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 つの装置に組み合せたもので、一部のモデルでは、AIP SSM と呼ばれる総合的な侵入防御モジュールや CSC SSM と呼ばれる総合的なコンテンツ セキュリティと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）、透過（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、高度な検査エンジン、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。

次の事項について説明します。

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（*Demiliterized 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 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。

ここでは、次の項目について説明します。

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。ここでは、次の項目について説明します。

アクセスリストによるトラフィックの許可または拒否

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、および外部から内部へのトラフィックを許可するために使用することができます。透過ファイアウォール 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。

スルー 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、認証と認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+ サーバにアカウンティ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推奨します。

- Websense Enterprise
- Secure Computing SmartFilter

アプリケーション検査の適用

検査エンジンは、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、セキュリティ アプライアンスが詳細なパケット検査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 へのトラフィック送信

使用しているモデルでこの機能をサポートしている場合、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優先順位を設定するネットワーク機能です。QoS は、特定のネットワーク 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を指します。

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す。

透過モードでは、セキュリティ アプライアンスは「bump-in-the-wire（BITW）」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。

透過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。透過モードは、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。透過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、透過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 インスペクションの概要

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。

しかし、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
- 「ファースト 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ースト 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 検査が必要なパケット（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 検査エンジンは、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、両方向でファースト パスを通過できます。ファースト 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、ファースト パスも使用できるようにします。

  レイヤ 7 検査を必要とするプロトコルに合致するデータ パケットもファースト 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、検査またはコンテンツ 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 検査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。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。

侵入防御サービス機能の概要

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、多数の埋め込みシグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックの監視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 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装置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装置です。マルチコンテキストは、複数のスタンドアロン装置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装置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。システム管理者は、システム コンフィギュレーションに設定することでコンテキストを追加および管理します。このコンフィギュレーションは、シングルモードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。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、自分自身のネットワーク インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要が生じたとき（サーバからコンテキストをダウンロードするときなど）は、管理コンテキストとして指定された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、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 モードまたは透過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 ルーティングのみサポートします。