# 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』を参照してください。

## VPN の互換性

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

## 新機能

このセクションでは、各リリースの新機能を示します。

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

# ASA 9.13(1)の新機能

リリース：**2019 年 9 月 25 日**

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| Firepower 1010 用の ASA | Firepower 1010 用の ASA を導入しました。このデスクトップモデルには、組み込みハードウェアスイッチと Power on Ethernet+（PoE+）のサポートが含まれています。<br>新規/変更されたコマンド：**boot system**、**clock timezone**、**connect fxos admin**、**forward interface**、**interface vlan**、**power inline**、**show counters**、**show environment**、**show interface**、**show inventory**、**show power inline**、**show switch mac-address-table**、**show switch vlan**、**switchport**、**switchport access vlan**、**switchport mode**、**switchport trunk allowed vlan** |
| Firepower 1120、1140、および 1150 用の ASA | Firepower 1120、1140、および 1150 用の ASA を導入しました。<br>新規/変更されたコマンド：**boot system**、**clock timezone**、**connect fxos admin**、**show counters**、**show environment**、**show interface**、**show inventory** |

| 機能 | 説明 |
| --- | --- |
| Firepower 2100 アプライアンス モード | Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティング システムを実行します。Firepower 2100 は、次のモードで実行できます。<br>• アプライアンス モード（現在はデフォルト）：アプライアンス モードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。<br>• プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Firepower Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。<br>9.13(1）にアップグレードしている場合、モードはプラットフォーム モードのままになります。<br>新規/変更されたコマンド：**boot system**、**clock timezone**、**connect fxos admin**、**fxos mode appliance**、**show counters**、**show environment**、**show fxos mode**、**show interface**、**show inventory** |
| ASAv 最小メモリ要件 | ASAv の最小メモリ要件は 2 GB です。現在の ASAv が 2 GB 未満のメモリで動作している場合、ASAv VM のメモリを増やすことなく、以前のバージョンから 9.13（1）にアップグレードすることはできません。また、バージョン 9.13（1）を使用して新しい ASAv VM を再展開することもできます。<br>変更されたコマンドはありません。 |
| ASAv MSLA サポート | ASAv は、シスコのマネージド サービス ライセンス契約（MSLA）プログラムをサポートしています。このプログラムは、マネージド ソフトウェア サービスをサードパーティに提供するシスコのお客様およびパートナー向けに設計された、ソフトウェアのライセンスおよび消費のフレームワークです。<br>MSLA はスマートライセンスの新しい形式で、ライセンス スマート エージェントは時間単位でライセンス権限付与の使用状況を追跡します。<br>新規/変更されたコマンド：**license smart**、**mode**、**utility**、**custom-id**、**custom-info**、**privacy**、**transport type**、**transport url**、**transport proxy** |
| ASAv の柔軟なライセンス | すべての ASAv ライセンスは、サポートされているすべての ASAv vCPU/メモリ構成で使用できるようになりました。AnyConnect および TLS プロキシのセッション制限は、モデルタイプに関連付けられたプラットフォーム制限ではなく、インストールされた ASAv プラットフォームの権限付与によって決まります。<br>新規/変更されたコマンド：**show version**、**show vm**、**show cpu**、**show license features** |

| 機能 | 説明 |
| --- | --- |
| AWS の ASAv での C5 イン[スタンスのサポート。C4、C3、およびM4インスタンスの拡張サポート | AWS パブリッククラウド上の ASAv は、C5 インスタンスをサポートするようになりました（c5.large、c5.xlarge、および c5.2xlarge）。<br>さらに、C4 インスタンス（c4.2xlarge および c4.4xlarge）、C3 インスタンス（c3.2xlarge、c3.4xlarge、および c3.8xlarge）および M4 インスタンス（m4.2xlarge および m4.4xlarge）のサポートが拡張されました。<br>変更されたコマンドはありません。 |
| より多くの Azure 仮想マシンサイズをサポートする Microsoft Azure の ASAv | Microsoft Azure パブリッククラウドの ASAv は、より多くの Linux 仮想マシンサイズをサポートするようになりました。<br>• Standard_D4、Standard_D4_v2<br>• Standard_D8_v3<br>• Standard_DS3、Standard_DS3_v2<br>• Standard_DS4、Standard_DS4_v2<br>• Standard_F4、Standard_F4s<br>• Standard_F8、Standard_F8s<br>以前のリリースでは、Standard_D3 と Standard_D3_v2 のサイズのみがサポートされていました。<br>変更されたコマンドはありません。 |
| DPDK の ASAv 拡張サポート | ASAv は、Data Plane Development Kit（DPDK）の拡張機能をサポートして、複数の NIC キューのサポートを有効にします。これにより、マルチコア CPU はネットワークインターフェイスに同時に効率よくサービスを提供できるようになります。<br>これは、Microsoft Azure と Hyper-v を除くすべての ASAv ハイパーバイザに適用されます。<br>（注） DPDK のサポートは、リリース ASA 9.10 (1) で導入されました。<br>変更されたコマンドはありません。 |
| VMware ESXi 6.7 用の ASAv サポート | ASAv 仮想プラットフォームは、VMware ESXi 6.7 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 6.7 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。<br>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** | |

| 機能 | 説明 |
|---|---|
| モバイル端末の場所のロギング（GTP インスペクション）。 | GTP インスペクションを設定すると、モバイル端末の初期の場所とそれ以降の場所の変更をログに記録できます。場所の変更を追跡すると、不正なローミング請求を識別するのに役立つ場合があります。<br>新規/変更されたコマンド：**location-logging**。 |
| GTPv2 および GTPv1 リリース 15 がサポートされています。 | システムで GTPv2 3GPP 29.274 V15.5.0 がサポートされるようになりました。GTPv1 の場合、3GPP 29.060 V15.2.0 までサポートしています。新しいサポートでは、2 件のメッセージおよび 53 件の情報要素の認識が追加されています。<br>変更されたコマンドはありません。 |
| アドレスとポート変換のマッピング（MAP-T） | アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー (SP) ネットワークで使用する機能です。サービス プロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリック インターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。<br>新規/変更されたコマンド：**basic-mapping-rule**、**default-mapping-rule**、**ipv4-prefix**、**ipv6-prefix**、**map-domain**、**share-ratio**、**show map-domain**、**start-port**。 |
| グループごとの AAA サーバ グループとサーバの制限が増えました。 | より多くの AAA サーバ グループを設定できます。In single context mode, you can configure 200 AAA server groups（the former limit was 100). In multiple context mode, you can configure 8（the former limit was 4).<br>In addition, in multiple context mode, you can configure 8 servers per group（the former limit was 4 servers per group). シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。<br>これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host**。 |
| SCCP（Skinny）インスペクションでは、TLS プロキシが廃止されました。 | **tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは廃止されました。このキーワードは今後のリリースで **inspect skinny** コマンドから削除される予定です。 |
| **VPN 機能** | |
| クライアントとしての WebVPN の HSTS サポート | http-headers と呼ばれる WebVPN モードの新しい CLI モードが追加され、WebVPN は、HTTP 参照を HSTS であるホストの HTTPS 参照に変換できるようになりました。ASA からブラウザへの WebVPN 接続用にこのヘッダーを送信する場合、ユーザ エージェントがリソースの埋め込みを許可するかどうかを設定します。<br>http-headers は次のように設定することも選択できます。**x-content-type-options**、**x-xss-protection**、**hsts-client**（クライアントとしての WebVPN の HSTS サポート）、**hsts-server**、または **content-security-policy**。<br>新規/変更されたコマンド：**webvpn**、**show webvpn hsts host (name <hostname&s{253}> \| all)**、および **clear webvpn hsts host (name <hostname&s{253}> \| all)**。 |

| 機能 | 説明 |
|---|---|
| キー交換用に追加された Diffie-Hellman グループ 15 および 16 | Diffie-Hellman グループ 15 および 16 のサポートを追加するために、これらの新しい制限を受け入れるようにいくつかの **crypto** コマンドが変更されました。<br>**crypto ikev2 policy <index> group <number>** および **crypto map <map-name> <map-index> set pfs <group>.** |
| **show asp table vpn-context** 出力の機能強化 | デバッグ機能を強化するために、次の VPN コンテキスト カウンタが出力に追加されました。 Lock Err、No SA、IP Ver Err、および Tun Down。<br>新しい/変更されたコマンド：**show asp table vpn-context**（出力のみ）。 |
| **ハイ アベイラビリティとスケーラビリティの各機能** | |
| デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。 | デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。<br>新しい/変更されたコマンド：**show conn**（出力のみ）。 |
| クラスタのトラフィック負荷のモニタ | クラスタ メンバのトラフィック負荷をモニタできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。<br>新規/変更されたコマンド：**debug cluster load-monitor**、**load-monitor**、**show cluster info load-monitor** |
| クラスタ結合の高速化 | スレーブ ユニットがマスター ユニットと同じ構成の場合、構成の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、マスターからスレーブには複製されません。<br>（注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。<br>新規/変更されたコマンド：**unit join-acceleration**、**show cluster info unit-join-acceleration incompatible-config** |
| **ルーティング機能** | |

| 機能 | 説明 |
|---|---|
| SMTP 設定の機能強化 | 必要に応じて、プライマリおよびバックアップインターフェイス名を指定してSMTPサーバを設定することで、ロギングに使用するルーティング テーブル（管理ルーティング テーブルまたはデータ ルーティング テーブル）を識別するためにASAを有効にできます。インターフェイスが指定されていない場合、ASAは管理ルーティングテーブルルックアップを参照し、適切なルートエントリが存在しない場合は、データ ルーティング テーブルを参照します。<br>新規/変更されたコマンド： **smtp-server [primary-interface][backup-interface]** |
| NSF 待機タイマーを設定するためのサポート | OSPF ルータは、すべてのネイバーがパケットに含まれているか不明な場合、Hello パケットにアタッチされている EO-TLV に RS ビットを設定することが期待されています。また、隣接関係（アジャセンシー）を維持するためにはルータの再起動が必要です。ただし、RS ビット値は RouterDeadInterval 秒より長くすることはできません。**timers nsf wait** コマンドは、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するために導入されました。<br>新規/変更されたコマンド： **timers nsf wait** |
| TFTPブロックサイズを設定するためのサポート | TFTP ファイル転送用に固定された一般的なブロックサイズは512オクテットです。新しいコマンド**tftp blocksize**は、より大きなブロックサイズを設定するために導入されました。これにより、TFTP ファイル転送速度が向上します。513 ～ 8192 オクテットのブロックサイズを設定できます。新しいデフォルトのブロックサイズは 1456 オクテットです。このコマンドの **no** 形式を使用すると、ブロックサイズが古いデフォルト値（512 オクテット）にリセットされます。**timers nsf wait** コマンドは、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するために導入されました。<br>新規/変更されたコマンド： **tftp blocksize** |
| **証明書の機能** | |
| FIPS ステータスを表示するためのサポート | **show running-configuration fips** コマンドは、FIPS が有効になっている場合にのみ FIPS ステータスを表示します。動作状態を確認するために、**show fips** コマンドが導入されました。このコマンドは、無効または有効状態になっている FIPS をユーザが有効化または無効化したときに、FIPSステータスを表示します。このコマンドは、有効化または無効化アクションの後にデバイスを再起動するためのステータスも表示します。<br>新規/変更されたコマンド： **show fips** |
| CRL 分散ポイント コマンドの変更 | スタティックCDP URL コンフィギュレーション コマンドが削除され、match certificate コマンドに移行しました。<br>新規/変更されたコマンド：**crypto-ca-trustpoint crl** と **crl url** はその他の関連ロジックで削除され、**match-certificate override-cdp** が導入されました。 |
| **管理およびトラブルシューティングの機能** | |

| 機能 | 説明 |
| --- | --- |
| Firepower 1000、 Firepower 2100 アプライアンス モードがライセンス評価モードの場合の管理アクセス | ASA には、管理アクセスのみを対象にしてデフォルトで 3DES 機能が含まれています。したがって、License Authority に接続し、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に License Authority に登録する必要がある高度暗号化ライセンスが有効になっている必要があります。<br>（注） ライセンスを取得する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。<br>変更されたコマンドはありません。 |
| 追加の NTP 認証アルゴリズム | 以前は、NTP 認証では MD5 だけがサポートされていました。ASA は、次のアルゴリズムをサポートするようになりました。<br>• MD5<br>• SHA-1<br>• SHA-256<br>• SHA-512<br>• AES-CMAC<br>新規/変更されたコマンド： **ntp authentication-key** |
| Firepower 4100/9300 の ASA Security Service Exchange（SSE）テレメトリ サポート | ネットワークで Cisco Success Network を有効にすると、デバイスの使用状況に関する情報と統計情報がシスコに提供され、テクニカル サポートの最適化に使用されます。ASA デバイスで収集されるテレメトリ データには、CPU、メモリ、ディスク、または帯域幅の使用状況、ライセンスの使用状況、設定されている機能リスト、クラスタ/フェールオーバー情報などが含まれます。<br>新規/変更されたコマンド：**service telemetry** および **show telemetry** |
| **show tech-support** に追加の出力が含まれている | **show tech-support** の出力が強化され、次の出力が表示されるようになりました。<br>**show flow-offload info detail**<br>**show flow-offload statistics**<br>**show asp table socket**<br>新しい/変更されたコマンド：**show tech-support**（出力のみ）。 |

| 機能 | 説明 |
|---|---|
| ドロップ ロケーション情報を含む **show-capture asp_drop** 出力の機能強化 | ASP ドロップ カウンタを使用したトラブルシューティングでは、同じ理由による ASP ドロップがさまざまな場所で使用されている場合は特に、ドロップの正確な位置は不明です。この情報は、ドロップの根本原因を特定する上で重要です。この拡張機能を使用すると、ビルド ターゲット、ASA リリース番号、ハードウェア モデル、および ASLR メモリ テキスト領域などの ASP ドロップの詳細が表示されます（ドロップの位置のデコードが容易になります）。<br>新規/変更されたコマンド： **show-capture asp_drop** |
| 変更内容 **debug crypto ca** | **debug crypto ca transactions** および **debug crypto ca messages** オプションは、すべての該当するコンテンツを **debug crypto ca** コマンド自体に提供するために統合されています。また、使用可能なデバッグ レベルの数が 14 に削減されました。<br>新規/変更されたコマンド： **debug crypto ca** |
| **Firepower 1000 および2100 の FXOS 機能** | |
| 安全消去 | 安全消去機能は、SSD 自体で特別なツールを使用してもデータを回復できないように、SSD 上のすべてのデータを消去します。デバイスをデコミッションする場合は、安全消去を実行する必要があります。<br>新規/変更されたコマンド：**erase secure** (local-mgmt)<br>サポートされているモデル：Firepower 1000 および 2100 |
| 設定可能な HTTPS プロトコル | HTTPS アクセス用の SSL/TLS のバージョンを設定できます。<br>新規/変更されたコマンド： **set https access-protocols**<br>サポートされているモデル：プラットフォーム モードの Firepower 2100 |
| IPSec およびキーリングの FQDN の適用 | ピアの FQDN がそのピアによって提示された x.509 証明書の DNS 名と一致する必要があるように、FQDN の適用を設定できます。IPSec の場合、9.13(1) より前に作成された接続を除き、適用はデフォルトで有効になっています。古い接続への適用は手動で有効にする必要があります。キーリングの場合、すべてのホスト名がFQDN である必要があり、ワイルドカードは使用できません。<br>新規/変更されたコマンド：**set dns**、**set e-mail**、**set fqdn-enforce**、**set ip**、**set ipv6**、**set remote-address**、**set remote-ike-id**<br>削除されたコマンド：**fi-a-ip**、**fi-a-ipv6**、**fi-b-ip**、**fi-b-ipv6**<br>サポートされているモデル：プラットフォーム モードの Firepower 2100 |

| 機能 | 説明 |
| --- | --- |
| 新しいIPSec暗号とアルゴリズム | 次の IKE および ESP 暗号とアルゴリズムが追加されました（設定不可）。<br>• 暗号：aes192。既存の暗号には、aes128、aes256、aes128gcm16 などがあります。<br>• 疑似乱数関数（PRF)（IKE のみ）：prfsha384、prfsha512、prfsha256。既存の PRF：prfsha1。<br>• 整合性アルゴリズム：sha256、sha384、sha512、sha1_160。既存のアルゴリズム：sha1。<br>• Diffie-Hellman グループ：curve25519、ecp256、ecp384、ecp521、modp3072、modp4096。既存のグループ：modp2048。<br>サポートされているモデル：プラットフォーム モードの Firepower 2100 |
| SSH 認証の機能拡張 | 次の SSH サーバ暗号化アルゴリズムが追加されました。<br>• aes128-gcm@openssh.com<br>• aes256-gcm@openssh.com<br>• chacha20-poly@openssh.com<br>次の SSH サーバ キー交換方式が追加されました。<br>• diffie-hellman-group14-sha256<br>• curve25519-sha256<br>• curve25519-sha256@libssh.org<br>• ecdh-sha2-nistp256<br>• ecdh-sha2-nistp384<br>• ecdh-sha2-nistp521<br>新規/変更されたコマンド：**set ssh-server encrypt-algorithm**、**set ssh-server kex-algorithm**<br>サポートされているモデル：プラットフォーム モードの Firepower 2100 |
| X.509 証明書の EDCS キー | 証明書に EDCS キーを使用できるようになりました。以前は、RSA キーだけがサポートされていました。<br>新規/変更されたコマンド：**set elliptic-curve**、**set keypair-type**<br>サポートされているモデル：プラットフォーム モードの Firepower 2100 |

| 機能 | 説明 |
| --- | --- |
| ユーザ パスワードの改善 | 次のようなパスワード セキュリティの改善が追加されました。<br>• ユーザ パスワードには最大 127 文字を使用できます。古い制限は 80 文字でした。<br>• デフォルトでは、強力なパスワード チェックが有効になっています。<br>• 管理者パスワードの設定を求めるプロンプトが表示されます。<br>• パスワードの有効期限切れ。<br>• パスワード再利用の制限。<br>• **set change-during-interval** コマンドを削除し、**set change-interval**、**set no-change-interval**、および **set history-count** コマンドの **disabled** オプションを追加しました。<br>新規/変更されたコマンド：**set change-during-interval**、**set expiration-grace-period**、**set expiration-warning-period**、**set history-count**、**set no-change-interval**、**set password**、**set password-expiration**、**set password-reuse-interval**<br>サポートされているモデル：プラットフォーム モードの Firepower 2100 |

# 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
- トランスペアレント

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

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

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

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

# ステートフル インスペクションの概要

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

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

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

- 新規の接続かどうか。

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

  セッション管理パスで行われるタスクは次のとおりです。

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

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

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

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

- 確立済みの接続かどうか。

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

  - IP チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック
  - 既存セッションに基づく NAT 変換

- レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

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

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

# VPN 機能の概要

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

ASA は、次の機能を実行します。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- 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