# Cisco ASA の概要

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

（注） ASDM では、多数の ASA バージョンをサポートしています。ASDM のマニュアルおよびオンライン ヘルプには、ASA でサポートされている最新機能がすべて含まれています。古いバージョンの ASA ソフトウェアを実行している場合、ご使用のバージョンでサポートされていない機能がこのマニュアルに含まれている場合があります。各章の機能履歴テーブルを参照して、機能がいつ追加されたかを確認してください。ASA の各バージョンでサポートされている ASDM の最小バージョンについては、『Cisco ASA Compatibility（Cisco ASA の互換性）』[英語] を参照してください。特殊なサービス非推奨のサービスおよびレガシー サービス （17 ページ） も参照してください。


- ASDM 要件 （2 ページ）
- ハードウェアとソフトウェアの互換性 （6 ページ）
- VPN の互換性 （6 ページ）
- 新機能 （6 ページ）
- ファイアウォール機能の概要 （11 ページ）
- VPN 機能の概要 （16 ページ）
- セキュリティ コンテキストの概要 （17 ページ）
- ASA クラスタリングの概要 （17 ページ）
- 特殊なサービス非推奨のサービスおよびレガシー サービス （17 ページ）

# ASDM 要件

## ASDM クライアントのオペレーティング システムとブラウザの要件

次の表には、ASDM および ASA FirePOWER モジュールに対応するクライアント オペレーティング システムと Java のリストが表示されています。

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

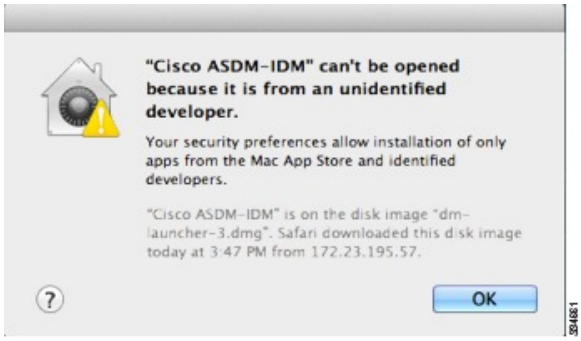
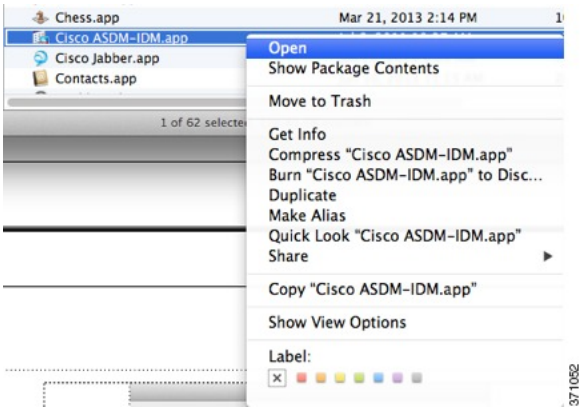
| オペレーティング システム | ブラウザ | | | | Java SE プラグイン |
|---|---|---|---|---|---|
| | Internet Explorer | Firefox | Safari | Chrome | |
| Microsoft Windows（英語および日本語）：<br>10<br>8<br>7<br>Server 2012 R2<br>Server 2012<br>Server 2008 | Yes | Yes | サポートなし | Yes | 8.0 |
| Apple OS X 10.4 以降 | サポートなし | Yes | Yes | Yes（64 ビット バージョンのみ） | 8.0 |
| Ubuntu Linux 14.04<br>Debian Linux 7 | 該当なし | Yes | 該当なし | 可 | 8.0（Oracle のみ。OpenJDK はサポートされていません） |

## 互換性メモ

次の表に、ASDM の互換性に関する警告を示します。

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

| 条件 | 注意 |
| --- | --- |
| サーバの IE9 | サーバの Internet Explorer 9.0 の場合は、[Do not save encrypted pages to disk] オプションがデフォルトで有効になっています（**[Tools]** > **[Internet Options]** > **[Advanced]** を参照）。このオプションでは、最初の ASDM のダウンロードは失敗します。ASDM でダウンロードを行うには、このオプションを確実にディセーブルにしてください。 |
| OS X | OS X では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。 |

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

# 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 9.10(1)/ASDM 7.10(1) の新機能

リリース日：**2018 年 10 月 25 日**

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| Azure 用の ASAv VHD カスタム イメージ | シスコが提供する圧縮 VHD イメージを使用して、Azure に独自のカスタム ASAv イメージを作成できるようになりました。VHD イメージを使用して展開するには、Azure ストレージアカウントに VHD イメージをアップロードする必要があります。次に、アップロードしたディスク イメージおよび Azure Resource Manager テンプレートを使用して、管理対象イメージを作成できます。Azure テンプレートは、リソースの説明とパラメータの定義が含まれている JSON ファイルです。 |
| FirePOWER モジュール バージョン 6.3 の ISA 3000 サポート | 以前サポート対象だったバージョンは FirePOWER 5.4 でした。 |
| **ファイアウォール機能** | |

| 機能 | 説明 |
|---|---|
| Cisco Umbrella サポート | Cisco Umbrella で定義されているエンタープライズセキュリティポリシーをユーザ接続に適用できるように DNS 要求を Cisco Umbrella へリダイレクトするようにデバイスを設定できます。FQDN に基づいて接続を許可またはブロックできます。または、疑わしい FQDN の場合は Cisco Umbrella インテリジェントプロキシにユーザをリダイレクトして URL フィルタリングを実行できます。Umbrella の設定は、DNS インスペクションポリシーに含まれています。<br>新しい/変更された画面：<br>**[Configuration]** > **[Firewall]** > **[Objects]** > **[Umbrella]**、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspect Maps]** > **[DNS]** |
| MSISDN および選択モードのフィルタリング、アンチリプレイ、およびユーザスプーフィング保護に対する GTP インスペクションの機能拡張 | モバイルステーション国際サブスクライバ電話番号（MSISDN）または選択モードに基づいて PDP コンテキストの作成メッセージをドロップするように GTP インスペクションを設定できるようになりました。また、アンチリプレイとユーザスプーフィング保護も実装できます。<br>新しい/変更された画面：<br>**[Configuration]** > **[Firewall]** > **[Objects]** > **[Inspection Maps]** > **[GTP]** > **[Add/Edit]** ダイアログボックス |
| TCP ステートバイパスのデフォルトのアイドルタイムアウト | TCP ステートバイパス接続のデフォルトのアイドルタイムアウトは 1 時間ではなく、2 分になりました。 |
| 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。<br>新規/変更されたコマンド：**aaa authentication listener no-logout-button**<br>ASDM サポートはありません。<br>*9.8(3)* でも同様。 |
| 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。<br>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**<br>ASDM サポートはありません。<br>*9.8(3)* でも同様。 |

| 機能 | 説明 |
|---|---|
| トランスペアレント モードでの NAT'ed フローのオフロードをサポート。 | フロー オフロード（**flow-offload enable** および **set connection advanced-options flow-offload** コマンド）を使用している場合、トランスペアレント モードで NAT を必要とするフローをオフロードされたフローに含めることができるようになりました。 |
| Firepower 4100/9300 ASA 論理デバイスのトランスペアレント モード展開のサポート | Firepower 4100/9300 に ASA を展開するときに、トランスペアレントまたはルーテッド モードを指定できるようになりました。<br>新規/変更された [Firepower Chassis Manager] 画面：<br>**[Logical Devices]** > **[Add Device]** > **[Settings]**<br>新規/変更されたオプション：[Firewall Mode] ドロップダウンリスト |
| **VPN 機能** | |
| 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（またはそれ以降）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。<br>新しい/変更された画面：<br>**[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[AnyConnect Connection Profiles]** ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add AnyConnect Connection Profile] ダイアログボックス<br>**[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Connection Profiles]** > ページ > [Connection Profiles] 領域 > [Add] ボタン > [Add Clientless SSL VPN Connection Profile] ダイアログボックス<br>新規および変更されたオプション：[SAML External Browser] チェックボックス<br>*9.8(3)* でも同様。 |
| AnyConnect VPN リモート アクセス接続のための DTLS 1.2 サポート。 | DTLS 1.2（RFC-6347 で規定）では、現在サポートされている DTLS 1.0（バージョン番号 1.1 は DTLS には使用されません）に加えて、AnyConnect リモート アクセスもサポートされるようになりました。これは、5506 を除くすべての ASA モデルに適用され、ASA がクライアントではなく、サーバとしてのみ機能している場合に適用されます。DTLS 1.2 は、現在のすべての TLS/DTLS 暗号方式と大きな Cookie サイズに加えて、追加の暗号方式をサポートしています。<br>新規/変更された画面：**[Configuration]** > **[Remote Access VPN]** > **[Advanced]** > **[SSL Settings]** |
| **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 |
|---|---|
| Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス | クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。FXOS でクラスタを展開するときに、ネットワークを設定できるようになりました。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを設定できるようになりました。<br><br>新規/変更された [Firepower Chassis Manager] 画面：<br><br>**[Logical Devices]** > **[Add Device]** > **[Cluster Information]**<br><br>新規/変更されたオプション：[CCL Subnet IP] フィールド |
| Firepower 9300 シャーシごとのクラスタ ユニットのパラレル参加 | Firepower 9300 の場合、この機能により、シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されるようになります。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。<br><br>新しい/変更された画面：<br><br>**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**<br><br>新規/変更されたオプション：[Parallel Join of Units Per Chassis] エリア |
| クラスタ インターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。 | インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで **health-check monitor-interface debounce-time** コマンドまたは ASDM **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタ ユニットの方がポートのバンドルが速いという理由だけで、クラスタ ユニット上でインターフェイスがエラー表示されるのを防ぐことができます。<br><br>変更された画面はありません。 |

| 機能 | 説明 |
|---|---|
| Microsoft Azure Government クラウドでの 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 ソリューションが、Azure Government クラウドで使用できるようになりました。<br>新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]**<br>**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]**<br>**[Monitoring]** > **[Properties]** > **[Failover]** > **[History]** |
| **インターフェイス機能** | |
| Firepower 2100/4100/9300 のスーパーバイザの関連付けを表示するための **show interface ip brief** および **show ipv6 interface** の出力の強化 | Firepower 2100/4100/9300 の場合、コマンドの出力は、インターフェイスのスーパーバイザの関連付けステータスを表示するために強化されています。<br>新規/変更されたコマンド：**show interface ip brief**、**show ipv6 interface** |
| Firepower 2100 では、**set lacp-mode** コマンドが **set port-channel-mode** に変更されています。 | **set lacp-mode** コマンドは、Firepower 4100/9300 でのコマンドの使用方法に合わせるために **set port-channel-mode** に変更されています。<br>新規/変更された FXOS コマンド： **set port-channel-mode** |
| **管理およびトラブルシューティングの機能** | |
| Firepower 2100 の NTP 認証のサポート | FXOS で SHA1 NTP サーバ認証を設定できるようになりました。<br>新規/変更された FXOS コマンド：**enable ntp-authentication**、**set ntp-sha1-key-id**、**set ntp-sha1-key-string**<br>新規/変更された [Firepower Chassis Manager] 画面：<br>**[Platform Settings]** > **[NTP]**<br>新規/変更されたオプション：[NTP Server Authentication: Enable] チェックボックス、[Authentication Key] フィールド、[Authentication Value] フィールド |
| ACL を使用せず IPv6 トラフィックを一致させるためのパケットキャプチャのサポート | **capture** コマンドの **match** キーワードを使用する場合、**any** キーワードは IPv4 トラフィックのみ照合します。IPv4 または IPv6 トラフィックをキャプチャするために、**any4** と **any6** キーワードを指定できるようになりました。**any** キーワードでは、引き続き IPv4 トラフィックのみ照合されます。<br>新規/変更されたコマンド：**capture match**<br>ASDM サポートはありません。 |

| 機能 | 説明 |
|---|---|
| Firepower 2100 の FXOS に対する SSH の公開キー認証のサポート | SSH キーを設定し、パスワード認証の代わりに公開キー認証を使用したり、両方の認証を使用したりできます。<br>新規/変更された FXOS コマンド：**set sshkey**<br>Firepower Chassis Manager のサポートはありません。 |
| GRE および IPinIP カプセル化のサポート | 内部インターフェイス上でパケット キャプチャを実行するときに、ICMP、UDP、TCP などでの GRE および IPinIP カプセル化を表示するコマンドの出力が強化されています。<br>新規/変更されたコマンド：**show capture** |
| アプリケーションのキャッシュの割り当てを制限するメモリしきい値を有効にするためのサポート | デバイスの管理性と安定性を維持するためのメモリの予約ができるように、特定のメモリしきい値に達するアプリケーション キャッシュの割り当てを制限することができます。<br>新規/変更されたコマンド：**memory threshold enable**、**show run memory threshold**、**clear conf memory threshold** |
| RFC 5424 ロギングのタイムスタンプのサポート | RFC 5424 形式に従ってロギング タイムスタンプを有効にできます。<br>新規/変更されたコマンド：**logging timestamp** |
| TCB-IPS のメモリ使用量を表示するためのサポート | TCB-IPS でのアプリケーション レベルのメモリ キャッシュを表示します。<br>新規/変更されたコマンド：**show memory app-cache** |

# 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 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

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。

# 特殊なサービス非推奨のサービスおよびレガシーサービス

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

### 特殊なサービスに関するガイド

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

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

### 非推奨のサービス

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

### レガシー サービス ガイド

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

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

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