



CHAPTER 1

セキュリティ アプライアンスの概要

セキュリティ アプライアンスは、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つのデバイスに組み合わせたもので、一部のモデルでは、AIP SSM と呼ばれる統合侵入防御モジュールや、CSC SSM と呼ばれる統合コンテンツ セキュリティおよび制御モジュールが組み込まれています。セキュリティ アプライアンスの多数の高度な機能には、マルチ 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)、トランスペアレント (レイヤ 2) ファイアウォール動作またはルーテッド (レイヤ 3) ファイアウォール動作、高度なインスペクション エンジン、IPSec および WebVPN のサポート、その他の機能があります。サポートされているプラットフォームおよび機能のリストについては、付録 A 「機能のライセンスと仕様」を参照してください。新機能のリストについては、『Cisco ASA 5500 Series Release Notes』または『Cisco PIX Security Appliance Release Notes』を参照してください。



(注)

Cisco PIX 501 および PIX 506E セキュリティ アプライアンスはサポートされていません。

この章は、次の項で構成されています。

- 「ファイアウォール機能の概要」(P.1-1)
- 「VPN 機能の概要」(P.1-5)
- 「侵入防御サービスの機能概要」(P.1-6)
- 「セキュリティ コンテキストの概要」(P.1-6)

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 (*Demilitarized Zone* (DMZ; 非武装地帯) 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 へのアクセスを制限できますが、DMZ には公開サーバしかないため、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、認証または許可を義務づける、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。セキュリティ アプライアンスを使用すると、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。

この項では、次のトピックについて取り上げます。

- 「セキュリティ ポリシーの概要」 (P.1-2)
- 「ファイアウォール モードの概要」 (P.1-4)
- 「ステートフル インспекションの概要」 (P.1-4)

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セキュリティ アプライアンス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。この項では、次のトピックについて取り上げます。

- 「アクセス リストによるトラフィックの許可または拒否」 (P.1-2)
- 「NAT の適用」 (P.1-2)
- 「通過トラフィックに対する AAA の使用」 (P.1-3)
- 「HTTP、HTTPS、または FTP フィルタリングの適用」 (P.1-3)
- 「アプリケーション インспекションの適用」 (P.1-3)
- 「Advanced Inspection and Prevention Security Services Module (AIP SSM) へのトラフィック送信」 (P.1-3)
- 「Content Security and Control Security Services Module (CSC SSM) へのトラフィック送信」 (P.1-3)
- 「QoS ポリシーの適用」 (P.1-3)
- 「接続の制限と TCP 正規化の適用」 (P.1-4)

アクセス リストによるトラフィックの許可または拒否

アクセスリストは、内部から外部へのトラフィックを制限するため、または外部から内部へのトラフィックを許可するために使用できます。トランスペアレント ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。

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。

通過トラフィックに対する AAA の使用

HTTP など特定のタイプのトラフィックに対して、認証と許可のいずれかまたは両方を要求することができます。セキュリティ アプライアンスは、RADIUS サーバまたは TACACS+ サーバにアカウントリング情報を送信することもあります。

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。セキュリティ アプライアンスを、次のインターネット フィルタリング製品のいずれかを実行している別のサーバと連携させて使用することをお勧めします。

- Websense Enterprise
- Secure Computing SmartFilter

アプリケーション インспекションの適用

インспекション エンジンには、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、セキュリティ アプライアンスが詳細なパケット インспекションを行うことを要求します。

Advanced Inspection and Prevention Security Services Module (AIP SSM) へのトラフィック送信

使用しているモデルが侵入防御用の AIP SSM をサポートしている場合、トラフィックを AIP SSM に送信して検査することができます。

Content Security and Control Security Services Module (CSC SSM) へのトラフィック送信

使用しているモデルでサポートされていれば、CSC SSM により、ウイルス、スパイウェア、スパム、およびその他の不要トラフィックから保護されます。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するように適応型セキュリティ アプライアンスを設定しておきます。

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。

接続の制限と 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。セキュリティ アプライアンスでは、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。

ファイアウォール モードの概要

セキュリティ アプライアンスは、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
- 透過

ルーテッド モードでは、セキュリティ アプライアンス は、ネットワークのルータ ホップと見なされません。

トランスペアレント モードでは、セキュリティ アプライアンス 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。セキュリティ アプライアンスでは、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。

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。

ステートフル インспекションの概要

セキュリティ アプライアンス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。

ただし、セキュリティ アプライアンス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、セキュリティ アプライアンスは、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」でのセッション確立



(注) セッション管理パスおよびファスト パスが「アクセラレーションセキュリティパス」を構成します。

レイヤ 7 インспек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спек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、セキュリティアプライアンス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

UDP プロトコルまたは他のコネクションレス型プロトコルに対して、セキュリティアプライアンスはコネクションステート情報を作成して、高速パスも使用できるようにします。

レイヤ 7 インспек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спек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спек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。セキュリティアプライアンスは、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、トンネルを通じ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。セキュリティアプライアンスは、双方向のトンネル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側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が解除され、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。セキュリティアプライアンスは、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。

セキュリティアプライアンスが実行する機能は次のとおりです。

- 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
- トンネルを通じ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データと発信データの転送の管理

セキュリティ アプライアンスは、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。

侵入防御サービスの機能概要

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、拡張埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探すことにより、ネットワーク トラフィックのモニタおよびリアルタイム分析を行う侵入防御サービス モジュールの AIP SSM をサポートします。システムで不正なアクティビティが検出されると、侵入防御サービス機能は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを **Device Manager** に送信します。その他の正規の接続は、中断することなく独立した動作を継続します。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』を参照してください。

セキュリティ コンテキストの概要

1 台のセキュリティ アプライアンスを、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分割することができます。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、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチ コンテキスト モードの場合、セキュリティ アプライアンスには、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、セキュリティ アプライアンス 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あるときに（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。



(注)

管理者は、自分のコンテキストすべてをルーテッド モードまたはトランスペアレント モードで実行することができますが、一部のコンテキストを一方のモードで実行し、他のコンテキストをもう一方のモードで実行することはできません。

マルチ コンテキスト モードでは、スタティック ルーティングのみをサポートします。