e8-9e5d-0fc002c5f931 など）です。通常、このフィルタを使用するには、イベント詳細情報内のエンティティ ID をクリックするか、REST API を使用し、関連する GET コールによって必要な ID を取得する必要があります。
- [エンティティ名（Entity Name）]：エンティティまたはオブジェクトの名前。ユーザが作成したエンティティの場合は、通常、ユーザがオブジェクトに付けた名前（ネットワーク オブジェクトのInsideNetwork など）です。システムが生成したエンティティの場合は（一部のユーザー定義のエンティティについても）、事前定義されていて理解できる名前です。たとえば、明示的に名前を付けない展開ジョブの場合は「User (admin) Triggered Deployment」です。
- [エンティティタイプ（Entity Type）]：エンティティまたはオブジェクトの種類。これらは、事前定義されていて理解できる名前（Network Object など）です。API エクスプローラで「type」値の関連オブジェクト モデルを調べることによってエンティティ タイプを確認できます。通常、API タイプはすべて小文字であり、スペースは含まれません。それらをモデルに表示されているとおりに正確に入力し、Enter キーを押すと、文字列が理解しやすい形式に変更されます。どちらの形式で入力しても機能します。API エクスプローラを開くには、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

複雑な監査ログ フィルタのルール

複数のアトミック要素を含む複雑なフィルタを作成する場合、次のルールに注意してください。

- 同じタイプの要素には、そのタイプのすべての値の間に OR 関係があります。たとえば、「User = admin」と「User = SYSTEM」が含まれている場合、いずれかのユーザによって開始されたイベントと一致します。
- 異なるタイプの要素には、AND 関係があります。たとえば、「Event Type = Entity Updated」と「User = SYSTEM」が含まれている場合、アクティブ ユーザではなくシステムがエンティティを更新したイベントだけが表示されます。
- ワイルドカード、正規表現、部分一致、または単純なテキスト文字列の一致は使用できません。

展開およびエンティティ変更履歴の確認

展開およびエンティティイベントの詳細には、[差異ビュー（Differences View）] タブが含まれています。このタブには、古い設定と変更の色分けされた比較が表示されます。

- 展開ジョブの場合は、展開前にデバイスで実行されていた設定と、実際に展開された変更との比較です。
- エンティティイベントの場合は、オブジェクトの以前のバージョンに行われた設定の変更です。エンティティイベントの場合は、オブジェクトの以前のバージョンに行われた設定の変更です。

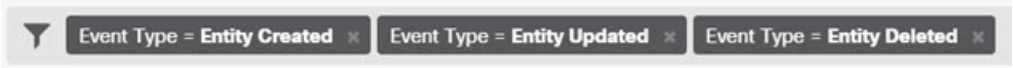
手順

ステップ 1 [デバイス（Device）] をクリックし、**[デバイス管理（Device Administration）]** > **[設定の表示（View Configuration）]** リンクをクリックします。

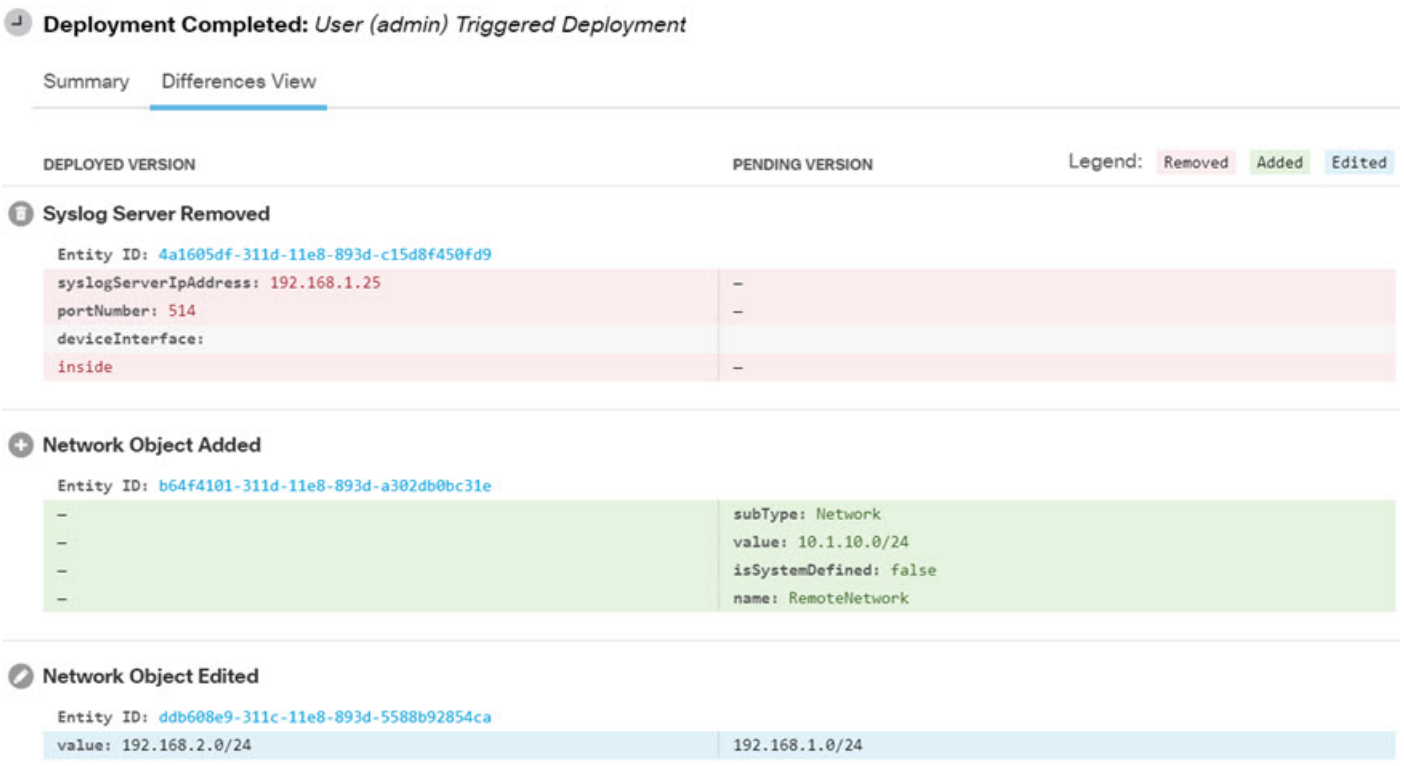
ステップ 2 目次の [監査ログ（Audit Log）] をクリックします（未選択の場合）。

ステップ 3 （オプション）メッセージのフィルタ処理：

- 展開イベント：フィルタ ボックスの下にある [展開履歴（Deployment History）] 事前定義フィルタをクリックします。
- エンティティ変更イベント：関心のある変更の種類に対して、[イベントの種類（Event Type）] 要素を使用してフィルタを手動で作成します。すべてのエンティティの変更を確認するには、[作成済みエンティティ（Entity Created）]、[更新済みエンティティ（Entity Updated）]、および [削除済みエンティティ（Entity Deleted）] の 3 つの仕様を含めます。フィルタは次のようになります。



ステップ 4 イベントを開き、[差異ビュー（Differences View）] タブをクリックします。



変更は色分けされていて、見出しにはオブジェクトの種類と、Added（作成）、Removed（削除）、または Edited（更新）が表示されます。Edited オブジェクトには、変更された属性またはオブジェクトから削除された属性のみ表示されます。展開ジョブの場合、変更されたエンティティごとに個別の見出しがあります。見出しには、オブジェクトのエンティティタイプが示されます。

保留中の全変更の廃棄

まだ展開されていない一連の設定の変更に納得していない場合は、すべての保留中の変更を破棄できます。破棄すると、すべての機能がデバイスに存在する状態に戻ります。その後、設定の変更をもう一度を開始できます。

手順

ステップ 1 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

保留中の変更がある場合、アイコンがドット付きで強調表示されます。

ステップ 2 **[詳細オプション（More Options）] > [すべて破棄（Discard All）]** をクリックします。

ステップ 3 確認ダイアログで [OK] をクリックします。

変更が破棄され、プロセスが完了すると、保留中の変更がないことを示すメッセージが表示されます。監査ログに [保留中の変更の破棄（Pending Changes Discarded）] イベントが追加されます。

デバイス設定のエクスポート

現在展開されている設定のコピーを JSON 形式でエクスポートできます。このファイルは、アーカイブまたはレコードの保存目的で使用できます。パスワードや秘密キーなどのセンシティブ データはすべてマスク処理されます。

ファイルを当該デバイスや別のデバイスにインポートすることはできません。この機能は、システム バックアップの代替機能ではありません。

設定をダウンロードする前に、少なくとも 1 つの展開ジョブが正常に完了している必要があります。

手順

ステップ 1 [デバイス（Device）] を選択し、[デバイス管理（Device Administration）] グループで [設定の表示（View Configuration）] をクリックします。

ステップ 2 目次で [設定のダウンロード（Download Configuration）] をクリックします。

ステップ 3 [デバイス設定の取得（Get Device Configuration）] をクリックして、ファイルを作成するジョブを開始します。

ファイルを事前に作成している場合、ファイルの作成日とともに、[ダウンロード（Download）] ボタンと「File is ready to download」メッセージが表示されます。

設定のサイズによっては、ファイルの生成に数分かかることがあります。タスク リストや監査ログを確認したり、定期的にこのページに戻ったりして、Export Config ジョブが完了してファイルが生成されるのを待ちます。

ステップ 4 ファイルが生成されたらこのページに戻り、[設定ファイルのダウンロード（Download the Configuration File）] ボタン（）をクリックして、ファイルをワークステーションに保存します。

Device Manager および Threat Defense ユーザーアクセスの管理

ユーザーが Threat Defense にログイン（HTTPS アクセス）するための外部認証および認可ソースを設定できますローカル ユーザ データベースとシステム定義の**管理者**ユーザに加えて（またはその代わりに）外部サーバを使用できます。Device Manager アクセス用の追加のローカルユーザーアカウントは作成できないことに注意してください。

設定を変更できる複数の外部 Device Manager ユーザーアカウントを用意できますが、それらの変更がユーザーごとに追跡されることはありません。1 人のユーザが変更を展開すると、すべてのユーザが行った変更が展開されます。ロック機能はありません。つまり、複数のユーザが同じオブジェクトの更新を同時に試みることができます。その結果、1 人のユーザだけが変更を正常に保存できます。また、ユーザに基づいて変更を破棄することもできません。

5 つのユーザーセッションを同時に処理できます。6 人目のユーザがログインすると、最も古いユーザ セッションが自動的にログオフされます。また、アイドル タイムアウトがあり、非アクティブ ユーザは 20 分後にログアウトされます。

脅威に対する防御 CLI への SSH アクセスでは、外部認証および認可を設定することもできます。ローカル データベースは外部ソースを使用する前に常にチェックされるため、フェールセーフ アクセスでは追加のローカル ユーザを作成することができます。ローカルソースと外部ソースの両方で重複するユーザを作成しないでください。**管理者**ユーザーを除き、CLI ユーザーと Device Manager ユーザーが入れ替わることはありません。ユーザーアカウントは完全に個別です。

（注） 外部サーバーを使用する場合、個別の AAA サーバーグループを設定するか、 AAA サーバー内に認証/認可ポリシーを作成して、ユーザーが特定の脅威に対する防御デバイスの IP アドレスだけにアクセスできるようにすることで、ユーザーによるデバイスのサブセットへのアクセスを制御できます。

ここでは、Device Manager および CLI ユーザーアクセスの設定方法と管理方法について説明します。

Device Manager （HTTPS）ユーザー用の外部認証（AAA）設定

外部 AAA サーバーからの Device Manager への HTTPS アクセスを提供できます。AAA 認証および認可を有効にすることにより、さまざまなレベルのアクセス権を付与でき、すべてのユーザーがローカル管理者アカウントを使用してログインする必要がなくなります。

これらの外部ユーザは、Threat Defense API および API エクスプローラについても認証されます。

AAA サーバーで管理ユーザーの認可を設定することで、ロールベース アクセス コントロール（RBAC）を提供できます。使用できる値はサーバータイプによって異なります。ユーザーが

Device Manager にログインすると、ページの右上隅にユーザー名とロールが表示されます。AAA サーバーで正しくアカウントを設定すると、次の手順で管理アクセス用にそのアカウントを有効にできます。

SAML ユーザー認証

SAML サーバー アイデンティティ ソースを設定するときに、承認レベルを含むフィールドを指定します。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバーの設定（210 ページ） を参照してください。

RADIUS ユーザー認証

ロールベース アクセス コントロール（RBAC）を提供するには、RADIUS サーバー上のユーザーアカウントを更新して、**cisco-av-pair** 属性を定義します（これはISE の場合で、FreeRADIUS ではこの属性のスペルはCisco-AVPair です。使用しているシステムで正しいスペルを確認してください）。この属性はユーザーアカウントで正しく定義されている必要があります。正しく定義されていないと、ユーザーの Device Manager へのアクセスが拒否されます。**cisco-av-pair** 属性のサポートされる値は、次のとおりです。

- **fdm.userrole.authority.admin** はフル管理者アクセスを提供します。これらのユーザは、ローカル**管理者**ユーザが実行できるすべてのアクションを実行できます。
- **fdm.userrole.authority.rw** は読み取り/書き込みアクセスを提供します。これらのユーザは、読み取り専用ユーザが実行できるすべてのアクションを実行でき、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、Device Manager ユーザーのセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- **fdm.userrole.authority.ro** は読み取り専用アクセスを提供します。これらのユーザは、ダッシュボードと設定を表示できますが、変更できません。ユーザが変更しようとすると、権限が不足していることを示すエラー メッセージが表示されます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンクの順にクリックします。

[System Settings] ページがすでに表示されている場合は、目次で [Management Access] をクリックします。

ステップ 2 まだ選択されていない場合は、[AAA設定（AAA Configuration）] タブをクリックします。

ステップ 3 [HTTPS接続（HTTPS Connection）] オプションの設定。

- [管理/REST API用のサーバーグループ（Server Group for Management/REST API）]：プライマリ認証ソースとして使用する RADIUS または SAML サーバーグループ（外部認証/認可用）またはローカル ユーザー データベース（LocalIdentitySource）を選択します。

サーバーグループがまだ存在しない場合は、リンクをクリックしてすぐに作成します。RADIUSの場合、サーバーごとにRADIUSサーバーオブジェクトを作成してグループに追加する必要もありますが、サーバーグループを定義するときにこれを実行できます。RADIUSの詳細については、RADIUSサーバおよびグループ（200ページ）を参照してください。SAMLの詳細については、SAMLサーバーの設定（210ページ）を参照してください。

- [ローカルによる認証（Authentication with LOCAL）]（RADIUSのみ）：外部RADIUSサーバーグループを選択する場合、ローカル[管理（admin）]アカウントを含むローカルアイデンティティソースを使用する方法を指定できます。次のいずれかを選択します。
  - [外部サーバの前（Before External Server）]：システムは、まずローカルソースに対してユーザ名とパスワードを確認します。
  - [外部サーバの後（After External Server）]：外部ソースが使用できない場合またはユーザアカウントが外部ソースで見つからなかった場合にのみ、ローカルソースが確認されます。
  - [使用しない（Never）]：（非推奨）ローカルソースがまったく使用されないため、管理者ユーザとしてログインできません。

    注意 [使用しない（Never）]を選択すると、[管理（admin）]アカウントを使用してDevice Managerにログインできなくなります。AAAサーバーが使用できなくなった場合またはAAAサーバーのアカウント設定が間違っている場合は、システムがロックされます。

（注） [ローカルによる認証（Authentication with LOCAL）]は、SAMLを使用する場合は適用されません。SAMLでは、SAMLログイン情報を入力するために[シングルサインオン（SSO）（Single-Sign On (SSO)）]リンクを明示的にクリックする必要があるため、ローカルのユーザー名とパスワードを入力することで、いつでもローカルデータベースを使用してログインできます。

ステップ4 [保存（Save）]をクリックします。

Threat Defense CLI（SSH）ユーザー用の外部認証（AAA）設定

外部RADIUSサーバーからのThreat Defense CLIへのSSHアクセスを提供できます。RADIUS認証および許可を有効にすることで、デバイスごとに個別のローカルユーザアカウントを定義するのではなく、単独の認証ソースからさまざまなレベルのアクセス権を提供することができます。

これらのSSH外部ユーザは、Threat Defense APIおよびAPIエクスプローラについては認証**されません**。SSHの許可を定義するために使用するメカニズムは、HTTPSアクセスに必要なものとは異なります。ただし、SSHとHTTPSの両方の許可条件で同じRADIUSユーザを設定し、どちらのプロトコルでも特定のユーザがシステムにアクセスできるようにすることは可能です。

SSH アクセスにロールベースのアクセス制御（RBAC）を提供するには、RADIUS サーバ上のユーザアカウントを更新して **Service-Type** 属性を定義します。この属性はユーザアカウントで定義されている必要があります。定義されていないと、ユーザの SSH へのアクセスが拒否されます。次に、**Service-Type** 属性でサポートされている値を示します。

- [Administrator (6)]：CLI への **config** アクセス認証を提供します。これらのユーザは、CLI ですべてのコマンドを使用できます。
- **NAS Prompt (7)** または 6 以外のレベル：CLI への **basic** アクセス認証を提供します。これらのユーザは **show** コマンドなど、モニタリングやトラブルシューティングのための読み取り専用コマンドを使用できます。

RADIUS サーバで正しくアカウントを設定すると、次の手順で SSH 管理アクセス用にそのアカウントを有効にできます。

（注） ローカルソースと外部ソースの両方で重複するユーザを作成しないでください。重複するユーザ名を作成する場合は、同じ認証権限を持っていることを確認します。許可権限がローカルユーザアカウントで異なる場合、外部バージョンのユーザアカウントのパスワードを使用してログインすることはできません。ログインできるのはローカルのパスワードを使用した場合のみです。権限が同じ場合、パスワードが異なると仮定して、使用するパスワードによって外部ユーザまたはローカルユーザのどちらでログインしているかが判断されます。最初にローカルデータベースが確認されますが、ユーザ名がローカルデータベースに存在するがパスワードが正しくない場合、外部サーバが確認され、外部ソースのパスワードが正しい場合、ログインが成功します。

始める前に

外部定義ユーザに次の動作を通知し、希望通りに設定できるようにしてください。

- 外部ユーザーが初めてログインすると、Threat Defense は必要な構造を作成しますが、ユーザーセッションを同時に作成することはできません。ユーザがセッションを開始するには、再度認証する必要があるだけです。ユーザには次のようなメッセージが表示されます。「New external username identified. Please log in again to start a session.」
- 同様に、最後のログイン以降に Service-Type で定義したユーザの認証が変更された場合は、ユーザは再認証する必要があります。ユーザには次のようなメッセージが表示されます。「Your authorization privilege has changed. セッションを開始するにはもう一度ログインしてください。（Please log in again to start a session.）」

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** リンクの順にクリックします。

[System Settings] ページがすでに表示されている場合は、目次で [Management Access] をクリックします。

ステップ 2 まだ選択されていない場合は、[AAA設定（AAA Configuration）] タブをクリックします。

ステップ 3 [SSH接続（SSH Connection）] のオプションを設定します。

- [サーバグループ（Server Group）]：プライマリ認証ソースとして使用する RADIUS サーバ グループまたはローカル ユーザ データベース（LocalIdentitySource）を選択します。外部認証を使用する RADIUS サーバ グループを選択する必要があります。

  サーバ グループがまだ存在しない場合は、[新しいRADIUSサーバグループの作成（Create New RADIUS Server Group）] リンクをクリックしてすぐに作成します。サーバごとに RADIUS サーバ オブジェクトを作成してグループに追加する必要もありますが、サーバ グループを定義するときにこれを実行できます。RADIUS の詳細については、RADIUS サーバおよびグループ （200 ページ）を参照してください。

  SSH 接続では、グループ内の最初の 2 台のサーバのみが使用されることに注意してください。3 つ以上のサーバがあるグループを使用する場合、追加のサーバが試行されることはありません。さらに、[デッドタイム（Dead Time）] と [最大失敗試行数（Maximum Failed Attempts）] グループ属性は使用されません。

- [ローカルによる認証（Authentication with LOCAL）]：外部サーバ グループを選択する場合、ローカル アイデンティティ ソースを使用する方法を指定できます。SSH アクセスでは、ローカルデータベースが常に外部サーバの前に確認されます。

ステップ 4 [保存（Save）] をクリックします。

Device Manager ユーザーセッションの管理

[モニタリング（Monitoring）] > [セッション（Sessions）] を選択すると、現在 Device Manager にログインしているユーザーのリストが表示されます。このリストには、各ユーザが現在のセッションにログインしている時間が示されます。

同じユーザ名が複数回表示される場合は、ユーザが異なる送信元アドレスからセッションを開いたことを意味します。セッションは、ユーザ名と送信元アドレスに基づいて個別に追跡され、各セッションは固有のタイムスタンプを持ちます。

このシステムでは、5 つの同時ユーザ セッションが可能です。6 人目のユーザがログインすると、最も古い現在のセッションが自動的にログアウトされます。また、アイドル状態のユーザは、アクティビティが 20 分間ないと自動的にログアウトされます。

Device Manager ユーザーが誤ったパスワードを入力し、3 回連続してログインに失敗した場合、アカウントは5分間ロックされます。ユーザーが再度ログインを試みるには、待機する必要があります。Device Manager ユーザーアカウントをロック解除する方法はありません。また、再試行回数やロックタイムアウトを調整することもできません（SSHユーザーの場合は、これらの設定を調整し、アカウントのロックを解除することができます）。

必要に応じて、セッションの[削除（delete）]アイコン（  ）をクリックすることにより、ユーザーセッションを終了させることができます。自分自身のセッションを削除すると、自分もログアウトされます。セッションを終了させた場合、ロックアウト期間はなく、ユーザーはすぐにログインしなおすことができます。

外部ユーザー用のスタンバイ HA ユニットでの Device Manager アクセスの有効化

Device Manager ユーザー用に外部認証を設定すると、これらのユーザーはハイアベイラビリティペアのアクティブおよびスタンバイ装置の両方にログインできます。ただし、スタンバイユニットへの初回ログインを成功させるには、アクティブユニットへのログインと比較して、いくつかの追加手順を実行する必要があります。

外部ユーザーがアクティブユニットに初めてログインすると、そのユーザーとユーザーのアクセス権を定義するオブジェクトが作成されます。管理者または読み取り/書き込みユーザーはその後、アクティブな装置からユーザーオブジェクトの設定を展開し、スタンバイ装置で表示されるようにする必要があります。

展開および後続の設定の同期が正常に完了して初めて、外部ユーザーはスタンバイユニットにログインできます。

管理者ユーザーと読み取り/書き込みユーザーは、アクティブユニットにログイン後に変更を展開できます。ただし、読み取り専用ユーザーは設定を展開できないため、適切な権限を持つユーザーに設定を展開を依頼する必要があります。

Threat Defense CLI のローカル ユーザー アカウントの作成

脅威に対する防御 デバイスで CLI にアクセスするユーザーを作成できます。これらのアカウントは管理アプリケーションへのアクセスは許可されず、CLI へのアクセスのみが有効になります。CLI はトラブルシューティングやモニターリング用に役立ちます。

複数のデバイス上にローカルユーザーアカウントを一度に作成することはできません。デバイスごとに固有のローカルユーザー CLI アカウントのセットがあります。

手順

ステップ 1 config 権限を持つアカウントを使用してデバイスの CLI にログインします。

管理者ユーザアカウントには必要な権限がありますが、config権限を持っていればどのアカウントでも問題ありません。SSH セッションまたはコンソール ポートを使用できます。

特定のデバイス モデルでは、コンソール ポートから FXOS CLI に移動します。**connect ftd** を使用して 脅威に対する防御 の CLI にアクセスします。

ステップ 2 ユーザー アカウントを作成します。

configure user add *username* {**basic** | **config**}

次の権限レベルを持つユーザを定義できます。

- **config**：ユーザーに設定アクセス権を付与します。すべてのコマンドの管理者権限がユーザに与えられます。
- **basic**：ユーザーに基本的なアクセス権を付与します。これはユーザに設定コマンドの入力を許可しません。

例：

次の例では、configアクセス権を使用して、joecoolという名前のユーザアカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

（注） **configure password** コマンドを使用してパスワードを変更できることをユーザーに伝えます。

ステップ 3 （任意）セキュリティ要件を満たすようにアカウントの性質を調整します。

次のコマンドを使用してデフォルトのアカウント動作を変更できます。

- **configure user aging** *username max_days warn_days*

  ユーザのパスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1 ~ 9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントの作成時はパスワードの有効期限はありません。

- **configure user forcereset** *username*

  次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

  アカウントがロックされる前の連続したログイン失敗の最大回数を 1 ～ 9999 までで設定します。**configure user unlock** コマンドを使用してアカウントのロックを解除します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswdlen** *username number*

  パスワードの最小長を 1 ～ 127 までで設定します。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザーパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザーが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりしなければならない可能性があります。システムのユーザーアカウントを管理するには、次のコマンドを使用します。

- **configure user access** ユーザ名 {**basic** | **config**}

  ユーザ アカウントの権限を変更します。

- **configure user delete** *username*

  指定したアカウントを削除します。

- **configure user disable** *username*

  指定したアカウントを削除せず無効にします。アカウントを有効にするまでユーザはログインできません。

- **configure user enable** *username*

  指定したアカウントを有効にします。

- **configure user password** *username*

  指定したユーザのパスワードを変更します。ユーザーは通常 **configure password** コマンドを使用して自分のパスワードを変更する必要があります。

- **configure user unlock** *username*

  ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザーアカウントをロック解除します。

システムの再起動またはシャットダウン

必要に応じて、システムを再起動またはシャットダウンできます。

下記の手順以外に、**reboot** コマンドまたは **shutdown** コマンドを使用して、SSH セッションまたは Device Manager CLI コンソールからこれらのタスクを実行することもできます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）]** > **[再起動/シャットダウン（Reboot/Shutdown）]** > リンクをクリックします。

すでに [システム設定（System Settings）] ページを表示している場合は、目次の [再起動/シャットダウン（Reboot/Shutdown）] をクリックします。

ステップ 2 必要な機能を実行するボタンをクリックします。

- [再起動（Reboot）]：システムが正常に動作しておらず、試行錯誤しても問題解決に至らない場合、デバイスを再起動できます。また、システムソフトウェアをリロードするためにデバイスを再起動するよう求める手順がいくつかあります。
- [シャットダウン（Shut Down）]：システムをシャットダウンして、制御された方法で電源をオフにします。ネットワークからデバイスを削除する場合、たとえばデバイスを交換する場合は、シャットダウンを使用します。デバイスをシャットダウンした後は、ハードウェアのオン/オフスイッチからのみ電源をオンにすることができます。

ステップ 3 アクションが完了するまで待ちます。

コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

ISA 3000 の場合、シャットダウンが完了すると、システム LED が消灯します。電源を切る前に、少なくとも 10 秒待ってください。

システムの再起動またはシャットダウン中は、Device Manager または CLI で他のアクションを実行できません。

再起動中、Device Manager のページが更新され、再起動が完了するとログインページに移動します。再起動が完了する前にページを更新しようとすると、その時点での Device Manager Web サーバーの動作状態に基づいて、Web ブラウザに 503 または 404 エラーが表示されることがあります。

シャットダウンの場合、システムは最終的にまったく応答しなくなり、404 エラーが表示されます。システムを完全にオフにしようとしているため、これは想定される結果です。

システムのトラブルシューティング

ここでは、いくつかのシステムレベルのトラブルシューティングのタスクおよび機能について説明します。特定の機能（アクセス コントロールなど）のトラブルシューティングの詳細については、その機能に関する章を参照してください。

接続をテストするための ping アドレス

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。これは基本接続が機能していることを意味します。ただし、デバイスで実行されている他のポリシーにより、特定のタイプのトラフィックは正常にデバイスを通過できないことがあります。**ping** CLI コンソールを開く、またはデバイス CLI へのログインによって、使用することができます。

（注） システムには複数のインターフェイスがあるため、アドレスのpingに使用されるインターフェイスを制御できます。接続をテストすることが重要であるため、確実に正しいコマンドを使用する必要があります。たとえば、システムは管理インターフェイスを介してシスコのライセンスサーバーに到達する必要があります。この場合、**ping system** コマンドを使用して接続をテストする必要があります。**ping** を使用すると、複数のデータ インターフェイスを通じて到達できるかをテストするため、同じ結果が得られない可能性があります。

通常の ping は、ICMP パケットを使用して接続をテストします。ネットワークで ICMP が禁止されている場合は、代わりに TCP ping を使用できます（データ インターフェイスの ping のみ）。

IP アドレスまたは完全修飾ホスト名（FQDN）のいずれかを ping できます。ping が FQDN で機能するためには、管理インターフェイスまたはデータインターフェイスのいずれかに設定された DNS サーバーが IP アドレスを正常に返す必要があります。管理インターフェイスとデータインターフェイスに個別に DNS サーバーを設定する必要があります。特定のインターフェイスに DNS サーバーが設定されていない場合は、**dig** コマンドを使用して、特定の FQDN の IP アドレスを検索します。

次に、ネットワーク アドレスを ping するための主なオプションを示します。

管理インターフェイスを介したアドレスの ping

ping system コマンドを使用します。

ping system *host*

ホストはIPアドレスまたは完全修飾ドメイン名（FQDN）（www.example.comなど）にできます。データ インターフェイスを介した ping とは違い、システム ping のデフォルト数はありません。pingはCtrl+cを使用して停止するまで続けられます。次に例を示します。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

ルーティング テーブルを使用するデータ インターフェイスを介したアドレスの ping

pingコマンドを使用します。インターフェイスを指定せずに、システムが一般的にホストへのルートを検索できるかどうかをテストします。システムは通常このようにしてトラフィックをルーティングするため、一般的に実行する必要があるのはこのテストです。

ping *host*

次に例を示します。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

（注） タイムアウト、繰り返し回数、パケット サイズ、さらには送信するデータ パターンを指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

特定のデータ インターフェイスを介したアドレスの ping

特定のデータインターフェイスを経由した接続をテストする場合、**ping interface** *if_name* コマンドを使用します。

ping interface *if_name host*

次に例を示します。

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping を使用するデータ インターフェイスを介したアドレスの ping

ping tcp コマンドを使用します。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。

ping tcp [**interface** *if_name*] *host port*

ホストと TCP ポートを指定する必要があります。FQDN のみが判明している場合は、**nslookup** *fqdn-name* コマンドを使用して、IP アドレスを判別します。

オプションで、pingを送信するインターフェイスではなく、pingの送信元インターフェイスであるインターフェイスを指定できます。このタイプの ping では、必ずルーティング テーブルを使用します。

TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。次に例を示します。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

（注） タイムアウト、繰り返し回数、および TCP ping の送信元アドレスも指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

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。トレースルートでは、宛先に対して、無効なポートでUDPパケットを送信したり、ICMPv6エコーを送信したりします。宛先までの途中にあるルータから ICMP Time Exceeded メッセージが返され、トレースルートにそのエラーが報告されます。各ノードは3つのパケットを受信するため、有益な結果を得る機会が 1 台のノードにつき 3 回あります。**traceroute** CLI コンソールを開く、またはデバイス CLI へのログインによって、 を使用することができます。

（注） データインターフェイス（**traceroute**）または仮想管理インターフェイス（**traceroute system**）を経由するルートをトレースするための個別のコマンドがあります。適切なコマンドを使用するようにしてください。

次の表に、パケットによって出力に表示される可能性のある結果を示します。

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。
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。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!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。

仮想管理インターフェイスを介したルートの追跡

traceroute system コマンドを使用します。

traceroute system *[*接続先（*Destination*）*]*

ホストには、IPv4/IPv6 アドレスまたは完全修飾ドメイン名（FQDN）（www.example.com など）を使用できます。次に例を示します。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

データ インターフェイスを介したルートの追跡

traceroute コマンドを使用します。

traceroute *[*接続先（*Destination*）*]*

データインターフェイスにDNSサーバーを設定する場合、ホストにはIPv4/IPv6アドレスまたはwww.example.comのような完全修飾ドメイン名（FQDN）を指定できます。特定のインターフェイスにDNSサーバーが設定されていない場合は、**dig** コマンドを使用して、特定の FQDN の IP アドレスを検索します。次に例を示します。

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

（注） タイムアウト、パケット存続時間、1 ノードあたりのパケット数、およびトレースルートの送信元として使用する IP アドレスまたはインターフェイスを指定できます。使用可能なオプションを表示するには、CLI でヘルプ インジケータの「?」を使用します。

デバイスのトレースルートへの表示

デフォルトでは、Threat Defense デバイスは、トレースルートにホップとして表示されません。表示されるようにするには、デバイスを通過するパケットの存続可能時間を減らし、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。そのためには、必要なサービス ポリシー ルールとその他のオプションを設定する FlexConfig オブジェクトを作成する必要があります。

サービス ポリシーとトラフィック クラスの詳細については、https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html で入手可能な『*Cisco ASA Series Firewall Configuration Guide*』を参照してください。

（注） パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間（TTL）をデクリメントすると、予期しない結果が発生する可能性があります。トラフィック クラスを定義する際には、これらの考慮事項に注意してください。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 TTL を減らすためのオブジェクトを作成します。

a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

b) オブジェクトの名前を入力します。例、**Decrement_TTL**。

c) [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

適切なサブモードでコマンドを有効にするために、ネゲートテンプレートに、親コマンドと同様にこれらのコマンドも含める必要があります。

FlexConfig ポリシーからこのオブジェクトを削除した場合（正常に導入された後）、および導入が失敗した場合でも（設定を前の状態にリセットするため）、ネゲートテンプレートが適用されます。

したがって、この例では、ネゲート テンプレートは次のようになります。

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  no set connection decrement-ttl
```

e) [OK] をクリックしてオブジェクトを保存します。

ステップ 4 オブジェクトを FlexConfig ポリシーに追加します。

FlexConfig ポリシー内の選択したオブジェクトのみ展開されます。

a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。
b) [グループリスト（Group List）] で [+] をクリックします。
c) Decrement_TTL オブジェクトを選択し、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

NTP のトラブルシューティング

システムは、正確で一貫性のある時間に基づいて正しく動作し、イベントやその他のデータ ポイントを正確に処理します。少なくとも 1 つ、理想的には 3 つの Network Time Protocol（NTP）サーバーで、システムが常に信頼できる時間情報を取得できるようにする必要があります。

デバイスの接続概要図（メイン メニューで [デバイス（Device）] をクリック）に、NTP サーバーへの接続ステータスが示されます。ステータスが黄色またはオレンジ色の場合、設定したサーバーへの接続に問題があります。接続の問題が解消されない（一時的な問題ではない）場合は、次の操作を試します。

- まず、**[デバイス（Device）] > [システム設定（System Settings）] > [NTP（NTP）]** で 3 つ以上の NTP サーバーが設定されていることを確認します。これは要件になっていませんが、NTP サーバーが 3 つ以上あると信頼性が大幅に向上します。
- 管理インターフェイス IP アドレス（**[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]** で定義される）と NTP サーバーの間にネットワーク パスがあることを確認します。
  - 管理インターフェイス ゲートウェイがデータ インターフェイスであり、デフォルト ルートが不適切な場合、**[デバイス（Device）] > [ルーティング（Routing）]** で NTP サーバーに対するスタティック ルートを設定できます。
  - 明示的な管理インターフェイス ゲートウェイを設定する場合は、デバイス CLI にログインし、**ping system** コマンドを使用して各 NTP サーバーへのネットワーク パスがあるかどうかテストします。
- デバイス CLI にログインし、次のコマンドを使用して NTP サーバーのステータスを確認します。
  - **show ntp**：このコマンドは、NTP サーバとその可用性に関する基本的な情報を示します。ただし、Device Manager の接続ステータスではその他の情報を使用してステータ

スを示すため、このコマンドが示す内容や接続ステータス図が示す内容と一致しないことがあります。このコマンドは CLI コンソールから発行することもできます。

- **system support ntp**：このコマンドには、**show ntp** の出力と、NTP プロトコルで記載される標準 NTP コマンド **ntpq** の出力が含まれています。NTP 同期を確認する必要がある場合は、このコマンドを使用します。

  「Results of 'ntpq -pn」の部分を探します。たとえば、次のように表示されます。

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

  この例では、NTP サーバのアドレスの前の「+」は、潜在的な候補であることを示します。アスタリスク * は、現在の時刻源のピアを示します。

  NTP デーモン（NTPD）は、各ピアから取得される 8 つのサンプルのスライディングウィンドウを使用して、1 つのサンプルをピックアップします。その後、クロック選択によって正しいチャイマーと不正なティッカーが特定されます。次に、NTPD がラウンドトリップ距離を特定します（候補のオフセットをラウンドトリップ遅延の半分以上にすることはできません）。接続の遅延、パケットの損失、またはサーバーの問題が発生して 1 つまたはすべての候補が拒否されると、同期中に長い遅延が生じます。また、調整にも非常に長い時間がかかります。クロック規律アルゴリズムによって、クロック オフセットおよびオシレータ エラーを解決する必要がありますが、これには数時間かかる可能性があります。

（注） refid が .LOCL. の場合は、ピアが無規律のローカル クロックであることを示します。つまり、時間設定にそのローカルクロックのみを使用します。選択したピアが .LOCL. の場合、Device Manager は NTP 接続を常に黄色（非同期）にマークします。通常 NTP は、より適切な候補を利用できる場合、.LOCL. 候補を選択しません。そのため、サーバーを 3 つ以上設定する必要があります。

管理インターフェイスの DNS のトラブルシューティング

管理インターフェイスで使用する少なくとも 1 つの DNS サーバを設定する必要があります。DNS サーバは、スマート ライセンス、データベースの更新（GeoDB、ルール、VDB など）、

およびドメイン名を解決する必要があるその他すべてのアクティビティなどのサービスへのクラウド接続のために必要です。

DNS サーバの設定は簡単な作業です。デバイスの初回設定時に、使用する DNS サーバの IP アドレスを入力するだけです。この設定は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバ（DNS Server）]** ページで後で変更できます。

ただし、ネットワークの接続性の問題や DNS サーバ自体の問題のために、システムが完全修飾ドメイン名（FQDN）を解決できないことがあります。システムが DNS サーバを使用できない場合は、問題を特定して解決するために、以下の操作を検討してください。DNS の一般的な問題のトラブルシューティング （946 ページ）も参照してください。

手順

ステップ 1 問題の有無を確認します。

a) SSH を使用してデバイスの CLI にログインします。

b) **ping system www.cisco.com** を入力します。次のような「unknown host」メッセージが表示される場合、システムはドメイン名を解決できていません。ping が成功する場合は、これで終了です。DNS は機能しています（ping を停止するには、Ctrl+C キーを押します）。

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

（注） **system** キーワードを **ping** コマンドに含めることが非常に重要です。**system** キーワードを指定すると、管理 IP アドレスから ping が送信されます。このインターフェイスは、管理 DNS サーバを使用する唯一のインターフェイスです。スマート ライセンスや更新のためにサーバへのルートが必要なため、www.cisco.com の ping 実行も適切なオプションです。

ステップ 2 管理インターフェイスの設定を確認します。

a) **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** をクリックし、[管理インターフェイス（Management Interface）] を編集して、次の点を確認します。変更を加える場合、それらの変更は [保存（Save）] をクリックするとすぐに適用されます。管理アドレスを変更する場合は、再度接続してログインし直す必要があります。

- 管理ネットワークのゲートウェイ IP アドレスが正しいこと。データ インターフェイスをゲートウェイとして使用している場合は、後続の手順でその設定を確認します。
- データインターフェイスをゲートウェイとして使用していない場合は、管理 IP アドレスとサブネットマスク、およびゲートウェイ IP アドレスが同じサブネット上にあることを確認します。

b) **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバ（DNS Server）]** をクリックして、正しい DNS サーバが設定されていることを確認します。

ネットワーク エッジにデバイスを展開している場合は、使用できる DNS サーバに関するサービス プロバイダー固有の要件が存在する場合があります。

c) データ インターフェイスをゲートウェイとして使用している場合は、必要なルートがあることを確認します。

0.0.0.0 のデフォルト ルートが必要です。デフォルト ルートのゲートウェイを介して DNS サーバを使用できない場合は、追加のルートが必要になります。次に、2 つの基本的な状況を示します。

- 外部インターフェイスのアドレスを取得するために DHCP を使用していて、[DHCPを使用してデフォルトルートを取得（Obtain Default Route using DHCP）] オプションを選択した場合、デフォルトルートは Device Manager には表示されません。SSH から **show route** を入力して、0.0.0.0 のルートがあることを確認します。これは外部インターフェイスのデフォルト設定であるため、発生する可能性が高い状況です。（**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** に移動して、外部インターフェイスの設定を確認します）。
- 外部インターフェイスで静的 IP アドレスを使用している場合、または DHCP からデフォルト ルートを取得していない場合は、**[デバイス（Device）]** > **[ルーティング（Routing）]** を開きます。デフォルト ルートに正しいゲートウェイが使用されていることを確認します。

デフォルトルートから DNS サーバに到達できない場合は、[ルーティング（Routing）] ページで DNS サーバへのスタティック ルートを定義する必要があります。直接接続ネットワーク（つまり、システムのいずれかのデータ インターフェイスに直接接続されているネットワーク）のルートは追加しないでください。システムは、それらのネットワークに自動的にルーティングできるためです。

また、誤ったインターフェイスからサーバにトラフィックを誤導するスタティックルートが存在しないことを確認します。

d) 展開ボタンに未展開の変更の存在が示されている場合は、ここで展開して、展開が完了するまで待ちます。

e) **ping system www.cisco.com** を再テストします。問題が解消しない場合は、次の手順に進みます。

ステップ 3 SSH セッションで、**dig www.cisco.com** を入力します。

- **dig** に、DNS サーバから応答を得たことが示されているのに、サーバが名前を検出できない場合、DNS は正しく設定されているものの、使用している DNS サーバに FQDN のアドレスが設定されていないことを意味しています。このエラーは、NXDOMAIN ステータスによって示されます。応答は次のようになります。

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

解決策：この場合、別の DNS サーバを設定するか、更新した DNS サーバを使用して、解決する必要がある FQDN を解決できるようにします。ネットワーク管理者や ISP と協力して、ネットワークで動作する DNS サーバの IP アドレスを取得します。

- コマンドがタイムアウトする場合、システムが DNS サーバーに到達できないか、または現在すべての DNS サーバーがダウンしていて応答していません（この可能性は低いです）。次の手順に進みます。

ステップ 4 **traceroute system** *DNS_server_ip_address* コマンドを使用して、DNS サーバーへのルートをトレースします。

たとえば、DNS サーバが 10.100.10.1 の場合は、次のように入力します。

```
> traceroute system 10.100.10.1
```

可能性がある結果を以下に示します。

- トレースルートが完了し、DNS サーバに到達している。この場合、DNS サーバへのルートが実際にあり、システムが到達できます。したがって、ルーティングの問題はありません。ただし、何らかの理由でこのサーバに対する DNS 要求の応答を得られていません。

  解決策：パス沿いのルータやファイアウォールで、DNS に使用されるポートである UDP/53 のトラフィックがドロップされている可能性があります。異なるネットワーク パスに沿って DNS サーバへのアクセスを試すことができます。これは解決が難しい問題です。トラフィックをブロックしているノードを確認し、システム管理者と協力してアクセス ルールを変更する必要があります。

- トレースルートから 1 つのノードにさえ到達できない。これは、次のように表示されます。

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
```

```
(and so forth)
```

解決策：この場合、システム内にルーティングの問題があります。ゲートウェイ IP アドレスに対して **ping system** を試行してください。前述の手順に従い、管理インターフェイスの設定を再度確認し、必要なゲートウェイとルートを設定していることを確認します。

- トレースルートは、ルートを解決できなくなる前にいくつかのノードを通過します。これは、次のように表示されます。

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
 2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
 3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
 4  * * *
 5  * * *
 6  * * *
```

解決策：この場合、最後のノードでルーティングが中断されています。システム管理者と協力して、そのノードに設定されているルートを修正する必要があります。ただし、意図的にそのノードから DNS サーバへのルートを設定していない場合は、ゲートウェイを変更するか、または独自のスタティック ルートを作成して、トラフィックを DNS サーバにルーティングできるルータを指すようにする必要があります。

CPU およびメモリ使用率の分析

CPU とメモリ使用率についてのシステムレベルの情報を表示するには、**[モニタリング（Monitoring）] > [システム（System）]** を選択して、CPU およびメモリ使用率を表す棒グラフを確認します。これらのグラフには **show cpu system** コマンドと **show memory system** コマンドを使用して CLI で収集した情報が表示されます。

CLI コンソールを開くか CLI にログインして、これらのコマンドの別バージョンを使用すると、他の情報を表示できます。通常、この情報を確認するのは使用状況に関する永続的な問題がある場合や、Cisco Technical Assistance Center（TAC）の指示があった場合に限られます。詳細情報の多くは複雑で、TAC の解釈が必要です。

以下に、調べることができるいくつかのポイントを示します。これらのコマンドの詳細については、http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html で Cisco Firepower Threat Defense コマンド リファレンスを参照してください。

- **show cpu** は、データプレーンの CPU 使用率を表示します。
- **show cpu core** は、各 CPU コアの使用率を別々に表示します。
- **show cpu detailed** は、追加のコアごと、およびデータプレーン全体の CPU の使用率を表示します。

- **show memory** は、データプレーンのメモリ使用量を表示します。

（注） 一部のキーワード（上記に説明されていない）は、最初に **cpu** または **memory** コマンドを使用して、プロファイリングまたは他の機能を設定する必要があります。これらの機能は、TACの指示があった場合のみ使用します。

ログの表示

システムはさまざまなアクションに関する情報をログに記録します。システムログを開くには **system support view-files** コマンドを使用します。Cisco Technical Assistance Center（TAC）への問い合わせ時にこのコマンドを使用すると、出力を解釈して、適切なログを表示できるようになります。

コマンドは、ログを選択するためのメニューを表示します。ウィザードに移動するには、次のコマンドを使用します。

- サブディレクトリに変更するには、ディレクトリの名前を入力して、Enter を押します。
- 表示するファイルを選択するには、プロンプトで **s** と入力します。その後、ファイル名の入力が求められます。完全な名前を入力する必要があります。大文字と小文字は区別されます。ファイルリストにはログのサイズが示されます。非常に大きいログを開く前には検討が必要な場合があります。
- 「--More--」が表示されたらSpaceキーを押してログエントリの次のページを表示します。次のログエントリのみを表示するにはEnterを押します。ログの最後に到達すると、メインメニューに戻ります。「--More--」の行には、ログのサイズと表示した量が示されます。**ログのすべてのページを表示する必要がなく、ログを閉じて、コマンドを終了するには、Ctrl+C を使用します。**
- メニュー構造のレベルを 1 つ上がるには、**b** を入力します。

ログを開いたままにして、新しいメッセージが追加されたときにそのメッセージを確認できるようにするには、**system support view-files** コマンドの代わりに **tail-logs** コマンドを使用します。

次の例は、システムへのログイン試行を追跡する cisco/audit.log ファイルがどのように表示されるかを示しています。ファイルリストは、最上位のディレクトリで始まり、その後、現在のディレクトリ内のファイル リストが続きます。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
```

```
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login
successful,
2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login
successful,
2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login
successful,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked
account.,

<remaining log truncated>
```

トラブルシューティング ファイルの作成

問題レポートを提出した際に、Cisco Technical Assistance Center（TAC）の担当者により、システム ログ情報の提出を求められることがあります。この情報は、問題の診断に役立ちます。診断ファイルの提出は、求められた場合だけでかまいません。

次の手順では、ログ レベルを設定して診断ファイルを作成する方法について説明します。

手順

ステップ 1 [the name of the device in the menu] をクリックします。[デバイス（Device）]

ステップ 2 [トラブルシューティング（Troubleshooting）] の下で、[ファイルの作成を要求（Request File to be Created）] または [ファイルの作成を再要求（Re-Request File to be Created）]（事前に作成していた場合）をクリックします。

システムが診断ファイルの生成を開始します。他のページに移動して、後で戻ってきてステータスを確認できます。ファイルの準備が整うと、ファイル作成日時が [ダウンロード（Download）] ボタンとともに表示されます。

ステップ 3 ファイルの準備が整ったら、[ダウンロード（Download）] ボタンをクリックします。

ファイルは、ブラウザの標準のダウンロード方式を使用してワークステーションにダウンロードされます。

一般的でない管理タスク

次に、ごくまれにしか行われないアクションについて説明します。これらすべてのアクションは、デバイス設定の消去を引き起こします。これらの変更を加える前に、デバイスが現在、実稼働ネットワークに対して重要なサービスを提供していないことを確認します。

ファイアウォール モードの変更

Threat Defense ファイアウォールは、ルーテッドモードまたはトランスペアレントモードで実行できます。ルーテッド モードのファイアウォールはルーテッド ホップであり、スクリーン 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。

ローカルの Device Manager はルーテッドモードのみをサポートします。ただし、デバイスをトランスペアレントモードで実行する必要がある場合は、ファイアウォールモードを変更して、Management Center でデバイスを管理することができます。逆に、トランスペアレント モードのデバイスをルーテッド モードに変換すると、ローカル マネージャでそのデバイスを設定することができ、Management Center を使用してルーテッド モードのデバイスを管理することもできます。

ローカル管理であるか、リモート管理であるかに関係なく、モードを変更するためにはデバイスの CLI を使用する必要があります。

次の手順では、ローカル マネージャを使用している場合、またはローカル マネージャを使用予定の場合のモードの変更方法について説明します。

⚠

注意 ファイアウォールモードを変更すると、デバイス設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は保持されます。

始める前に

トランスペアレントモードに移行するには、ファイアウォールのモードを変更する前に Management Center をインストールします。

いずれかの機能ライセンスを有効にしている場合、ローカルマネージャを削除してリモート管理に切り替える前に、Device Manager でそれらのライセンスを無効にする必要があります。無効にしないと、それらのライセンスが Cisco Smart Software Manager のデバイスに割り当てられたままになります。「オプション ライセンスの有効化または無効化（109 ページ）」を参照してください。

デバイスが高可用性用に設定されている場合は、まず、デバイスマネージャ(可能な場合)または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

手順

ステップ 1 SSH クライアントを使用して [管理IPアドレス（management IP address）] への接続を開き、設定 CLI アクセスを持つユーザー名でデバイス CLI にログインします。たとえば、[管理者（admin）] ユーザー名など。

管理 IP アドレスに接続している間は、この手順に従うことが重要です。Device Manager を使用する場合、データインターフェイスの IP アドレスを介してデバイスを管理することもできます。ただしデバイスをリモートで管理するには、管理物理ポートと管理 IP アドレスを使用する必要があります。

管理 IP アドレスに接続できない場合、次のように対処します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理ネットワークに管理IPアドレスとゲートウェイが設定されていることを確認します。Device Manager から、**[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]** を選択して、アドレスおよびゲートウェイを設定します（CLI では、**configure network ipv4/ipv6 manual** コマンドを使用してください）。

  （注） 管理IPアドレスに外部ゲートウェイを使用していることを確認します。リモート マネージャを使用している場合、データ インターフェイスをゲートウェイとして使用することはできません。

ステップ 2 モードをルーテッドからトランスペアレントに変更して、リモート管理を使用するには、次の手順を実行します。

a) ローカル管理を無効にし、ノー マネージャ モードを開始します。

アクティブなマネージャが存在する間は、ファイアウォール モードを変更できません。マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) ファイアウォール モードをトランスペアレントに変更します。

configure firewall transparent

例：

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) リモート マネージャを設定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

ここで、

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} で、このデバイスを管理する Management Center の DNS ホスト名または IP アドレス（IPv4 または IPv6）を指定します。Management Center が直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、*nat_id* が必要です。
- *Regkey* はデバイスを Management Center へ登録するのに必要な、英数字の一意の登録キーです。
- *nat_id* は、Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

たとえば、登録キー **secret** で 192.168.0.123 のマネージャを使用するには、以下のコマンドを入力します。

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.
```

```
> show managers
Host                    : 192.168.0.123
Registration Key        : ****
Registration            : pending
RPC Status              :
```

d) Management Center にログインし、デバイスを追加します。

詳細については、Management Center のオンライン ヘルプを参照してください。

ステップ 3 モードをトランスペアレントからルーテッドに変更して、ローカル管理に変換するには、次の手順を実行します。

a) Management Center からデバイスを登録解除します。

b) 脅威に対する防御 デバイスの CLI にアクセスします。可能ならばコンソール ポートからアクセスします。

これは、モードを変更すると設定が削除され、管理IPアドレスはデフォルトに戻ってしまうため、モード変更後に管理 IP アドレスへの SSH 接続が失われることがあるためです。

c) ファイアウォール モードをルーテッドに変更します。

configure firewall routed

例：

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) ローカル マネージャを有効にします。

configure manager local

次に例を示します。

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

これで、Web ブラウザで **https://***management-IP-address* にアクセスしてローカル マネージャを開くことができるようになりました。

設定のリセット

最初からやり直す場合は、システム設定を工場出荷時のデフォルトにリセットできます。設定を直接リセットすることはできませんが、マネージャを削除して追加すると設定がクリアされます。

設定を消去してバックアップを復元する場合は、復元するバックアップ コピーを既にダウンロードしていることを確認してください。システムを復元するには、システムのリセット後にバックアップ コピーをアップロードする必要があります。

始める前に

いずれかの機能ライセンスを有効にした場合は、ローカルマネージャを削除する前に Device Manager でそれらを無効にする必要があります。無効にしないと、それらのライセンスが Cisco Smart Software Manager のデバイスに割り当てられたままになります。「オプション ライセンスの有効化または無効化 （109 ページ）」を参照してください。

デバイスが高可用性用に設定されている場合は、まず、Device Manager （可能な場合）または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

手順

ステップ 1 SSH クライアントを使用して、管理 IP アドレスへの接続を開き、設定 CLI アクセス権を持つユーザー名でデバイスの CLI にログインします。たとえば、[管理者（admin）] ユーザー名など。

ステップ 2 マネージャを削除するには、**configure manager delete** コマンドを使用します。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 3 ローカル マネージャを設定します。

configure manager local

次に例を示します。

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

これで、Web ブラウザで **https://***management-IP-address* にアクセスしてローカル マネージャを開くことができるようになりました。設定をクリアすると、デバイス セットアップ ウィザードの完了を求めるメッセージが表示されます。

Cisco Secure Firewall 3100 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で Threat Defense CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

⚠

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
> configure raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
> show raid
```

```
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。

b) SSD を RAID に追加します。

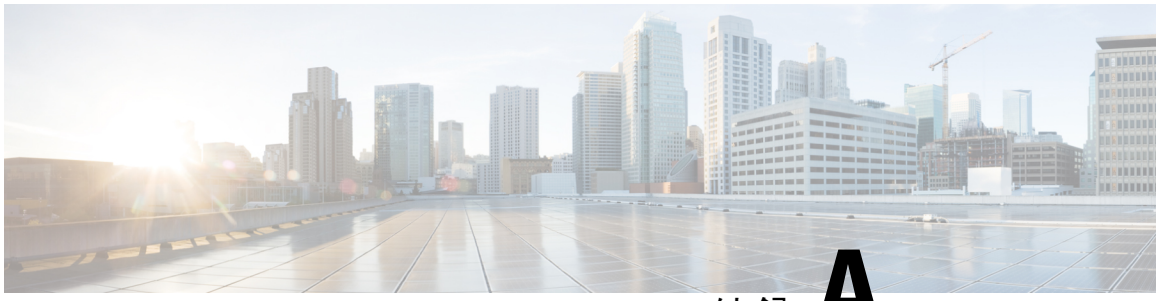
configure raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

configure raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。



付録 A

詳細設定

いくつかのデバイスの機能は、ASA 設定コマンドを使用して設定されます。Device Manager はコマンドベースの多くの機能を設定できますが、それらのすべてはサポートしません。Device Manager でサポートされていないこれらの ASA 機能の一部を使用する必要がある場合は、Smart CLI または FlexConfig を使用して手動で機能を設定できます。

次のトピックでは、このタイプの高度な設定について、より詳細に説明します。

Smart CLI と FlexConfig について

Threat Defense では、ASA 設定コマンドを使用して、すべての機能ではなく一部の機能を実装します。脅威に対する防御 設定コマンドの一意のセットはありません。

次の方法により CLI を使用して機能を設定できます。

- **Smart CLI**：（推奨の方法です。）Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。

- **FlexConfig**：FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。

Smart CLI と FlexConfig のポイントは、Device Manager のポリシーと設定によって直接サポートされていない機能を設定できることです。

注意 Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。禁止されていないコマンドはすべて、設定できます。Smart CLI と FlexConfig を使用して機能を有効にすると、その他の設定済みの機能で予期しない結果が生じる可能性があります。

設定した Smart CLI と FlexConfig のオブジェクトに関するサポートについては、Cisco Technical Assistance Center にお問い合わせください。Cisco Technical Assistance Center は、顧客に代わってカスタム設定を設計したり、作成したりしません。正常な動作や他の 脅威に対する防御 機能の相互運用性について、シスコは一切保証しません。Smart CLI と FlexConfig の機能は、いつでも廃止になる可能性があります。完全に保証された機能のサポートについては、Device Manager サポートを待つ必要があります。疑問がある場合、Smart CLI または FlexConfig は使用しないでください。

ここでは、これらの機能についてさらに詳しく説明します。

Smart CLI と FlexConfig の推奨される使用法

FlexConfig ポリシーには、推奨される使用法が主に 2 つあります。

- ASA から 脅威に対する防御 に移行中で、互換性はあるが、Device Manager が直接サポートしていない機能を使用しています（および使用を継続する必要があります）。この場合、ASA で **show running-config** コマンドを使用してその互換機能の設定を確認し、その機能を実装する FlexConfig オブジェクトを作成します。2 台のデバイスでの **show running-config** の出力を比較して確認します。
- 脅威に対する防御 を使用しているが、ある設定または機能を設定する必要があります。たとえば、Cisco Technical Assistance Center が、発生している特定の問題が特定の設定により解決されると伝えます。複雑な機能については、ラボ デバイスを使用して FlexConfig をテストし、期待する動作を得られることを確認します。

ASA設定を再作成する前に、まず標準的なポリシーで同等の機能を設定できるかどうかを判断します。たとえば、アクセス コントロール ポリシーには侵入検知および防御、HTTPおよびその他のタイプのプロトコル インスペクション、URL フィルタリング、アプリケーション フィルタリング、アクセス制御が含まれており、ASAはこれらの要素を別個の機能を使用して実装します。多くの機能はCLIコマンドを使用して設定されていないので、**show running-config** の出力にすべてのポリシーが表示されるわけではありません。

（注） 常に、ASA と 脅威に対する防御 との間の重複は 1 対 1 であるわけではないことに注意してください。ASAの設定を 脅威に対する防御デバイス上で完全に再現しようとしないでください。設定する機能は、FlexConfig を使用して慎重にテストする必要があります。

Smart CLI および FlexConfig オブジェクトの CLI コマンド

脅威に対する防御 では一部の機能の設定に ASA コンフィギュレーション コマンドを使用します。ASA のすべての機能に 脅威に対する防御 との互換性があるわけではありませんが、脅威に対する防御 で使用はできるが Device Manager ポリシーでは設定できない機能があります。Smart CLI および FlexConfig オブジェクトを使用すると、これらの機能を設定するために必要な CLI を指定できます。

Smart CLI または FlexConfig を使用して機能を手動で設定することに決めた場合、適切な構文を認識し、これに従ってコマンドを実装する必要があります。FlexConfig は CLI コマンド構文を検証しません。正しいシンタックスと CLI コマンドの設定に関する詳細については、ASA ドキュメンテーションを参照してください。

- 『ASA CLI Configuration Guides』では機能を設定する方法について説明しています。ガイドはこちらからご覧ください。 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- 『ASA Command References』ではコマンド名ごとにその他の情報が記載されています。リファレンスはこちらからご覧ください。 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

ここでは、コンフィギュレーション コマンドについて詳しく説明します。

ソフトウェアのアップグレードが FlexConfig ポリシーに与える影響

新しいバージョンの 脅威に対する防御 ソフトウェアにはそれぞれ、Device Manager の機能を設定するためのサポートが追加されています。これらの新機能は、FlexConfig を使用して以前に設定した機能と重複する場合があります。

アップグレードの後に、FlexConfig ポリシーおよびオブジェクトを調べる必要があります。Device Manager または Smart CLI 内の追加されたサポートのために禁止されたコマンドがある場合は、オブジェクトのアイコンとメッセージに問題が示されます。その場合は、設定をやりなおしてください。禁止されたコマンドのリストは、コマンドをどのように設定する必要があるのかを判断するために役立ちます。

FlexConfig ポリシーに添付されている FlexConfig オブジェクトに新しく禁止されたコマンドが含まれていても、システムは変更の展開を妨げません。ただし、FlexConfig ポリシーに示されているすべての問題を解決するまでは、新しい Smart CLI オブジェクトを作成できません。

FlexConfig ポリシーから問題のあるオブジェクトを単に削除できます。これは、デバイス設定にアクティブに展開しているオブジェクトにのみ制限が適用されるためです。そのため、オブジェクトを削除してから、それらを、対応する Smart CLI または統合された Device Manager 設定を作成する際にリファレンスとして使用できます。新しい設定に不満がない場合は、単にオブジェクトを削除できます。削除されたオブジェクトに、禁止されていない要素が含まれている場合は、それらを編集してサポートされていないコマンドを削除してから、オブジェクトを FlexConfig ポリシーに再添付できます。

ASA ソフトウェアのバージョンおよび現在の CLI 設定の特定

システムが ASA ソフトウェア コマンドを使用して一部の機能を設定するため、脅威に対する防御 デバイスで実行するソフトウェアで使用されている現在の ASA バージョンを特定する必要があります。このバージョン番号に従って、機能設定時の手順に使用する ASA CLI 設定ガイドを選択します。また、現在の CLI ベースの設定を確認し、実装する ASA 設定と比較する必要があります。

脅威に対する防御 設定とどの ASA 設定も大きく異なることに注意してください。脅威に対する防御 ポリシーの多くは CLI の外部で設定されるため、コマンドを調べても設定を確認することができません。ASA と 脅威に対する防御 設定が 1 対 1 で対応するように作成しようとしないでください。

この情報を表示するには、Device Manager の CLI コンソールを開くか、デバイスの管理インターフェイスに SSH 接続し、次のコマンドを発行します。

- **show version system** また、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号を検索します。
- **show running-config** 現在の CLI 設定を表示します。
- **show running-config all** 現在の CLI 設定にすべてのデフォルト コマンドを含めます。

禁止された CLI コマンド

Smart CLI と FlexConfig の目的は、Device Manager を使用して 脅威に対する防御 デバイスで設定できない ASA デバイスで利用可能な機能を設定することです。

したがって、Device Manager に同等の機能がある ASA 機能は設定することができません。次の表に、これらの禁止されたコマンド領域のいくつかを示します。このリストには、設定モードを開始する多数の親コマンドが含まれています。親の禁止には、子コマンドの禁止が含まれています。また、コマンドの **no** バージョンと、関連する **clear** コマンドも含まれます。

FlexConfig オブジェクトエディタでは、オブジェクトにこれらのコマンドを含めることができません。Smart CLI テンプレートは、設定可能なコマンドのみが含まれるため、このリストが適用されません。

禁止された CLI コマンド	説明
aaa	**[オブジェクト（Objects)]**>**[アイデンティティソース（Identity Sources）]** を使用します。
aaa-server	**[オブジェクト（Objects)]**>**[アイデンティティソース（Identity Sources）]** を使用します。

禁止された CLI コマンド	説明
access-list	部分的にブロックされます。 • **ethertype** アクセス リストを作成できます。 • **extended** および **standard** アクセスリストは作成できません。Smart CLI 拡張アクセス リストまたは標準アクセス リスト オブジェクトを使用してこれらの ACL を作成します。その後、それらは、サービス ポリシー トラフィック クラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド（**match access-list** など）で使用できます。 • **advanced** アクセス リスト（システムが **access-group** コマンドで使用する）は作成できません。代わりに、**[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を使用してアクセス ルールを設定します。 • **webtype** アクセス リストは作成できません。
anyconnect-custom-data	**[デバイス（Device）] > [リモートアクセスVPN（Remote Access VPN）]** を使用して セキュアクライアント を設定します。
asdm	この機能は脅威に対する防御システムには適用されません。
as-path	Smart CLI AS パス オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、自律システム パス フィルタを設定します。
attribute	—
auth-prompt	この機能は脅威に対する防御システムには適用されません。
boot	—
call-home	—
captive-portal	**[ポリシー（Policies）] > [アイデンティティ（Identity）]** を使用して、アクティブな認証に使用するキャプティブ ポータルを設定します。
clear	—
client-update	—
clock	**[デバイス（Device）] > [システム設定（System Settings）] > [NTP]** を使用してシステム時間を設定します。
cluster	—

禁止された CLI コマンド	説明
command-alias	—
community-list	Smart CLI 拡張コミュニティ リストまたは標準コミュニティ リスト オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、コミュニティ リスト フィルタを設定します。
compression	—
configure	—
crypto	[オブジェクト（Objects）]ページで、[証明書（Certificates）]、[IKEポリシー（IKE Policies）]、および [IPsecプロポーザル（IPSec Proposals）] を使用します。
ddns	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DDNSサービス（DDNS Service）]** を使用してダイナミック DNS を設定します。
dhcp-client	—
dhcpd	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DHCPサーバ（DHCP Server）]** を使用します。 ただし、**dhcpd option** コマンドは許可されます。
dhcprelay	代わりに、脅威防御 APIの dhcprelayservices リソースを使用します。
dns	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を使用してグループを割り当てます。
dns-group	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を使用してグループを割り当てます。
domain-name	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を使用してグループを割り当てます。
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—

禁止された CLI コマンド	説明
event	—
failover	—
fips	—
firewall	Device Manager 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。
hostname	**[デバイス（Device）] > [システム設定（System Settings）] > [ホスト名（Hostname）]** を使用します。
hpm	この機能は脅威に対する防御システムには適用されません。
http	**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** で[データインターフェイス（Data Interfaces）] タブを使用します。
inline-set	—
interface（BVI、管理、イーサネット、GigabitEthernet、およびサブインターフェイス用）	部分的にブロックされます。 **[デバイス（Device）]>[インターフェイス（Interfaces）]** ページで物理インターフェイス、サブインターフェイス、およびブリッジ仮想インターフェイスを設定します。FlexConfig を使用して追加のオプションを設定できます。 ただし、次の **interface** モードコマンドは、これらのタイプのインターフェイスでは禁止されています。 **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
vni、**redundant**、**tunnel** の **interface**	**[デバイス（Device）]>[インターフェイス（Interfaces）]** ページでインターフェイスを設定します。Device Manager は、これらのタイプのインターフェイスをサポートしていません。

禁止された CLI コマンド	説明
ip audit	この機能は脅威に対する防御システムには適用されません。代わりに、アクセス制御ルールを使用して侵入ポリシーを適用します。
ip-client	管理ゲートウェイとしてデータ インターフェイスを使用するようシステムを設定するには、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** を使用します。
ip local pool	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** を使用してアドレス プールを設定します。
ipsec	—
ipv6	Smart CLI IPv6 プレフィックス リスト オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、IPv6 のプレフィックス リスト フィルタを設定します。
ipv6-vpn-addr-assign	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** を使用してアドレス プールを設定します。
isakmp	**[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用します。
jumbo-frame	デフォルトの 1500 以上のインターフェイスの MTU を増やす場合、システムは自動的にジャンボ フレームのサポートを有効にします。
ldap	—
license-server	**[デバイス（Device）]** > **[スマートライセンス（Smart License）]** を使用します。
logging	**[オブジェクト（Objects）]** > **[Syslogサーバー（Syslog Servers）]** および **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ロギング設定（Logging Settings）]** を使用します。 ただし、FlexConfig で **logging history** コマンドを設定できます。
management-access	—
migrate	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** および **[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用して IKEv2 サポートを有効にします。

禁止された CLI コマンド	説明
mode	Device Manager はシングルコンテキストモードのみをサポートしています。
mount	—
mtu	**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** でインターフェイスごとに MTU を設定します。
nat	**[ポリシー（Policies）]** > **[NAT]** を使用します。
ngips	—
ntp	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[NTP]** を使用します。
object-group network **object network**	**[オブジェクト（Objects）]**>**[ネットワーク（Network）]** を使用します。 FlexConfig でネットワーク オブジェクトまたはグループを作成することはできませんが、テンプレート内で変数としてオブジェクト マネージャで定義されているネットワーク オブジェクトおよびグループは使用できます。
object service |natorigsvc **object service |natmappedsvc**	**object service** コマンドは一般に使用できますが、|natorigsvc または |natmappedsvc という内部オブジェクトは編集できません。これらの名前の垂直バーは意図的であり、制限されているオブジェクト名の最初の文字です。
passwd **password**	—
password-policy	—
policy-list	スマート CLI ポリシー リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシー リストを設定します。
policy-map sub-commands	ポリシー マップでは次のコマンドを設定できません。 **priority** **police** **match tunnel-group**
prefix-list	Smart CLI IPv4 プレフィックス リスト オブジェクトを作成し、それらを Smart CLI OSPF または BGP オブジェクトで使用して、IPv4 のプレフィックス リスト フィルタを設定します。
priority-queue	—

禁止された CLI コマンド	説明
privilege	—
reload	リロードはスケジュールできません。システムは、システムを再起動するために **reload** コマンドを使用せず、**reboot** コマンドを使用します。
rest-api	この機能は脅威に対する防御システムには適用されません。REST API は常にインストールされ、有効になります。
route	**[デバイス（Device）]** > **[ルーティング（Routing）]** を使用してスタティック ルートを設定します。
route-map	スマート CLI ルート マップ オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルート マップを設定します。
router bgp	BGP には Smart CLI テンプレートを使用します。
router eigrp	EIGRP には Smart CLI テンプレートを使用します。
router ospf	OSPF には Smart CLI テンプレートを使用します。
scansafe	この機能は脅威に対する防御システムには適用されません。代わりに、アクセス制御ルールで URL フィルタリングを設定します。
setup	この機能は脅威に対する防御システムには適用されません。
sla	—
snmp-server	SNMP を設定するには、FTP API SNMP リソースを使用します。
ssh	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** で [データインターフェイス（Data Interfaces）] タブを使用します。
ssl	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[SSL設定（SSL Settings）]** を使用します。
telnet	Threat Defense は Telnet 接続をサポートしません。デバイス CLI にアクセスするには、Telnet の代わりに SSH を使用します。
time-range	—

禁止された CLI コマンド	説明
tunnel-group	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** および **[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用します。
tunnel-group-map	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** および **[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用します。
user-identity	**[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** を使用します。
username	CLI ユーザーを作成するには、デバイスに対して SSH またはコンソールセッションを開き、**configure user** コマンドを使用します。
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	この機能は脅威に対する防御システムには適用されません。

Smart CLI テンプレート

次の表では、機能に基づく Smart CLI テンプレートについて説明します。

（注） スマート CLI テンプレートを使用して OSPF と BGP を設定することもできます。ただし、これらのテンプレートは、[詳細設定（Advanced）] ページではなく **[デバイス（Device）]** > **[ルーティング（Routing）]** ページから使用できます。

機能	テンプレート	説明
オブジェクト：AS パス	AS パス	ルーティング プロトコル オブジェクトで使用する AS パス オブジェクトを作成します。

機能	テンプレート	説明
オブジェクト：アクセス リスト	拡張アクセス リスト 標準アクセス リスト	ルーティング オブジェクトで使用する拡張 ACL または標準 ACL を作成します。ACL を使用する許可コマンドを設定する FlexConfig オブジェクトからの名前によって、これらのオブジェクトを参照することもできます。
オブジェクト：コミュニティ リスト	拡張コミュニティ リスト 標準コミュニティ リスト	ルーティング オブジェクトで使用する拡張コミュニティ リストまたは標準コミュニティ リストを作成します。
オブジェクト：プレフィックス リスト	IPv4 プレフィックス リスト IPv6 プレフィックス リスト	ルーティング オブジェクトで使用する IPv4 または IPv6 プレフィックス リストを作成します。
オブジェクト：ポリシー リスト	ポリシー リスト	ルーティング オブジェクトで使用するポリシー リストを作成します。
オブジェクト：ルート マップ	ルート マップ	ルーティング オブジェクトで使用するルート マップを作成します。

Smart CLI および FlexConfig に関する注意事項と制限事項

Smart CLI または FlexConfig を介して機能を設定するときは、次の点に注意してください。

- FlexConfig オブジェクトで定義されているコマンドは、Smart CLI を含む Device Manager で定義された機能のすべてのコマンドの後に展開されます。したがって、デバイスに対してこれらのコマンドが発行される前に設定されているオブジェクト、インターフェイスなどに依存する場合があります。Smart CLI テンプレートで FlexConfig が展開された項目を使用する必要がある場合は、Smart CLI テンプレートを作成して展開する前に FlexConfig を作成して展開します。たとえば、OSPF Smart CLI テンプレートを使用して EIGRP ルートを再配布する場合は、最初に FlexConfig を使用して EIGRP を設定し、それから OSPF Smart CLI テンプレートを作成します。
- FlexConfig から設定した機能または機能の一部を削除するが、Smart CLI テンプレートがその機能を参照している場合は、最初に機能を使用する Smart CLI テンプレートでコマンドを削除する必要があります。その後、Smart CLI で設定された機能が参照しないように設定を展開します。FlexConfig から機能を削除して設定を再展開すると、最終的に完全削除できます。

Smart CLI オブジェクトの設定

Smart CLI オブジェクトは、Device Manager の他では構成することができない機能を定義します。Smart CLI オブジェクトは、機能の構成において一定レベルのガイダンスを提供します。指定された機能（テンプレート）について、すべての可能なコマンドが事前に読み込まれ、入力した変数が検証されます。したがって、機能を構成するためにCLIコマンドを使用しても、Smart CLI オブジェクトは FlexConfig オブジェクトほど自由な形式ではありません。

Smart CLI テンプレートは一定レベルのガイダンスを提供しますが、ネットワークで正しく動作するように値を選択するために ASA 構成ガイドとコマンド リファレンスを読み、コマンドの使用方法を理解する必要があります。理想的には、動作する ASA 構成はすでにあり、必要とされるのは Smart CLI オブジェクトでコマンドの同じシーケンスを構築することだけです。

Smart CLI オブジェクトは、機能エリアによってグループ化されます。

（注） 定義したすべての Smart CLI オブジェクトが展開されます。FlexConfig とは異なり、いくつかの Smart CLI オブジェクトを作成し、その中から選択して展開することはできません。構成する機能に対してのみ Smart CLI オブジェクトを作成します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で [スマートCLI（Smart CLI）] の下の該当する機能のエリアをクリックします。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

オブジェクトを削除するには、そのオブジェクトのごみ箱アイコン（）をクリックします。

ステップ 4 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 5 構成する機能の [CLIテンプレート（CLI Template）] を選択します。

システムはコマンドテンプレートを [テンプレート（Template）] ウィンドウに読み込みます。最初に必要なコマンドのみが表示されます。これらはテンプレートに必要な最小構成を表します。

ステップ 6 変数を入力し、必要に応じてテンプレートにコマンドを追加します。

理想的には、ASA または Threat Defense デバイス（Management Center によって管理されているもの）から既存の構成を使用して作業します。所有している構成では、単にネットワーク内

のこの特定のデバイスの場所に応じて IP アドレス、インターフェイス名などの変数を変更して、テンプレートをそれに適合させる必要があります。

テンプレートへの入力に関するいくつかのヒントを次に示します。

- 変数の値を選択するには、変数のいずれかをクリックして適切な値を入力するか、リストから選択します（値が列挙されている場合）。入力を必要とする変数をマウスオーバーすると、数値の範囲など、オプションの有効な値が表示されます。一部のケースでは推奨値が記載されています。

  たとえば、OSPF のテンプレートでは、必要なコマンドの **router ospf** *process-id* をマウスオーバーすると「Process ID (1-65535)」と表示され、*process-id* をクリックするとフィールドが強調表示されます。単に希望の数値を入力します。

- 変数のオプションを選択するときに、オプションを構成するために使用できる追加のコマンドがある場合、それらが自動的に公開され必要に応じて有効または無効になります。これらの追加のコマンドを確認します。

- テンプレート上の [表示（Show）] /[無効を非表示（Hide Disabled）] リンクを使用してビューを制御します。無効なコマンドは構成されませんが、それらを表示して構成する必要があります。完全なテンプレートを表示するには、テンプレート上の[無効を表示（Show Disabled）] リンクをクリックします。構成されるコマンドのみを表示するには、テーブルの上の [無効を非表示（Hide Disabled）] リンクをクリックします。

- オブジェクトを最後に保存して以降のすべての編集をクリアするには、テンプレートの上の [リセット（Reset）] リンクをクリックします。

- オプションのコマンドを有効にするには、行番号の左側にある [+] のボタンをクリックします。

- オプションのコマンドを無効にするには、行番号の左側にある [-] のボタンをクリックします。行を編集した場合、編集内容は削除されません。

- コマンドを複製するには、[オプション...（Options...）] ボタンをクリックして [複製（Duplicate）] を選択します。コマンドを複数回入力することが有効な場合にのみ、コマンドを複製できます。

- 複製したコマンドを削除するには、[オプション...（Options...）] ボタンをクリックして [削除（Delete）] を選択します。ベース テンプレートの一部であるコマンドは削除できません。

ステップ 7 [OK] をクリックします。

FlexConfig ポリシーの設定

FlexConfig ポリシーは単にデバイスの構成に展開する FlexConfig オブジェクトのリストです。ポリシーに含まれるこれらのオブジェクトのみが展開され、他はすべてが単に定義されるだけで使用されません。

FlexConfig オブジェクトで定義されているコマンドは、Smart CLI を含む Device Manager で定義された機能のすべてのコマンドの後に展開されます。したがって、デバイスに対してこれらのコマンドが発行される前に設定されているオブジェクト、インターフェイスなどに依存する場合があります。Smart CLI テンプレートで FlexConfig が展開された項目を使用する必要がある場合は、Smart CLI テンプレートを作成して展開する前に FlexConfig を作成して展開します。たとえば、OSPF Smart CLI テンプレートを使用して EIGRP ルートを再配布する場合は、最初に FlexConfig を使用して EIGRP を設定し、それから OSPF Smart CLI テンプレートを作成します。

（注） 機能の Smart CLI テンプレートがある場合、FlexConfig を使用してそれを構成できません。Smart CLI オブジェクトを使用する必要があります。

始める前に

FlexConfig オブジェクトを作成します。次のトピックを参照してください。

- FlexConfig オブジェクトの設定 （1044 ページ）
- FlexConfig オブジェクトの変数の作成 （1047 ページ）
- 秘密キー オブジェクトの設定 （1056 ページ）

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigポリシー（FlexConfig Policy）]** をクリックします。

ステップ 3 [グループリスト（Group List）] 内のオブジェクトのリストを管理します。

- オブジェクトを追加するには、[+] ボタンをクリックします。オブジェクトがまだ存在しない場合は、[新規FlexConfigオブジェクトを作成（Create New FlexConfig Object）] をクリックして定義します。
- オブジェクトを削除するには、オブジェクトエントリの右側にある [X] ボタンをクリックします。

（注） 各オブジェクトは完全に自己完結型で、他の FlexConfig オブジェクトで定義されている構成に依存しないことをお勧めします。これにより、他のオブジェクトに影響を与えずにオブジェクトを追加または削除できます。

ステップ 4 [プレビュー（Preview）] ペインで提案されたコマンドを評価します。

[展開（Expand）] ボタン（その後 [折りたたむ（Collapse）]）をクリックすると画面を拡大できます。これにより長いコマンドがより見やすくなります。

プレビューは、変数を評価し、発行される正確なコマンドを生成します。これらのコマンドが正しく有効なことを確認します。コマンドがエラーを生じたり、デバイスが使用できなくなる不適切な構成でないことを確保する責任があります。

注意 システムはコマンドを検証しません。無効なコマンドや、破壊の可能性があるコマンドも展開が可能です。変更を展開する前に慎重にプレビューを確認します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

FlexConfig ポリシーを編集した後は、次の展開の結果を慎重に調べてください。エラーがある場合は、オブジェクトの CLI を修正します。FlexConfig ポリシーのトラブルシューティング（1057 ページ） を参照してください。

FlexConfig オブジェクトの設定

FlexConfig オブジェクトには、別の方法では Device Manager を使用して設定できない特定の機能を設定するために必要な ASA コマンドが含まれます。コマンドのシーケンスは、入力ミスなく正しく入力する必要があります。システムは、FlexConfig オブジェクトの内容を検証しません。

設定する一般的な機能ごとに別のオブジェクトを作成することをお勧めします。たとえば、バナーを定義し、RIP ルーティング プロトコルも設定する場合は、2 つの独立したオブジェクトを使用します。機能を別のオブジェクトに分離すると、展開するオブジェクトの選択が容易になり、またトラブルシューティングも容易になります。

（注） **enable** および **configure terminal** コマンドは含めないでください。システムは、自動的にコンフィギュレーション コマンドに適切なモードに入ります。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 5 [変数（Variables）] セクションで、オブジェクト本文内で使用する変数を作成します。

作成する必要がある唯一の変数は Device Manager 内で定義されているオブジェクトを指すもので、具体的にはネットワーク、ポート、および秘密キーの変数の型、または名前付きインターフェイスを指すインターフェイス変数です。他の変数の型では、単にオブジェクト本文に値を入力できます。

変数の作成と使用の詳細については、FlexConfig オブジェクトの変数の作成 （1047 ページ）を参照してください。

ステップ 6 [テンプレート（Template）] セクションに、機能を設定するために必要な ASA コマンドを入力します。

機能を設定するために正しい順序でコマンドを入力する必要があります。ASA CLI 構成ガイドを使用して、コマンドを入力する方法を学習します。理想的には、ASA または参照として使用できる別の 脅威に対する防御 デバイスから事前テスト済みの構成ファイルを取得します。

変数を参照および処理するために Mustache 表記を使用することもできます。詳細については、FlexConfig 変数の参照と値の取得 （1048 ページ）を参照してください。

オブジェクト本文を作成するためのいくつかのヒントを次に示します。

- 行を追加するには、行の末尾にカーソルを置いて、Enter キーを押します。
- 変数を使用するには、二重括弧に間に変数名を入力します：{{変数名}}。オブジェクトを参照する変数では、取得する値の属性を含める必要があります：{{変数名.属性}}。使用可能な属性は、オブジェクト タイプによって異なります。詳細については、変数参照：{{variable}} または {{{variable}}} （1048 ページ）を参照してください。
- Smart CLI オブジェクトを使用するには、オブジェクト名を入力します。Smart CLI に設定されているルーティング プロセスを参照する必要がある場合は、プロセス ID を入力します。FlexConfig オブジェクト内の Smart CLI オブジェクトの参照 （1054 ページ）を参照してください。
- テンプレート本体の上の [展開する/折りたたむ（Expand/Collapse）] リンクをクリックして、本体を大きくまたは小さくします。
- [リセット（Reset）] リンクをクリックして、オブジェクトを最後に保存した後に行ったすべての変更を消去します。

ステップ 7 [ネゲートテンプレート（Negate Template）] セクションに、オブジェクト本体で設定したコマンドを削除または入れ替えるために必要なコマンドを入力します。

ネゲート セクションは非常に重要であり、2 つの目的を果たします。

- 展開を簡単にします。本体でコマンドを再展開する前に、最初に設定を消去したり元に戻すためにこれらのコマンドを使用します。これにより正常に展開されます。
- FlexConfig ポリシーからオブジェクトを削除することによって機能を削除する場合、システムはデバイスからコマンドを削除するためにこれらのコマンドを使用します。

オブジェクト本体内でCLIをネゲートまたは入れ替えるために必要なコマンドを指定しない場合、展開ではデバイス全体の構成をクリアし、オブジェクト内のコマンドだけではなく、すべてのポリシーを再展開する必要があります。これにより展開にかかる時間が長くなり、またトラフィックが中断されます。オブジェクト本体で定義されている構成を元に戻すために必要なこれらのコマンドがすべてあり、これだけであることを確認します。negate コマンドは通常、テンプレートで**no**形式または**clear**形式のコマンドになりますが、有効だった機能を実際にオフする場合、「negate」コマンドは実際には機能を有効にする正形式のコマンドになります。

ASA 構成ガイドとコマンド リファレンスを使用して、適切なコマンドを判断します。場合によっては、単一のコマンドで設定を元に戻すことができます。たとえば、RIP を構成するオブジェクトでは、単純な **no router rip** コマンドで、サブコマンドを含めた **router rip** 構成全体を削除します。

同様に、複数行のバナーを作成するために **banner login** コマンドをいくつかを入力した場合、単一の **no banner login** コマンドでログインバナー全体が無効になります。

テンプレートで複数のネストされたオブジェクトを作成する場合、ネゲートテンプレートでは逆の順番でオブジェクトを削除する必要があります（つまり、オブジェクトを削除する前にオブジェクトへの参照を最初に削除します）。たとえば、まず ACL を作成して、トラフィック クラスで ACL を参照し、ポリシー マップでトラフィック クラスを参照し、最後にサービス ポリシーを使用してポリシー マップを有効にする場合、ネゲート テンプレートではまずサービス ポリシーを削除してからポリシー マップ、トラフィック クラス、最後に ACL の順で削除して、設定を元に戻す必要があります。

ステップ 8 [OK] をクリックします。

次のタスク

単に FlexConfig オブジェクトを作成するだけでは、それを展開するのには十分ではありません。オブジェクトを FlexConfig ポリシーに追加する必要があります。FlexConfig ポリシー内のこれらのオブジェクトのみ展開されます。これにより FlexConfig オブジェクトの改善が可能になり、すべてが自動的に展開されるのではなくいくつかは特別な用途のために利用可能になります。FlexConfig ポリシーの設定 （1043 ページ） を参照してください。

FlexConfig オブジェクトの変数の作成

FlexConfig オブジェクト内部で使用する変数は、オブジェクト自体の内部で定義されます。変数の個別のリストはありません。したがって、変数を定義して個別の FlexConfig オブジェクト内で使用することはできません。

変数はこれらの主な利点を提供します。

- Device Manager を使用して定義されているオブジェクトを指し示すことを可能にします。これには、ネットワーク、ポート、および秘密鍵オブジェクトが含まれます。
- これらは変更する可能性がある値をオブジェクト本体から分離します。したがって、値を変更する場合は単に変数を編集します。オブジェクト本体を編集する必要はありません。これは、いくつかのコマンドライン内のオブジェクトを参照する必要がある場合に特に便利です。

この手順では、FlexConfig オブジェクトに変数を追加するプロセスについて説明します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページから FlexConfig オブジェクトを編集または作成します。

「FlexConfig オブジェクトの設定 （1044 ページ）」を参照してください。

ステップ 2 [変数（Variables）] セクションで次のいずれかを実行します。

- 変数を追加するには、[+] ボタンをクリックします（またはまだ定義されていない場合は [変数の追加（Add Variable）] をクリックします）。
- 変数を編集するには、その変数の編集アイコン（  ）をクリックします。

変数を削除するには、その変数のごみ箱アイコン（  ）をクリックします。その変数への参照をテンプレート本体から削除していることを確認します。

ステップ 3 変数の名前を入力し、任意で説明を入力します。

ステップ 4 変数のデータの [タイプ（Type）] を選択し、値を入力または選択します。

次のタイプの変数を作成できます。変数を使用するコマンドのデータ要件に適合するタイプを選択します。

- [文字列（String）]：テキスト文字列です。 たとえば、ホスト名、ユーザ名など。
- [数値（Numeric）]：整数値です。 コンマ、小数、（マイナスなどの）記号または 16 進数表記を含めないでください。非整数の場合は文字列変数を使用します。
- [ブール値（Boolean）]：論理的 true/false です。 True または False を選択します。

- [ネットワーク（Network）]：[オブジェクト（Objects）] ページで定義されているネットワーク オブジェクトやグループです。ネットワーク オブジェクトまたはグループを選択します。
- [ポート（Port）]：[オブジェクト（Objects）] ページで定義されている TCP または UDP ポート オブジェクトです。ポート オブジェクトを選択します。グループやその他のプロトコル用のオブジェクトは選択できません。
- [インターフェイス（Interface）]：[デバイス（Device）]>[インターフェイス（Interfaces）] のページで定義されている名前付きインターフェイスです。インターフェイスを選択します。名前を持たないインターフェイスは選択できません。
- [IP]：ネットマスクまたはプレフィックス長がない単一の IPv4 または IPv6 IP アドレスです。
- [秘密（Secret）]：FlexConfig に定義された秘密キー オブジェクトです。オブジェクトを選択します。秘密キー オブジェクトの作成の詳細については、秘密キー オブジェクトの設定 （1056 ページ）を参照してください。

ステップ 5 [変数（Variable）] ダイアログ ボックスで [追加（Add）] または [保存（Save）] をクリックします。

これで FlexConfig オブジェクトの本体内の変数を使用できます。変数を参照する方法は、変数のタイプによって異なります。これらの変数の使用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。

- 変数参照：{{variable}} または {{{variable}}} （1048 ページ）
- セクション {{#key}} {{/key}} と逆セクション {{^key}} {{/key}} （1052 ページ）

ステップ 6 [FlexConfigオブジェクト（FlexConfig Object）] ダイアログボックスで [OK] をクリックします。

FlexConfig 変数の参照と値の取得

FlexConfig はテンプレート言語として Mustache を使用しますが、サポートは、次のセクションで説明する機能に限定されます。これらの機能を使用して、変数を参照し、その値を取得して、処理します。

変数参照：{{variable}} または {{{variable}}}

FlexConfig オブジェクト内で定義した変数を参照するには、次の表記を使用します。

{{*variable_name*}}

または

{{{*variable_name*}}}

次の種類の変数を含む、単一値の変数の場合はこれで十分です：[数値（Numeric）]、[文字列（String）]、[ブール値（Boolean）]、[IP]。変数に & などの特殊文字が含まれている場合、三重カッコを使用します。または、すべての変数で常に三重カッコを使用することもできます。

ただし、構成データベース内のオブジェクトとしてモデル化される要素を指し示す変数の場合は、ドット表記を使用し、取得するオブジェクト属性の名前を含める必要があります。関連するオブジェクト タイプの API エクスプローラでのモデルを調べることによって、これらの属性名を確認できます。次の種類の変数を使用するには次の標記を使用する必要があります：[秘密（Secret）]、[ネットワーク（Network）]、[ポート（Port）]、[インターフェイス（Interface）]。

{{*variable_name.attribute*}}

たとえば、net-object1（ネットワーク グループではなく、ネットワーク オブジェクトを示す）という名前のネットワーク変数のアドレスを取得するには、次を使用します。

{{net-object1.value}}

オブジェクト内のオブジェクトから属性値を取得しようとする場合は、一連のドット区切りの属性を使用して、目的の値にドリルダウンする必要があります。たとえば、インターフェイスの IP アドレスは、ipv4 と ipv6 という名前のサブオブジェクトとして、インターフェイス オブジェクトにモデル化されます。したがって、int-inside という名前の（内部インターフェイスを示す）インターフェイス変数の IPv4 アドレスとサブネット マスクを取得するには、次を使用します。

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

（注） API エクスプローラを開くには、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

次の表に、変数の型とそれらを参照する方法、オブジェクトの場合は、API モデルの名前と使用する可能性が高い参照を示します。

変数の型	参照モデル	説明
ブール値 （単純変数）	**変数**： {{*variable_name*}} **セクション**： {{#*variable_name*}} commands {{/*variable_name*}} **反転セクション**： {{^*variable_name*}} commands {{/*variable_name*}}	論理的 true/false。ブール変数の主な目的は、セクションまたは反転セクションです。たとえば、定期的にまたは特別な事情の下でのみ機能を有効にする必要がある場合、ブール変数の値を編集してコマンドのセクションをオンまたはオフにできます。 いくつかのオブジェクトにも、セクションのオプションの処理を提供するために使用できるそれらのモデルのブール型の属性があります。

変数の型	参照モデル	説明
インターフェイス （オブジェクト変数：API モデルはインターフェイスです）	**変数**： {{*variable_name*.*attribute*}} **セクション**： {{#*variable_name.attribute*}} commands {{/*variable_name.attribute*}} **反転セクション**： {{^*variable_name.attribute*}} commands {{/*variable_name.attribute*}}	[デバイス（Device）] > [インターフェイス（Interfaces）] のページで定義されている名前付きインターフェイス。無名のインターフェイスを指定することはできません。 インターフェイス モデルで使用できるさまざまな属性があります。またインターフェイス モデルには、サブオブジェクト、たとえば IP アドレスが含まれます。 次に、役に立つ主な属性をいくつか示します。 • *variable_name*.**name** はインターフェイスの論理名を返します。 • *variable_name*.**hardwareName** は GigabitEthernet1/8 などのインターフェイスポート名を返します。 • *variable_name*.**managementOnly** はブール値です。TRUE は、インターフェイスが管理限定として定義されていることを意味します。FALSE は、インターフェイスがデバイスを通過するトラフィックに使用されることを意味します。このオプションは、セクション キーとして使用できます。 • *variable_name*.**ipv4.ipAddress.ipAddress** はインターフェイスの IPv4 アドレスを返します。 • *variable_name*.**ipv4.ipAddress.netmask** はインターフェイスの IPv4 アドレスのサブネットマスクを返します。
IP （単純変数）	**変数**： {{*variable_name*}}	ネットマスクまたはプレフィックス長がない単一の IPv4 または IPv6 IP アドレス。

変数の型	参照モデル	説明
ネットワーク （オブジェクト変数：API モデルは NetworkObject です）	**変数（ネットワークオブジェクト）**： {{*variable_name.attribute*}} **セクション（グループオブジェクト）**： {{#*variable_name*.**networkObjects**}} commands referring to one of {{**value**}} {{**name**}} {{/*variable_name*.**networkObjects**}}	[オブジェクト（Objects）]ページで定義されているネットワーク オブジェクトやグループです。セクションを使用してネットワーク グループを処理できます。 次に、役に立つ主な属性を示します。 • {{*variable_name*.**name**}} はネットワークオブジェクトまたはグループの名前を返します。 • {{*variable_name*.**value**}} はネットワークオブジェクト（ネットワークグループではありません）の IP アドレスの内容を返します。ネットワーク オブジェクトの持つ内容のタイプが指定されたコマンドに対して正しいことを確認します。たとえば、サブネット アドレスではなくホスト アドレスです。 • {{*variable_name*.**groups**}} はネットワークグループに含まれるネットワークオブジェクトのリストを返します。これはネットワーク グループを指す変数でのみ使用します。またグループの内容を繰り返し処理するセクション タグに使用します。{{**value**}} または {{**name**}} のいずれかを使用して、次に各ネットワークオブジェクトの内容を取得します。
数値 （単純変数）	**変数**： {{*variable_name*}}	整数値。コンマ、小数、（マイナスなどの）記号または 16 進数表記を含めないでください。非整数の場合は文字列変数を使用します。
ポート （オブジェクト変数：API モデルは、PortObject、tcpports または udpports です）	**変数**： {{*variable_name.attribute*}}	[オブジェクト（Objects）] ページで定義されている TCP または UDP ポート オブジェクトです。これは、ポート グループではなく、ポート オブジェクトである必要があります。 次に、役に立つ主な属性を示します。 • {{*variable_name*.**port**}} はポート番号を返します。プロトコルは含まれません。 • {{*variable_name*.**name**}} はポートオブジェクトの名前を返します。
秘密（Secret） （オブジェクト変数：API モデルは Secret です）	**変数**： {{*variable_name*.**password**}} または {{{*variable_name*.**password**}}}	FlexConfig に定義された秘密キー オブジェクトです。 参照する必要があるのは、暗号化された文字列を返す **password** 属性のみです。 パスワードに & などの特殊文字が含まれている場合、三重カッコを使用します。

変数の型	参照モデル	説明
文字列 （単純変数）	**変数**： {{*variable_name*}}	テキスト文字列です。たとえば、ホスト名、ユーザー名など。

セクション{{#key}}{{/key}}と逆セクション{{^key}}{{/key}}

セクションまたは逆セクションは、セクションの開始タグと終了タグの間のコマンドのブロックで、処理条件としてキーを使用します。セクションの処理方法は、それが通常か逆セクションかによって異なります。

- 通常のセクション（または単にセクション）は、キーがTRUEであるか、または空でないコンテンツを含む場合に処理されます。キーがFALSEであるか、またはオブジェクトにコンテンツがない場合、セクション内のコマンドは設定されません。セクションはバイパスされます。

  次に、通常のセクションの構文を示します。

```
{{#key}}
one or more commands
{{/key}}
```

- 逆セクションは、セクションの反対です。キーがFALSEであるか、またはオブジェクトに内容がない場合に処理されます。キーがTRUEであるか、またはオブジェクトにコンテンツがある場合、逆セクションはバイパスされます。

  次に、逆セクションの構文を示します。唯一の違いは、キャレットがハッシュタグを置き換えることです。

```
{{^key}}
one or more commands
{{/key}}
```

次のトピックで、セクションおよび逆セクションの主な用途について説明します。

複数値の変数を処理する方法

複数値の変数の処理の主な例は、ネットワークグループを指すネットワーク変数です。グループに複数のオブジェクトが含まれている（**objects**属性の下）ので、ネットワークグループ内の値を繰り返し実行し、異なる値を使用して複数回同じコマンドを設定できます。

オブジェクトグループによってオブジェクトの属性に含まれるネットワークオブジェクトが定義されますが、ネットワークオブジェクトの内容はオブジェクトに含まれていません。代わりに、**networkObjects**属性を使用してネットワークオブジェクトの内容を取得します。

たとえば、ホスト192.168.30.0、192.168.20.0、192.168.10.0を含むnet-groupという名前のネットワーク グループがある場合は、次の方法を使用して、RIPルーティング用の各アドレスにネットワーク コマンドを設定できます。ネットワークオブジェクトの**value**属性のみを使用す

ることに注意してください。セクションの開始時に **net-group.networkObjects** を使用すると、属性値がメンバオブジェクトから取得されるためです。（FlexConfigオブジェクト内の「value」属性に個別の変数を作成しないでください）。

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

システムはセクションの構造を次のように変換します。

```
router rip
   network 192.168.10.0
   network 192.168.20.0
   network 192.168.30.0
```

ブール値または空のオブジェクトに基づいて省略可能な処理を実行する方法

（注） このトピックの例は、説明のみを目的としたものです。たとえば、FlexConfig を使用してバージョン 6.7 以降の SNMP を設定することはできません。代わりに Threat Defense API SNMP リソースを使用する必要があります。

セクションの開始タグ内の変数のコンテンツがTRUEの場合、またはオブジェクトが空でない場合、セクションは処理されます。ブール値が FALSE または空（空のオブジェクトなど）のセクションは省略されます。

ここでの主な用途はブール値用です。たとえば、ブール変数を作成し、変数の対象であるセクション内にコマンドを置きます。その後、FlexConfig オブジェクト内のコマンドのセクションを有効または無効にする必要がある場合、ブール変数の値を変更する必要があるだけで、これらの行をコードから削除する必要はありません。これにより、簡単に、機能を有効または無効にできます。

たとえば、SNMP を有効にする FlexConfig を使用する場合、SNMP トラップをオフにできます。enable-traps という名前のブール変数を作成し、最初はTRUEに設定します。次に、トラップをオフにする場合、変数を編集して FALSE に変更し、オブジェクトを保存して、設定を再展開するだけです。コマンド シーケンスは次のようになります。

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

オブジェクト内のブール値に基づいてこのタイプの処理を行うこともできます。たとえば、そこでいくつかの特性を設定する前に、インターフェイスが管理専用かどうかをチェックできます。次の例で、int-inside は inside という名前のインターフェイスを指すインターフェイス変数です。インターフェイスが管理専用に設定されていない場合にのみ、FlexConfig はそのイン

ターフェイスで EIGRP 関連のインターフェイス オプションを設定します。ブール値が FALSE の場合にのみコマンドが設定されるように、逆セクションを使用します。

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

FlexConfig オブジェクト内の Smart CLI オブジェクトの参照

FlexConfig オブジェクトを作成する場合、変数を使用して、Device Manager 内で設定可能なオブジェクトを示すことができます。たとえば、インターフェイス要素やネットワーク オブジェクトを示す変数を作成できます。

ただし、同じ方法で Smart CLI オブジェクトを示すことはできません。

代わりに、FlexConfig ポリシーで使用する必要がある Smart CLI オブジェクトを作成する場合は、適切な場所で Smart CLI オブジェクトの名前を単純に入力します。

たとえば、プロトコル インスペクションを設定する場合、トラフィック クラスとして、拡張アクセス リストを使用することがあります。これは、拡張アクセスリストの Smart CLI オブジェクトが存在するため、Smart CLI オブジェクトを使用して ACL を作成する必要があるためです。FlexConfig オブジェクトで **access-list** コマンドを使用することはできません。

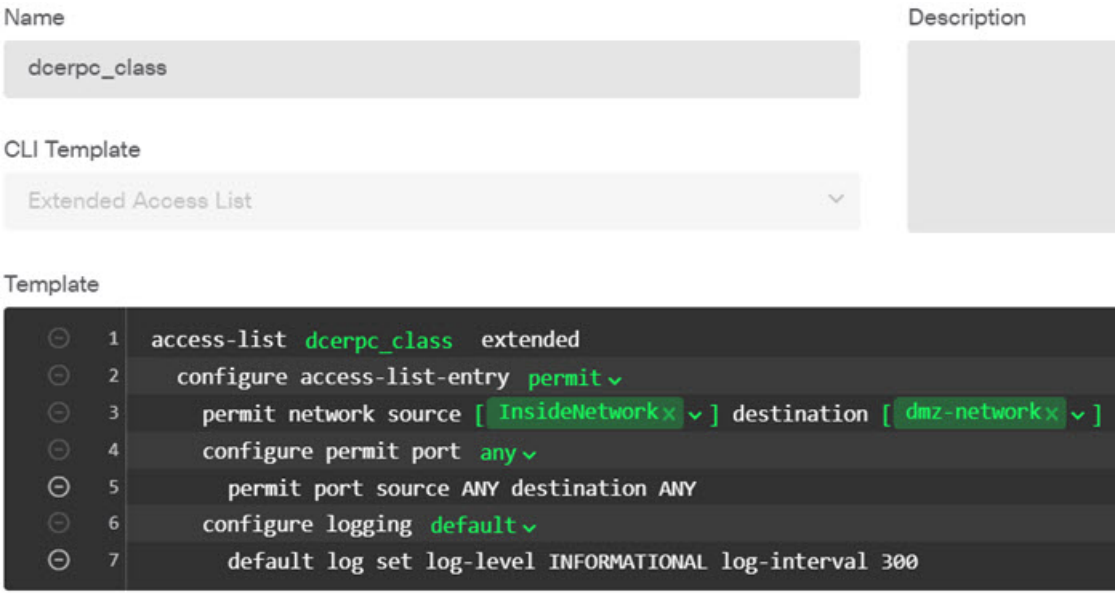
たとえば、192.168.1.0/24 および 192.168.2.0/24 ネットワーク間でグローバルに DCERPC インスペクションを有効化する場合は、次の手順を実行します。

手順

ステップ 1 2つのネットワークに個別のネットワーク オブジェクトを作成します。たとえば、InsideNetwork と dmz-network。

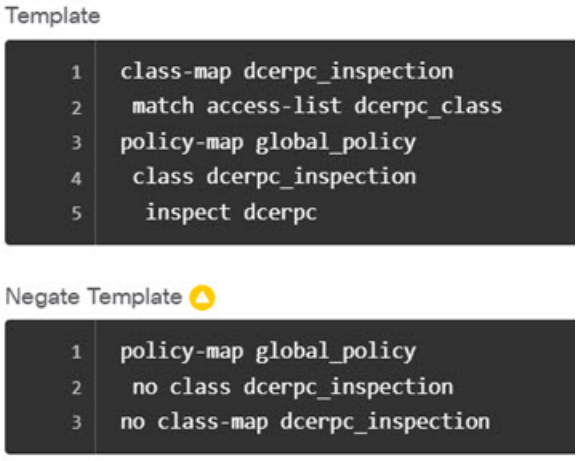
ステップ 2 これらのオブジェクトを Smart CLI 拡張アクセス リスト オブジェクトで使用します。

詳細設定



ステップ 3 名前で Smart CLI オブジェクトを示す FlexConfig オブジェクトを作成します。

たとえば、オブジェクトの名前が「dcerpc_class」の場合、FlexConfig オブジェクトは次のようになります。ネゲートテンプレートでは、Smart CLI オブジェクトから作成したアクセス リストは無効にできない点に注意してください。そのオブジェクトは、実際には FlexConfig から作成されたオブジェクトではないためです。



ステップ 4 オブジェクトを FlexConfig ポリシーに追加します。

秘密キー オブジェクトの設定

秘密キー オブジェクトのポイントは、パスワードや機密性の高い文字列を隠すことです。FlexConfig オブジェクトまたは Smart CLI テンプレートで使用される文字列を誰かに見られるリスクを避けたい場合は、文字列の秘密キー オブジェクトを作成します。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、コンテンツ テーブルから [秘密キー（Secret Keys）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [パスワード（Password）] と [パスワードの確認（Confirm Password）] フィールドの両方にパスワードまたはその他秘密の文字列を入力します。

入力すると、システムがテキストを隠します。

ステップ 5 [OK] をクリックします。

次のタスク

- 新しいオブジェクトの場合は、FlexConfig でそれを使用するために、FlexConfig オブジェクトを編集し、秘密キーの型の変数を作成してオブジェクトを選択します。その後、オブジェクト本体内で変数を参照します。詳細については、FlexConfig オブジェクトの変数の作成 （1047 ページ）を参照してください。
- FlexConfig ポリシーの一部である FlexConfig オブジェクトで使用されている既存のオブジェクトを編集する場合は、新しい文字列でデバイスを更新するために構成を展開する必要があります。
- Smart CLI テンプレートでは、コマンドに秘密キーが必要な場合、関連するプロパティを編集するときにこれらのオブジェクトの一覧が表示されます。目的にあわせて適切なキーを選択します。

FlexConfig ポリシーのトラブルシューティング

FlexConfig ポリシーを編集した後は、次の展開の結果を慎重に調べてください。[保留中の変更（Pending Changes）] ダイアログボックスに「最後の展開は失敗しました（Last Deployment Failed）」というメッセージが表示された場合は、[詳細の表示（See Details）] リンクをクリックします。リンクから監査ログが表示されます。このログで失敗した展開ジョブを確認できます。特定のエラー メッセージを検索するには、ジョブを開きます。

展開が FlexConfig の問題のため失敗した場合、詳細には不正なコマンドを含む FlexConfig オブジェクトについて記述され、失敗したコマンドが表示されます。この情報を使用して、オブジェクトを修正し、もう一度展開を試みてください。オブジェクト名はリンクであり、クリックしてオブジェクトの編集のダイアログを開きます。

たとえば、最大 TCP セグメント サイズ（TCP MSS）を設定できます。この設定は、**sysopt connection tcpmss** コマンドを使用して制御できます。Device Manager により設定する場合、このオプションに対する Threat Defense のデフォルトは 0 で、ASA のデフォルトは 1380 です。

MTU のデフォルトの 1500 を使用するインターフェイスで IPv4 VPN を実行している場合、ASA のデフォルトは処理を最適化するように設計されています。システムでは、VPN のヘッダーに 120 バイトが必要です。IPv6 の場合、システムでは 140 バイト必要です。Threat Defense のデフォルトの 0 では、エンドポイントによる MSS のネゴシエートが許可されるだけで、これは通常のトラフィック、特にデバイス上のインターフェイス間で、1500 以上の MTU を含む、異なる MTU を使用する場合には理想的な設定です。TCP の MSS はグローバル設定であり、インターフェイスごとに設定されないので、トラフィックのかなりの割合が VPN を介すものであり、過剰に断片化している場合のみ変更します。その場合は、TCP の MSS を MTU マイナス 120（IPv4 用）または 140（IPv6 用）に設定し、すべてのインターフェイスに同じ MTU を使用します。MSS を明示的に設定した場合でも、TLS/SSL 復号やサーバー検出などのコンポーネントが特定の MSS を必要とする場合、その MSS はインターフェイス MTU に基づいて設定され、MSS 設定は無視されます。

この図では、TCP の MSS を 3 バイトに設定するとします。コマンドは最小値として 48 バイトを取るので、次のような展開エラーが発生します。

エラーは、これらの要素で構成されます。

1. エラーが発生した FlexConfig オブジェクトの名前が含まれている展開エラー メッセージ。オブジェクト名は編集ダイアログ ボックスにリンクされているので、オブジェクトを開いてすぐにエラーを修正できます。これはメッセージの最初の文です。
2. 「ERROR:」から始まるテキストがデバイスから返されるメッセージです。これは SSH クライアントの書式なしで、誤ったコマンドで入力した場合の、ASA の正確な応答内容です。この例では、エラー メッセージは「エラー：[3] は RFC 791 で 許可されている MSS

の最小値 48 よりも小さいです。（ERROR: [3] is smaller than the minimum allowed MSS of 48 by RFC 791.）」です。「Config Error」で始まるテキストが、エラー メッセージを生成した特定の行を示しています。

3. 黒のテキストは、エラーを引き起こした FlexConfig オブジェクトからの実際の行です。この行を修正する必要があります。この例では、MTU 1500 インターフェイス（共通の状態）上の IPv4 VPN トラフィックに対応しようとする場合、3 を 1380 に変更します。

   この例を修正する場合、CLI コンソールを開いたままにし、**show running-config all sysopt** を使用して、**sysopt** コマンドのすべての設定を確認できます。ほとんどの **sysopt** コマンドには大部分の用途に適したデフォルトの設定があり、実行コンフィギュレーションには表示されません。**all** キーワードでは、出力にこれらのデフォルト設定が含まれます。

FlexConfig の例

ここでは、FlexConfig を使用して機能を設定するいくつかの例を示します。

グローバル デフォルト インスペクションを有効/無効にする方法

一部のプロトコルでは、IP アドレッシング情報がユーザ データ パケットに埋め込まれるか、動的に割り当てられたポートにセカンダリ チャネルが開かれます。そのようなプロトコルの場合、システムはディープ パケット インスペクションを実行し、NAT を適用して、セカンダリ チャネルを許可できるようにする必要があります。いくつかの一般的なインスペクション エンジンはデフォルトで有効になっていますが、ネットワークによっては、他のインスペクション エンジンを有効化したり、デフォルトのインスペクションを無効化したりする必要があります。

現在有効になっているインスペクションの一覧を表示するには、CLI コンソールまたは SSH セッションで **show running-config policy-map** コマンドを使用します。以下の出力は、インスペクションの設定に変更が加えられていないシステムで表示される内容です。この出力では、出力の最後にある **inspect** コマンドの一覧に有効になっているプロトコルインスペクションが表示されています。先行するコマンドにより、inspection_default トラフィック クラスでこれらのインスペクションが有効になります（通常のプロトコル、該当する場合はインスペクション済みプロトコルのポート番号）。このクラスは global_policy ポリシー マップの一部で、service-policy コマンド（出力には未表示）を使用して、すべてのインターフェイスに対するインスペクションに適用されます。たとえば、ICMP インスペクションは、デバイスを通過するすべての ICMP トラフィックに対して行われます。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
```

```
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

（注） 各インスペクションの詳細については、https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html で入手可能な『*Cisco ASA Series Firewall Configuration Guide*』を参照してください。

次の手順では、このグローバルに適用されるデフォルト インスペクション クラスのインスペクションを有効化または無効化する方法を示します。説明のための例：

- PPTP（Point-to-Point Tunneling Protocol）を有効にします。このプロトコルは、エンドポイント間のポイントツーポイント接続のトンネリングに使用されます。
- SIP（Session Initiation Protocol）を無効にします。通常は、インスペクションによってネットワークに問題が発生している場合にのみSIPを無効化します。SIPを無効化する場合は、アクセス コントロール ポリシーで SIP トラフィック（UDP/TCP 5060）と動的に割り当てられるポートが許可されていること、SIP接続にNATのサポートが必要ないことを確認します。アクセス コントロール ポリシーと NAT ポリシーを、FlexConfig ではなく、標準のページを使用して適宜調整します。

始める前に

適切な計画を立てることでFlexConfigを効率的に使用できます。この例では、同じトラフィック クラスに変更を加えていますが、2つの異なる関連性のないインスペクションを変更しています。ただし、それらのポリシーを変更する必要がある場合（可能性は高い）は、個別に変更します。

そのため、この例のインスペクションごとに個別のFlexConfigオブジェクトを作成することをお勧めします。そうすることで、他のインスペクションを変更することなく、1 つのインスペクションの設定を簡単に変更でき、FlexConfig オブジェクトを編集する必要もありません。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 PPTP インスペクションを有効にするオブジェクトを作成します。

a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

b) オブジェクトの名前を入力します。例、**Enable_PPTP_Global_Inspection**。

c) [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

適切なサブモードでコマンドを有効にするために、ネゲートテンプレートに、親コマンドと同様にこれらのコマンドも含める必要があります。

FlexConfig ポリシーからこのオブジェクトを削除した場合（正常に導入された後）、および導入が失敗した場合でも（設定を前の状態にリセットするため）、ネゲートテンプレートが適用されます。

したがって、この例では、ネゲート テンプレートは次のようになります。

```
policy-map global_policy
 class inspection_default
  no inspect pptp
```

オブジェクトは次のようになります。

詳細設定

（注） Iinspection_default クラスには有効になっているその他のインスペクション コマンドがあるため、クラス全体を無効にはしたくありません。同様に、global_policy ポリシーマップにはその他のインスペクションが含まれているため、ポリシーマップも無効にはしたくありません。

e) [OK] をクリックしてオブジェクトを保存します。

ステップ 4 SIP 検査を無効にするオブジェクトを作成します。

a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

b) オブジェクトの名前を入力します。例、**Disable_SIP_Global_Inspection**。

c) [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

「no」コマンドを無効化するための「negate」コマンドは、機能を有効化するコマンドです。そのため、「ネゲート」テンプレートは機能を無効化するためだけのコマンドではな

く、「ポジティブ」テンプレートでの操作を元に戻すためのコマンドです。ネゲートテンプレートの要点は、変更を元に戻す点にあります。

したがって、この例では、ネゲート テンプレートは次のようになります。

```
policy-map global_policy
 class inspection_default
  inspect sip
```

オブジェクトは次のようになります。

e) [OK] をクリックしてオブジェクトを保存します。

ステップ 5 オブジェクトを FlexConfig ポリシーに追加します。

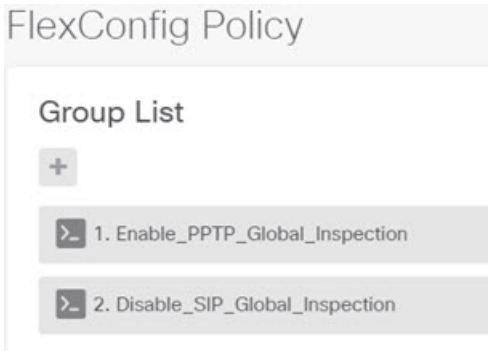
オブジェクトを作成するだけでは不十分です。オブジェクトは、FlexConfig ポリシーに追加（および変更を保存）した場合にのみ展開されます。これにより、未終了の作業で展開が失敗するリスクを犯すことなく、オブジェクトを試す（および部分的に完了した状態で残す）ことができます。その後、オブジェクトを追加および削除することで、機能を簡単にオン/オフできます。オブジェクトを毎回再作成する必要はありません。

a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。

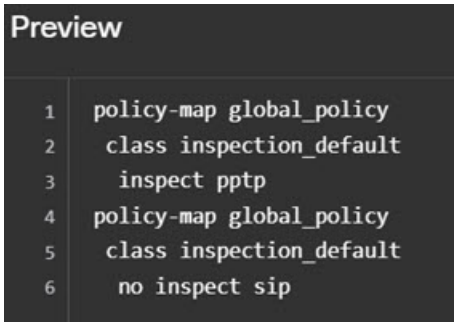
b) [グループリスト（Group List）] で [+] をクリックします。

c) Enable_PPTP_Global_Inspection オブジェクトと Disable_SIP_Global_Inspection オブジェクトを選択して、[OK] をクリックします。

グループ リストは次のようになります。



プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。



d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 6 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 7 CLI コンソールまたは SSH セッションで、**show running-config policy-map** コマンドを使用し、実行コンフィギュレーションが正しく変更されているか確認します。

次の出力では、**inspect pptp** が inspection_default クラスの最後に追加されていて、**inspect sip** はクラスに含まれていないことに注意してください。これにより、FlexConfig オブジェクトで定義された変更が正常に導入されたことが確認されます

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

FlexConfig の変更を元に戻す方法

FlexConfig オブジェクトに正しいネゲートテンプレートを入力すると、そのオブジェクトを使用して行った変更の削除が容易になります。FlexConfig ポリシーから単純にオブジェクトを削除すると、次の展開時に、システムがネゲートテンプレートを使用して変更を元に戻します。

変更を元に戻すために新しいオブジェクトを作成する必要はありません。

次の例は、グローバルな SIP 検査を再度有効にする方法を示しています。この例では、SIP 検査を無効化しているグローバルデフォルトインスペクションを有効/無効にする方法（1058ページ）で説明した変更を元に戻しています。

始める前に

FlexConfig オブジェクトにネゲートテンプレートが正しく設定されていることを確認します。正しくない場合は、オブジェクトを編集してネゲート テンプレートを修正します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigポリシー（FlexConfig Policy）]** をクリックします。

ステップ 3 FlexConfig ポリシーの **Disable_SIP_Global_Inspection** オブジェクトのエントリの右側にある [X] をクリックして、ポリシーから削除します。

オブジェクトのコマンドは、プレビューから削除されます。negate コマンドはプレビューには追加されず、バックグラウンドで実行されます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 6 CLI コンソールまたは SSH セッションで、**show running-config policy-map** コマンドを使用し、実行コンフィギュレーションが正しく変更されているか確認します。

次の出力では、**inspect sip** が inspection_default クラスの一番下に追加されていることに注意してください。これにより、FlexConfig オブジェクトで定義された変更が正常に導入されたことが確認されます（このクラスでは順序は重要ではないため、**inspect sip** が最後にあり、元の場所になくても問題ありません）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
```

!

一意のトラフィック クラスのインスペクションを有効にする方法

この例では、特定のインターフェイスの 2 つのエンドポイント間でトラフィックの PPTP インスペクションを有効にします。これは、エンドポイント間にポイントツーポイント トンネルが設定されているエンドポイントのインスペクションだけをターゲットにします。

2 つのエンドポイント間で PPTP インスペクションを有効にするために必要な CLI には、以下の内容が含まれます。

1. 送信元と宛先がエンドポイントのホストの IP アドレスに設定されている ACL。
2. この ACL を参照するトラフィック クラス。
3. トラフィック クラスを含み、そのトラフィック クラスでの PPTP インスペクションを有効にするポリシー マップ。
4. 目的のインターフェイスにポリシー マップを適用するサービス ポリシー。これは、実際にポリシーをアクティブにして、インスペクションを有効にする手順です。

（注） インスペクション関連のサービス ポリシーの詳細については、https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html で入手可能な『*Cisco ASA Series Firewall Configuration Guide*』を参照してください。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

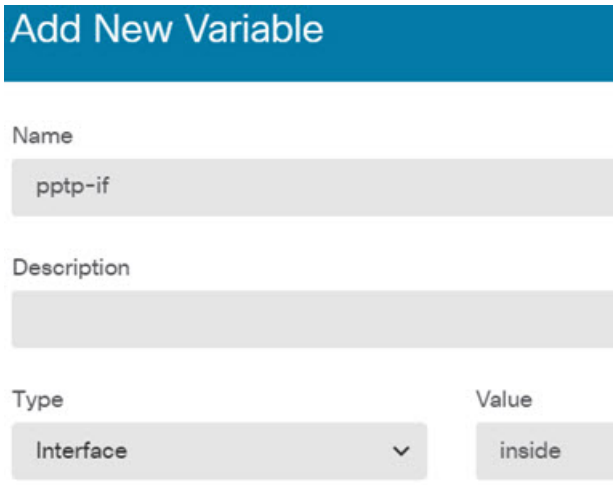
ステップ 3 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

ステップ 4 オブジェクトの名前を入力します。例、[Enable_PPTP_Inspection_on_Interface]。

ステップ 5 内部インターフェイスの変数を追加します。

a) [変数（Variables）] リストの上にある [+] をクリックします。
b) 変数の名前、[pptp-if] などを入力します。
c) [種類（Type）] で [インターフェイス（Interface）] を選択します。
d) [値（Value）] で [内部（inside）] インターフェイスを選択します。

ダイアログボックスは次のようになります。



e) [追加（Add）] をクリックします。

ステップ 6 [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

変数を使用するには、二重ブレースの間に変数名を入力する点に注意してください。また、インターフェイスを定義するオブジェクトには多数の属性が設定されているため、取得する属性を選択するにはドット表記法を使用する必要があります。インターフェイス名は「name」属性に保持されるため、[{{pptp-if.name}}] を入力すると、変数に割り当てられているインターフェイスの name 属性の値が取得されます。PPTP インスペクションのインターフェイスを変更する必要がある場合は、変数定義で単純に別のインターフェイスを選択する必要があります。

ステップ 7 [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

この例では、クラス マップ、ポリシー マップ、およびサービス ポリシーは、PPTP インスペクションを適用するためにのみ存在していると仮定しています。したがって、ネゲートテンプレートでこれらをすべて削除します。

ただし、インターフェイスの既存のサービス ポリシーに PPTP インスペクションを実際に追加する場合は、ポリシー マップやサービス ポリシーを無効にはしません。ポリシー マップからクラスを無効にするか、またはポリシーマップ内のクラス内でインスペクションを単純にオフにします。ネゲート テンプレートで予期せぬ結果が生じないようにするには、その他の FlexConfig オブジェクトに実装している内容について明確に把握する必要があります。

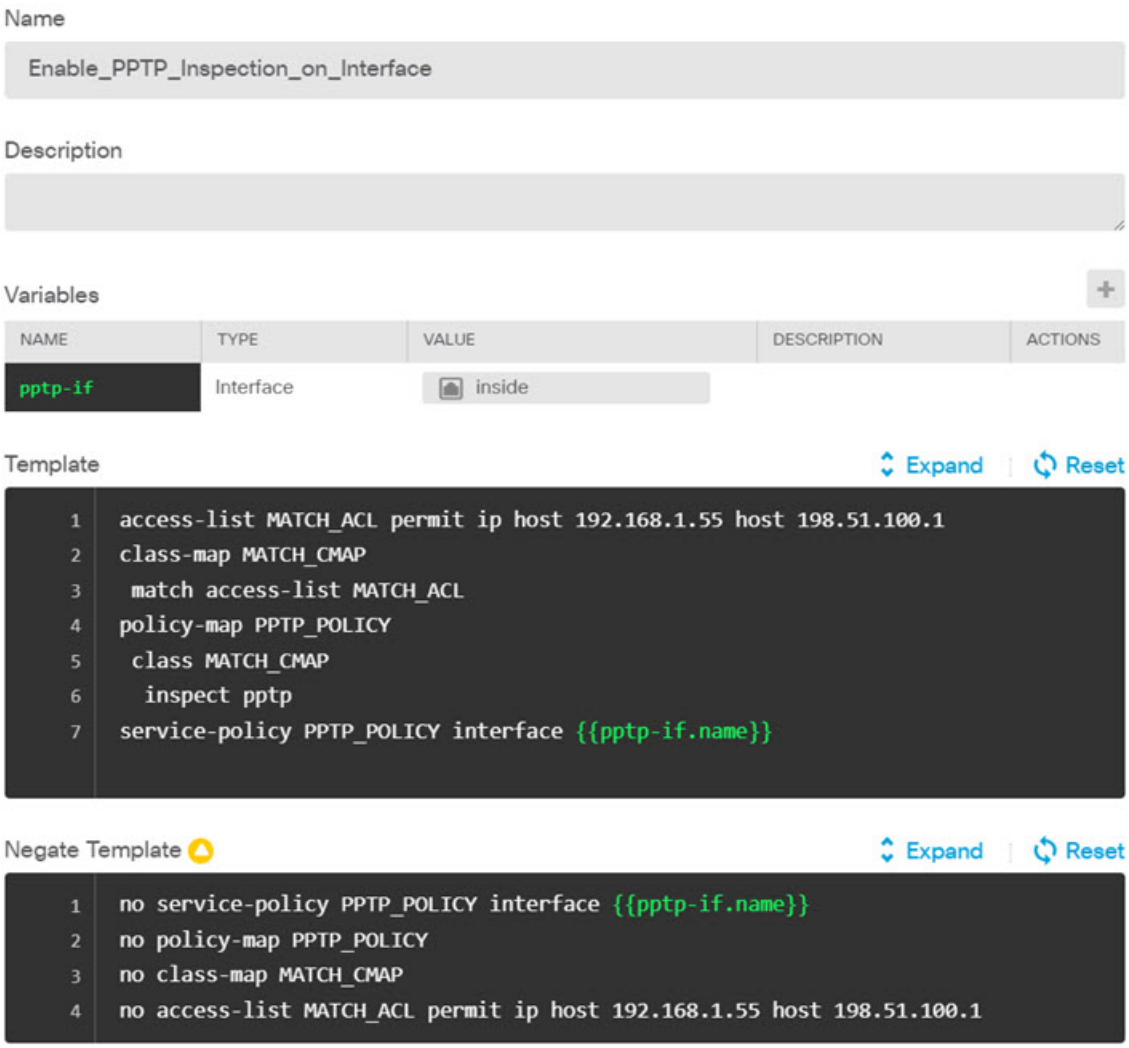
ネストされた項目を削除する場合は、作成順とは逆の順番で削除する必要があります。したがって、最初にサービス ポリシーを削除して、最後にアクセス リストを削除します。そうし

詳細設定

ないと、使用中のオブジェクトを削除しようとして、システムからエラーが返され、削除できなくなります。

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

オブジェクトは次のようになります。



ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ステップ 9 オブジェクトを FlexConfig ポリシーに追加します。

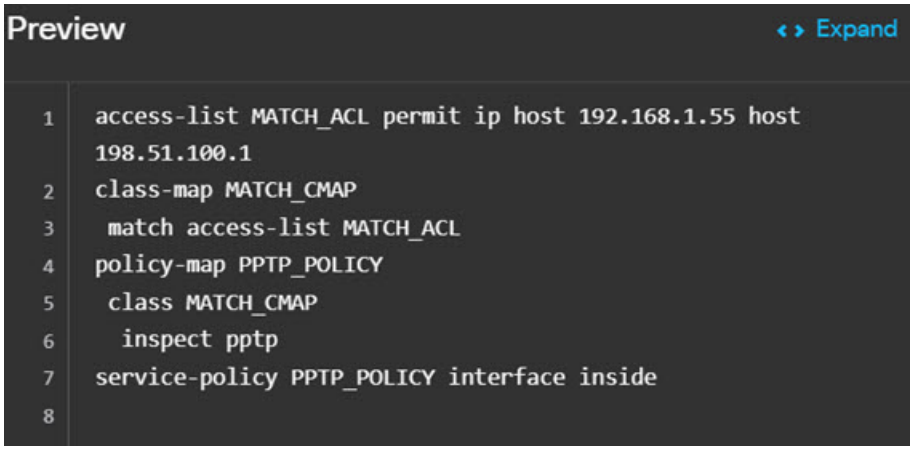
a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。

b) [グループリスト（Group List）] で [+] をクリックします。

c) [Enable_PPTP_Inspection_on_Interface] オブジェクトを選択し、[OK] をクリックします。

グループ リストは次のようになります。

プレビューはテンプレートのコマンドで更新されます。次の図に示されているように、予想していたコマンドが表示されていることを確認します。プレビューでは、インターフェイス変数は名前「inside」に解決されることに注意してください。変数には特に注意してください。プレビューで正しく解決されていない場合、変数は正確に展開されません。プレビューで変数が正しく変換されるまで、FlexConfig オブジェクトを編集します。



d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 10 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 11 CLI コンソールまたは SSH セッションで **show running-config** コマンドのバリエーションを使用して、実行コンフィギュレーションに正しい変更が含まれていることを確認します。

show running-config を入力して CLI の設定全体を検査したり、以下のコマンドを使用して、この設定の各部分を確認したりすることができます。

- **show running-config access-list MATCH_ACL** （ACL の確認用）。

- **show running-config class**（クラスマップの確認用）。すべてのクラス マップが表示されます。
- **show running-config policy-map PPTP_POLICY**（クラスおよびポリシーマップ設定の確認用）。
- **show running-config service-policy**（インターフェイスに適用されているポリシーマップの確認用）。すべてのサービス ポリシーが表示されます。

次の出力には、この一連のコマンドが表示されており、設定が正しく適用されていることを確認できます。

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

翻訳について
このドキュメントは、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。