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 （19 ページ） も参照してください。

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

次の表は、ASA と ASA FirePOWER モジュールの両方を管理する場合に ASDM でサポートされているクライアント オペレーティング システムと Java の一覧を示します。

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

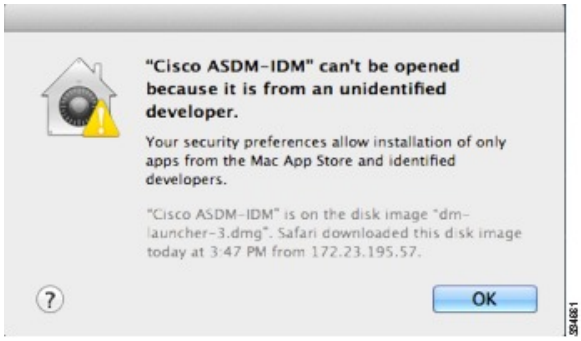
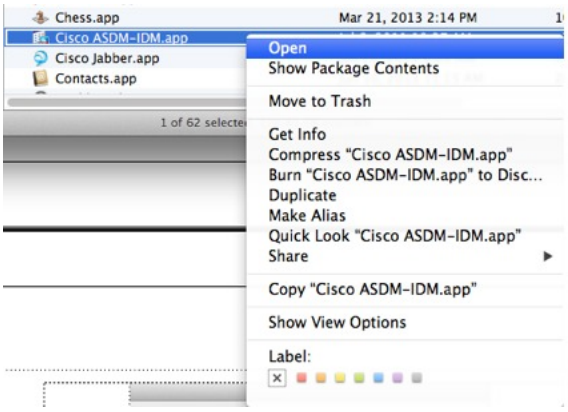
オペレーティング システム	ブラウザ				Java SE プラグイン
	Internet [illegible]	Firefox	Safari	Chrome	
Microsoft Windows（英語および日本語）： 10 8 7 Server 2012 R2 Server 2012 Server 2008	Yes	Yes	サポートなし	Yes	8.0
Apple OS X 10.4 以降	サポートなし	Yes	Yes	Yes（64 ビット バージョンのみ）	8.0
Ubuntu Linux 14.04 Debian Linux 7	該当なし	Yes	該当なし	Yes	8.0（Oracle 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

互換性に関する注意事項

次の表に、ASDM の互換性に関する注意事項を示します。

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

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。

ASDM 7.9(2.152) の新機能

リリース：**2018年5月9日**

機能	説明
VPN 機能	
レガシー SAML 認証のサポート	CSCvg65072 の修正を含む ASA を展開する場合、デフォルト SAML の動作では、AnyConnect 4.4 または 4.5 ではサポートされていない組み込みのブラウザを使用します。したがって、AnyConnect 4.4 または 4.5 の使用を続行するには、レガシー外部ブラウザ SAML の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のため、AnyConnect 4.6 に移行する際の一時的な計画の一環としてのみこのオプションを使用してください。このオプションは、将来廃止される予定です。 新しい/変更された画面： **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[AnyConnect Connection Profiles]** ページ > [Connection Profiles] エリア > [Add] ボタン > [Add AnyConnect Connection Profile] ダイアログボックス **[Configuration]** > **[Remote Access VPN]** > **[Clientless SSL VPN Access]** > **[Connection Profiles]** > ページ > [Connection Profiles] エリア > [Add] ボタン > [Add Clientless SSL VPN Connection Profile] ダイアログボックス 新しい/変更されたオプション：[SAML External Browser] チェック ボックス

ASA 9.9(2)/ASDM 7.9(2) の新機能

リリース：**2018年3月26日**

機能	説明
プラットフォーム機能	
VMware ESXi 6.5 用の ASAv サポート	ASAv 仮想プラットフォームは、VMware ESXi 6.5 で動作するホストをサポートしています。*vi.ovf* および *esxi.ovf* ファイルに新しい VMware ハードウェア バージョンが追加され、ESXi 6.5 で ASAv の最適なパフォーマンスと使いやすさを実現しました。 変更された画面はありません。
VMXNET3 インターフェイス用の ASAv サポート	ASAv 仮想プラットフォームは、VMware ハイパーバイザ上の VMXNET3 インターフェイスをサポートしています。 変更された画面はありません。
初回起動時の仮想シリアル コンソール用の ASAv サポート	ASAv にアクセスして設定するために、仮想 VGA コンソールではなく初回起動時に仮想シリアル コンソールを使用するように ASAv を設定できるようになりました。
Microsoft Azure 上での高可用性のために複数の Azure サブスクリプションでユーザ定義ルートを更新する ASAv サポート	Azure 高可用性構成で ASAv を構成して、複数の Azure サブスクリプションでユーザ定義ルートを更新できるようになりました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** > **[Route-Table]**
VPN 機能	
IKEv2 プロトコルに拡張されたリモートアクセス VPN マルチコンテキスト サポート	AnyConnect やサード パーティ製標準ベース IPSec IKEv2 VPN クライアントがマルチコンテキスト モードで稼働する ASA へのリモート アクセス VPN セッションを確立できるように、ASA を構成することをサポートします。
RADIUS サーバへの IPv6 接続	ASA 9.9.2 では、外部 AAA RADIUS サーバへの IPv6 接続がサポートされるようになりました。

機能	説明
BVI サポートのための Easy VPN 拡張	Easy VPN は、ブリッジ型仮想インターフェイスを内部セキュア インターフェイスとしてサポートするように拡張され、管理者は新しい **vpnclient secure interface** [*interface-name*] コマンドを使用して内部セキュア インターフェイスを直接設定できるようになりました。 物理インターフェイスまたはブリッジ型仮想インターフェイスを内部セキュア インターフェイスとして割り当てることができます。これが管理者によって設定されていない場合、Easy VPN はそれが独立した物理インターフェイスまたは BVI かに関わらず、以前と同じセキュリティ レベルを使用してその内部セキュア インターフェイスを選択します。 また、管理アクセスがその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で設定できるようになりました。
分散型 VPN セッションの改善	• 分散型 S2S VPN のアクティブ セッションとバックアップ セッションのバランスをとるアクティブセッションの再配布ロジックが改善されました。また、管理者が入力した単一の **cluster redistribute vpn-sessiondb** コマンドに対し、バランシング プロセスをバックグラウンドで最大 8 回繰り返すことができます。 • クラスタ全体のダイナミック リバース ルート インジェクション（RRI）の処理が改善されました。
ハイ アベイラビリティとスケーラビリティの各機能	
内部障害発生後に自動的にクラスタに再参加する	以前は、多くのエラー状態によりクラスタ ユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** > **[Auto Rejoin]**
ASA 5000-X シリーズの障害としてインターフェイスをマーキングするために設定可能なデバウンス時間	ここで、ASA がインターフェイスの障害と見なし、ASA 5500-x シリーズでユニットがクラスタから削除されるまでのデバウンス時間を設定することができます。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイス ステータスの更新が発生すると、ASA は、インターフェイスを障害としてマーキングしユニットがクラスタから削除されるまで、指定された時間（ミリ秒数）待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。この機能は以前は Firepower 4100/9300 で使用できました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]**

機能	説明
クラスタの信頼性の高いトランスポート プロトコル メッセージのトランスポートに関連する統計情報の表示	ユニットごとのクラスタの信頼性の高いトランスポート バッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**
ピア ユニットからのフェールオーバー履歴の表示	ピアユニットから、**details** キーワードを使用して、フェールオーバー履歴を表示できるようになりました。これには、フェールオーバー状態の変更と状態変更の理由が含まれます。 新規または変更されたコマンド：**show failover**
管理機能	
RSA キー ペアによる 3072 ビット キーのサポート	モジュラス サイズを 3072 に設定できるようになりました。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Certificate Management]** > **[Identity Certificates]**
FXOS ブートストラップ設定によるイネーブル パスワードの設定	ASA Firepower 4100/9300 で ASA を展開すると、ブートストラップのパスワード設定が、イネーブル パスワードと管理ユーザ パスワードを設定するようになりました。FXOS バージョン 2.3.1 が必要です。
モニタリング機能とトラブルシューティング機能	
SNMP IPv6 のサポート	ASA は、IPv6 経由での SNMP サーバとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
単一ユーザ セッションのトラブルシューティングのための条件付きデバッグ	条件付きデバッグ機能は、設定されたフィルタ条件に基づく特定の ASA VPN セッションのログを確認することを支援するようになりました。IPv4 および IPv6 サブネットの「any, any」のサポートが提供されます。

ASDM 7.9(1.151) の新機能

リリース：**2018 年 2 月 14 日**

このリリースに新機能はありません。

ASA 9.9(1)/ASDM 7.9(1) の新機能

リリース：**2017年12月4日**

機能	説明
ファイアウォール機能	
Ethertype アクセス コントロール リストの変更	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス コントロール エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケットキャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 新規または変更された画面：**[Configuration]** > **[Firewall]** > **[Ethertype Rules]**
VPN 機能	

機能	説明
Firepower 9300 上のクラスタリングによる分散型サイト間 VPN	Firepower 9300 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）マスター ユニットだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスタ（合計 6 つのクラスタ メンバー）上で動作し、各モジュールは最大約 36,000 のアクティブ セッション（合計 72,000)に対し、最大 6,000 のアクティブ セッション（合計 12,000）をサポートします。 新規または変更された画面： **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] > [Slave]** **[Configuration] > [Device Management] > [High Availablility and Scalability] > [ASA Cluster]** **[Wizards] > [Site-to-Site]** **[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [VPN Cluster Summary]** **[Monitoring] > [ASA Cluster] > [ASA Cluster] > [System Resource Graphs] > [CPU/Memory]** **[Monitoring] > [Logging] > [Real-Time Log Viewer]**
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。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** **[Monitoring]** > **[Properties]** > **[Failover]** > **[History]** バージョン *9.8(1.200)* でも同様です。
Firepower 9300 のシャーシ ヘルス チェックの障害検出の向上	シャーシ ヘルス チェックの保留時間をより低い値（100 ms）に設定できるようになりました。以前の最小値は 300 ms でした。 新規または変更されたコマンド：**app-agent heartbeat interval** ASDM サポートはありません。

機能	説明
クラスタリングのサイト間冗長性	サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更された画面：**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster]**
モニタリング機能とトラブルシューティング機能	
強化されたパケット トレーサおよびパケット キャプチャ機能	パケット トレーサは次の機能で強化されました。 • パケットがクラスタ ユニット間を通過するときにパケットを追跡します。 • シミュレートされたパケットが ASA から出られるようにします。 • シミュレートされたパケットのセキュリティ チェックをバイパスします。 • シミュレートされたパケットを IPsec/SSL で復号化されたパケットとして扱います。 パケット キャプチャは次の機能で強化されました。 • パケットを復号化した後にキャプチャします。 • トレースをキャプチャし、永続リストに保持します。 新規または変更された画面： **[Tools] > [Packet Tracer]** 次のオプションをサポートする [Cluster Capture] フィールドを追加しました：**decrypted**、**persist**、**bypass-checks**、**transmit** [All Sessions] ドロップダウンリストの下の [Filter By] ビューに 2 つの新しいオプションを追加しました：[Origin] および [Origin-ID] **[Monitoring] > [VPN] > [VPN Statistics] > [Packet Tracer and Capture]** [Packet Capture Wizard] 画面に [ICMP Capture] フィールドを追加しました：**[Wizards] > [Packet Capture Wizard]** ICMP キャプチャをサポートする 2 つのオプション、**include-decrypted** および **persist** を追加しました。

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