Cisco ASA の概要

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

ハードウェアとソフトウェアの互換性

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

VPN の互換性

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

新機能

このセクションでは、各リリースの新機能を示します。

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

ASA 9.8(4) の新機能

リリース日：**2019 年 4 月 24 日**

機能	説明
VPN 機能	
webVPN HSTS へのサブドメインの追加	ドメイン所有者は、Web ブラウザの HSTS プリロード リストに含める必要があるドメインを送信できます。 新規/変更されたコマンド： **hostname(config-webvpn) includesubdomains** *9.12(1)* でも同様です。
管理機能	
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。 新規/変更されたコマンド： **http server basic-auth-client** *9.12(1)* でも同様です。
show tech-support に追加の出力が含まれている	**show tech-support** の出力が拡張され、次の出力が表示されるようになりました。 • **show ipv6 interface** • **show aaa-server** • **show fragment** 新規/変更されたコマンド： **show tech-support** *9.12(1)* でも同様です。

機能	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規/変更されたコマンド：**snmp-server enable oid** *9.10(1)* でも同様です。

ASA 9.8(3) の新機能

リリース日：**2018 年 7 月 2 日**

機能	説明
プラットフォーム機能	
Firepower 2100 アクティブ LED はスタンバイ モードのときにオレンジ色に点灯するようになりました。	以前は、スタンバイ モード時にはアクティブ LED は点灯していませんでした。
ファイアウォール機能	
カットスルー プロキシ ログイン ページからのログアウト ボタンの削除をサポート。	ユーザ ID 情報（AAA 認証 リスナー）を取得するようにカットスルー プロキシを設定している場合、ページからログアウト ボタンを削除できるようになりました。これは、ユーザが NAT デバイスの背後から接続し、IP アドレスで識別できない場合に便利です。1 人のユーザがログアウトすると、その IP アドレスのすべてのユーザがログアウトされます。 新規/変更されたコマンド：**aaa authentication listener no-logout-button**。
Trustsec SXP 接続の設定可能な削除ホールド ダウン タイマー	デフォルトの SXP 接続ホールド ダウン タイマーは 120 秒です。このタイマーを 120 ～ 64000 秒に設定できるようになりました。 新規/変更されたコマンド：**cts sxp delete-hold-down period**、**show cts sxp connection brief**、**show cts sxp connections**
VPN 機能	

機能	説明
従来の SAML 認証のサポート	CSCvg65072 の修正とともに ASA を展開すると、SAML のデフォルト動作で、AnyConnect 4.4 または 4.5 ではサポートされていない組み込みブラウザが使用されます。そのため、引き続き AnyConnect 4.4 または 4.5 を使用するには、従来の外部ブラウザで SAML 認証方式を有効にする必要があります。セキュリティ上の制限があるため、このオプションは、AnyConnect 4.6 に移行するための一時的な計画の一環としてのみ使用してください。このオプションは近い将来に廃止されます。 新規/変更されたコマンド： **saml external-browser**

ASA 9.8(2) の新機能

リリース：**2017年8月28日**

機能	説明
プラットフォーム機能	
FirePOWER 2100 シリーズ用の ASA	FirePOWER 2110、2120、2130、2140 用の ASA を導入しました。FirePOWER 4100 および 9300 と同様に、FirePOWER 2100 は基盤の FXOS オペレーティング システムを実行してから、ASA オペレーティング システムをアプリケーションとして実行します。FirePOWER 2100 実装では、FirePOWER 4100 および 9300 よりも緊密に FXOS を ASA と連携させます（軽量な FXOS 機能、単一デバイス イメージ バンドル、ASA および FXOS の両方に対する簡単な管理アクセス）。 FXOS には、EtherChannel の作成、NTP サービス、ハードウェアのモニタリング、およびその他の基本機能を含む、インターフェイスの構成ハードウェア設定があります。この構成では、Firepower Chassis Manager または FXOS CLI を使用できます。ASA には、（FirePOWER 4100 および 9300 とは異なり）スマート ライセンスを含む、その他すべての機能があります。ASA および FXOS はそれぞれ、管理 1/1 インターフェイスでの独自の IP アドレスを持っています。ユーザは、任意のデータ インターフェイスから ASA および FXOS インスタンス両方の管理を設定できます。 次のコマンドが導入されました。**connect fxos**、**fxos https**、**fxos snmp**、**fxos ssh**、**ip-client**
国防総省（DoD）統合機能認定製品リスト	ASA は、統合機能認定製品リスト（UC APL）の要件に準拠するように更新されました。このリリースでは、**fips enable** コマンドを入力すると、ASA がリロードされます。フェールオーバーを有効にする前に、両方のフェールオーバー ピアが同じ FIPS モードになっている必要があります。 **fips enable** コマンドが変更されました。
Amazon Web Services M4 インスタンスの ASAv サポート	ASAv を M4 インスタンスとして展開できるようになりました。 変更されたコマンドはありません。

機能	説明
ASAv5 1.5 GB RAM 機能	バージョン 9.7(1) 以降、ASAv5 では、AnyConnect の有効化やファイルの ASAv へのダウンロードなどの特定の機能が失敗した場合に、メモリが枯渇することがあります。1.5 GB の RAM を ASAv5 に割り当てられるようになりました（1 GB から増加しました）。 変更されたコマンドはありません。
VPN 機能	
HTTP Strict Transport Security（HSTS）ヘッダーのサポート	HSTS は、クライアントレス SSL VPN でのプロトコル ダウングレード攻撃や Cookie ハイジャックから Web サイトを保護します。これにより Web サーバは、Web ブラウザ（またはその他の準拠しているユーザ エージェント）が Web サーバと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。HSTS は IETF 標準化過程プロトコルであり、RFC 6797 で指定されます。 次のコマンドが導入されました。**hsts enable, hsts max-age** *age_in_seconds*
インターフェイス機能	
ASAv50 の VLAN サポート	ASAv50 では、SR-IOV インターフェイスの ixgbe-vf vNIC で VLAN がサポートされるようになりました。 変更されたコマンドはありません。

ASA 9.8(1.200) の新機能

リリース：2017年7月30日

（注） このリリースは、Microsoft Azure の ASAv でのみサポートされます。これらの機能は、バージョン 9.8(2) ではサポートされていません。

機能	説明
ハイ アベイラビリティとスケーラビリティの各機能	
Microsoft Azure での ASAv のアクティブ/バックアップの高可用性	アクティブな ASAv の障害が Microsoft Azure パブリック クラウドのバックアップ ASAv へのシステムの自動フェールオーバーをトリガーするのを許可するステートレスなアクティブ/バックアップ ソリューション。 次のコマンドが導入されました。**failover cloud** ASDM サポートはありません。

ASA 9.8(1) の新機能

リリース：2017年5月15日

機能	説明
プラットフォーム機能	
ASAv50 プラットフォーム	ASAv 仮想プラットフォームに、10 Gbps のファイアウォール スループット レベルを提供するハイエンド パフォーマンス ASAv50 プラットフォームが追加されました。ASAv50 には ixgbe-vf vNIC が必要です。これは VMware および KVM でのみサポートされます。
ASAv プラットフォームの SR-IOV	ASAv 仮想プラットフォームでは、Single Root I/O Virtualization（SR-IOV）インターフェイスがサポートされます。これにより、複数の VM でホスト内の 1 つの PCIe ネットワーク アダプタを共有できるようになります。ASAv SR-IOV サポートは、VMware、KVM、および AWS でのみ使用可能です。
ASAv での自動 ASP ロード バランシングのサポート	以前は、ASP ロード バランシングは手動でのみ有効または無効にできました。 次のコマンドを変更しました。**asp load-balance per-packet-auto**
ファイアウォール機能	
TLS プロキシ サーバの SSL 暗号スイートの設定サポート	ASA が TLS プロキシ サーバとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、 **ssl cipher** コマンドを使用した ASA のグローバル設定のみが可能でした。 次のコマンドが導入されました。 **server cipher-suite**
ICMP エラーのグローバル タイムアウト	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間を設定できるようになりました。このタイムアウトが無効（デフォルト）で、ICMP インスペクションが有効に設定されている場合、ASA はエコー応答を受信するとすぐに ICMP 接続を削除します。したがって、終了しているその接続に対して生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。 次のコマンドが追加されました。 **timeout icmp-error**
ハイ アベイラビリティとスケーラビリティの各機能	

機能	説明
改善されたクラスタ ユニットのヘルス チェック障害検出	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージング アクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビート メッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次のコマンドを変更しました。**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details**
に対してインターフェイスを障害としてマークするために設定可能なデバウンス時間 Firepower 4100/9300 シャーシ	ASA がインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。 新規または変更されたコマンド：**health-check monitor-interface debounce-time**
VPN 機能	
VTI での IKEv2、証明書ベース認証、および ACL のサポート	仮想トンネル インターフェイス（VTI）は、BGP（静的 VTI）をサポートするようになりました。スタンドアロン モードとハイ アベイラビリティ モードで、IKEv2 を使用できます。IPsec プロファイルにトラストポイントを設定することにより、証明書ベースの認証を使用できます。また、入力トラフィックをフィルタリングする access-group コマンドを使用して、VTI 上でアクセス リストを適用することもできます。 IPsec プロファイルのコンフィギュレーション モードに次のコマンドが導入されました。**set trustpoint**
モバイル IKEv2（MobIKE）はデフォルトで有効になっています	リモート アクセス クライアントとして動作するモバイル デバイスは、移動中にトランスペアレント IP アドレスを変更する必要があります。ASA で MobIKE をサポートすることにより、現在の SA を削除せずに現在の IKE セキュリティ アソシエーション（SA）を更新することが可能になります。MobIKE は [always on] に設定されます。 次のコマンドが導入されました。**ikev2 mobike-rrc**。リターン ルータビリティのチェックを有効または無効にするために使用されます。

機能	説明
SAML 2.0 SSO の更新	SAML 要求におけるシグネチャのデフォルト署名メソッドが SHA1 から SHA2 に変更され、ユーザが rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 の中から署名メソッドを選択して設定できるようになりました。 webvpn モードでの **saml idp signature** コマンドが変更されました。このコマンドには *value* を設定できます。デフォルトは [disabled] のままです。
tunnelgroup webvpn-attributes の変更	pre-fill-username および secondary-pre-fill-username の値が *clientless* から *client* に変更されました。 webvpn モードでの **pre-fill-username** および **secondary-pre-fill-username** コマンドが変更されました。これらのコマンドには *client* 値を設定できます。
AAA 機能	
ログイン履歴	デフォルトでは、ログイン履歴は90日間保存されます。この機能を無効にするか、期間を最大365日まで変更できます。1つ以上の管理メソッド（SSH、ASDM、Telnetなど）でローカルAAA認証を有効にしている場合、この機能はローカルデータベースのユーザ名にのみ適用されます。 次のコマンドが導入されました。**aaa authentication login-history**、**show aaa login-history**
パスワードの再利用とユーザ名と一致するパスワードの使用を禁止するパスワード ポリシーの適用	最大 7 世代にわたるパスワードの再利用と、ユーザ名と一致するパスワードの使用を禁止できるようになりました。 次のコマンドが導入されました。**password-history**、**password-policy reuse-interval**、**password-policy username-check**
SSH公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。	9.6(2) より前のリリースでは、ローカル ユーザ データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザ名にのみ適用されます。また、任意の AAA サーバ タイプ （**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザはローカルデータベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用できます。 変更されたコマンドはありません。 バージョン *9.6(3)* でも同様です。
モニタリング機能とトラブルシューティング機能	

機能	説明
ASA クラッシュ発生時に実行中のパケット キャプチャの保存	以前は、ASA がクラッシュするとアクティブなパケット キャプチャは失われました。現在は、クラッシュが発生すると、パケット キャプチャは disk 0 に以下のファイル名で保存されます。[*context_name*.]*capture_name*.**pcap**。 変更されたコマンドはありません。

ファイアウォール機能の概要

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

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数のDMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

セキュリティ ポリシーの概要

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

アクセス ルールによるトラフィックの許可または拒否

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

NAT の適用

NAT の利点のいくつかを次に示します。

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

IP フラグメントからの保護

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

HTTP、HTTPS、または FTP フィルタリングの適用

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

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

アプリケーション インスペクションの適用

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

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

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

QoS ポリシーの適用

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

接続制限と TCP 正規化の適用

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

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

脅威検出のイネーブル化

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

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

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャニング脅威検出機能は、スキャン アクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

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

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

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- Transparent

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

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

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

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

ステートフル インスペクションの概要

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

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

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

- 新規の接続かどうか。

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

  セッション管理パスで行われるタスクは次のとおりです。

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

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

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

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

- 確立済みの接続かどうか。

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

  - IP チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック
  - 既存セッションに基づく NAT 変換
  - レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

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

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

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成およ

び管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASAは、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASAは、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

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

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

セキュリティ コンテキストの概要

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

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

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

ASA クラスタリングの概要

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

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

特殊なサービスおよびレガシー サービス

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

特殊なサービスに関するガイド

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

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

レガシー サービス ガイド

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

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

- RIP の設定

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