Cisco ASA ファイアウォール サービスの概要

ファイアウォールサービスとは、トラフィックをブロックするサービス、内部ネットワークと外部ネットワーク間のトラフィック フローを可能にするサービスなど、ネットワークへのアクセス制御に重点を置いた ASA の機能です。これらのサービスには、サービス妨害（DoS）、その他の攻撃などの脅威からネットワークを保護するサービスが含まれています。

以降のトピックでは、ファイアウォール サービスの概要を示します。

- ファイアウォール サービスの実装方法 （1 ページ）
- 基本アクセス制御 （2 ページ）
- アプリケーション フィルタリング （3 ページ）
- URL フィルタリング （3 ページ）
- データ保護 （4 ページ）
- 仮想環境のファイアウォール サービス （5 ページ）
- ネットワーク アドレス変換 （5 ページ）
- アプリケーション インスペクション （6 ページ）
- 使用例：サーバの公開 （7 ページ）

ファイアウォール サービスの実装方法

次の手順は、ファイアウォールサービスを実装するための一般的な手順を示します。ただし、各手順は任意であり、サービスをネットワークに提供する場合にのみ必要です。

始める前に

一般的な操作の設定ガイドに従って ASA を設定してください（最小限の基本設定、インターフェイス コンフィギュレーション、ルーティング、管理アクセスなど）。

手順

ステップ 1 ネットワークのアクセス制御を実装します。基本アクセス制御 （2 ページ）を参照してください。

ステップ 2 アプリケーション フィルタリングを実装します。アプリケーション フィルタリング （3 ページ）を参照してください。

ステップ 3 URL フィルタリングを実装します。URL フィルタリング （3 ページ）を参照してください。

ステップ 4 脅威からの保護を実装します。データ保護 （4 ページ）を参照してください。

ステップ 5 仮想環境に適合するファイアウォール サービスを実装します。仮想環境のファイアウォール サービス （5 ページ）を参照してください。

ステップ 6 ネットワーク アドレス変換（NAT）を実装します。ネットワーク アドレス変換 （5 ページ）を参照してください。

ステップ 7 デフォルト設定がネットワークに十分でない場合は、アプリケーション インスペクションを実装します。「アプリケーション インスペクション （6 ページ）」を参照してください。

基本アクセス制御

インターフェイスごとに、またはグローバルに適用するアクセス ルールは、防御の最前線となります。エントリ時に、特定のタイプのトラフィック、または特定のホストあるいはネットワーク間のトラフィックをドロップできます。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。

アクセス ルールは、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。

基本的なアクセス ルールでは、送信元アドレスとポート、宛先アドレスとポート、およびプロトコルの「5タプル」を使用してトラフィックを制御します。アクセス ルールおよびアクセス コントロール リスト を参照してください。

ルールをアイデンティティ アウェアにすることで、ルールを増やすことができます。これにより、ユーザ アイデンティティまたはグループ メンバーシップに基づいてルールを設定できます。アイデンティティ制御を実装するには、次のいずれかの組み合わせを実行します。

- AD エージェントとも呼ばれる Cisco Context Directory Agent（CDA）を別のサーバにインストールして、 Active Directory（AD）サーバにすでに定義されているユーザおよびグループ情報を収集します。次に、この情報を取得するように ASA を設定し、ユーザまたはグループ基準をアクセス ルールに追加します。アイデンティティ ファイアウォールを参照してください。
- Cisco Identity Services Engine（ISE）を別のサーバにインストールして、Cisco Trustsec を実装します。その後、セキュリティ グループ基準をアクセス ルールに追加できます。ASA および Cisco TrustSecを参照してください。

- ASA FirePOWER モジュールを ASA にインストールして、モジュールのアイデンティティ ポリシーを実装します。ASA FirePOWER のアイデンティティアウェアなアクセス ポリシーは、モジュールにリダイレクトするトラフィックに適用されます。「ASA FirePOWER モジュール」を参照してください。

アプリケーション フィルタリング

Web ベース アプリケーションを広範に使用すると、大量のトラフィックが HTTP または HTTPS プロトコルで伝送されます。従来の 5 タプル アクセス ルールでは、すべての HTTP/HTTPS トラフィックを許可または拒否します。Web トラフィックをより細かく制御する必要がある場合があります。

モジュールを ASA にインストールしてアプリケーション フィルタリングを可能にし、使用されるアプリケーションに基づいて HTTP または他のトラフィックを選択的に許可することができます。したがって、HTTP を包括的に許可する必要はありません。トラフィック内部を監視し、ネットワークで受け入れられないアプリケーション（不適切なファイル共有など）を防止できます。アプリケーション フィルタリングのモジュールを追加する場合は、ASA で HTTP インスペクションを設定しないでください。

アプリケーション フィルタリングを実装するには、ASA FirePOWER モジュールを ASA にインストールし、ASA FirePOWER アクセス ルールでアプリケーション フィルタリング基準を使用します。これらのポリシーは、モジュールにリダイレクトするトラフィックに適用されます。「ASA FirePOWER モジュール」を参照してください。

URL フィルタリング

URL フィルタリングは、宛先サイトの URL をベースにしたトラフィックを拒否または許可します。

URL フィルタリングの目的は、主に Web サイトへのアクセスを完全にブロックまたは許可することです。個々のページをターゲットにすることができますが、通常はホスト名（www.example.com など）または特定のタイプのサービスを提供するホスト名の一覧を定義する URL カテゴリ（ギャンブルなど）を指定します。

HTTP/HTTPS トラフィックに対して、URL フィルタリングとアプリケーション フィルタリングのどちらを使用するかを決定する際は、その Web サイトに送信するすべてのトラフィックに適用するポリシーを作成するかどうかを考慮に入れてください。このようにすべてのトラフィックを同じように処理する（トラフィックを拒否または許可する）場合は、URL フィルタリングを使用します。トラフィックをサイトでブロックするか、許可するかを選択する場合は、アプリケーション フィルタリングを使用します。

URL フィルタリングを実装するには、次のいずれかの手順を実行します。

- ASA FirePOWER モジュールを ASA にインストールし、ASA FirePOWER アクセス ルールで URL フィルタリング基準を使用します。これらのポリシーは、モジュールにリダイレクトするトラフィックに適用されます。ASA FirePOWER モジュールを参照してください。

- 完全修飾ドメイン名（FQDN）に基づいて悪意のあるサイトをブロックするには、Cisco Umbrella サービスをサブスクライブし、エンタープライズ セキュリティ ポリシーを設定します。疑わしいと見なされた FQDN の場合は、ユーザ接続を Cisco Umbrella インテリジェント プロキシにリダイレクトし、URL フィルタリングを実行します。Umbrella サービスは、ユーザの DNS ルックアップ要求を処理し、ブロック ページの IP アドレスまたはインテリジェント プロキシの IP アドレスを返すことによって機能します。このサービスは、ホワイトリストに記載されたドメインの FQDN の実際の IP アドレスを返します。Cisco Umbrellaを参照してください。
- ScanCenter のフィルタリング ポリシーを設定するクラウド Web セキュリティ サービスに登録して、トラフィックをクラウド Web セキュリティ アカウントに送信するように ASA を設定します。ASA および Cisco クラウド Web セキュリティを参照してください

データ保護

スキャニング、サービス妨害（DoS）、および他の攻撃から保護するために多くの手段を実装できます。ASA の数多くの機能は、接続制限を適用して異常な TCP パケットをドロップすることで、攻撃から保護するのに役立ちます。一部の機能は自動ですが、ほとんどの場合でデフォルトが適切である設定可能な機能もあれば、完全に任意で必要な場合に設定する必要がある機能もあります。

次に、ASA で使用可能な脅威からの保護サービスを示します。

- IP パケット フラグメンテーションの保護：ASA は、すべての ICMP エラー メッセージの完全リアセンブリ、および ASA を介して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、セキュリティ チェックに失敗したフラグメントをドロップします。コンフィギュレーションは必要ありません。
- 接続制限、TCP 正規化、およびその他の接続関連機能：TCP と UDP の接続制限値とタイムアウト、TCP シーケンス番号のランダム化、TCP ステート バイパスなどの接続関連サービスを設定します。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ています。接続設定を参照してください。

  たとえば、TCP と UDP の接続、および初期接続（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）を制限できます。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。
- 脅威検出：攻撃を識別できるように統計情報の収集するために脅威検出を ASA に実装します。基本脅威検出はデフォルトでイネーブルになっていますが、高度な統計情報とスキャン脅威検出を実装できます。スキャン脅威であると特定されたホストを遮断できます。脅威の検出を参照してください。
- 次世代 IPS：ASA FirePOWER モジュールを ASA にインストールして、次世代 IPS の侵入ルールを ASA FirePOWER に実装します。これらのポリシーは、ASA FirePOWER にリダ

イレクトするトラフィックに適用されます。「ASA FirePOWER モジュール」を参照してください。

仮想環境のファイアウォール サービス

仮想環境は仮想マシンとしてサーバを導入します（VMware ESXi など）。仮想環境でのファイアウォールは、従来のハードウェア デバイスが可能ですが、ASAv などの仮想マシンのファイアウォールでも可能です。

従来のファイアウォールと次世代のファイアウォール サービスは、仮想マシン サーバを使用しない環境に適用する場合と同じ方法で、仮想環境に適用されます。ただし、仮想環境では、サーバの作成と切断が容易なため、追加の課題を提供できます。

さらに、データセンター内のサーバ間のトラフィックは、データセンターと外部ユーザ間のトラフィックと同じ程度の保護を必要とする可能性があります。たとえば、攻撃者がデータセンター内のあるサーバの制御を手に入れた場合、データセンターのその他のサーバに攻撃を広げる可能性があります。

仮想環境のファイアウォール サービスは、ファイアウォール保護を特に仮想マシンに適用する機能を追加します。以下に、仮想環境で使用可能なファイアウォール サービスを示します。

- 属性ベースのアクセス制御：属性に基づいて一致するトラフィックにネットワーク オブジェクトを設定し、アクセス制御ルールでこれらのオブジェクトを使用します。これにより、ネットワーク トポロジからファイアウォール ルールを分離することができます。たとえば、Engineering 属性を持つすべてのホストに Lab Server 属性を持つホストへのアクセスを許可できます。これらの属性を持つホストを追加および削除することができ、ファイアウォール ポリシーは、アクセス ルールを更新する必要なく自動的に適用されます。詳細については、属性ベースのアクセス制御を参照してください。

ネットワーク アドレス変換

ネットワーク アドレス変換（NAT）の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベート ネットワーク内のプライベート アドレスをパブリック インターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズすることができるからです。

NAT の他の機能には、次のおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。

- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定 IP アドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常どおりに適用されます。

次を参照してください。

- Network Address Translation（NAT）
- NAT の例と参照

アプリケーション インスペクション

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では、必要なピンホールを開く、およびネットワーク アドレス変換（NAT）を適用するために ASA で詳細なパケット インスペクションを行う必要があります。

デフォルトの ASA ポリシーは、すでに DNS、FTP、SIP、ESMTP、TFTP などの数多くの一般的なプロトコルのインスペクションをグローバルに適用しています。デフォルトのインスペクションでネットワークに必要なすべてが揃うことがあります。

ただし、他のプロトコルのインスペクションをイネーブルにしたり、インスペクションを微調整したりする必要がある場合があります。多くのインスペクションには、それらの内容に基づいてパケットを制御できる詳細なオプションがあります。プロトコルを十分に理解している場合には、そのトラフィックをきめ細かく制御できます。

サービス ポリシーを使用して、アプリケーション インスペクションを設定します。グローバル サービス ポリシーを設定するか、サービス ポリシーを各インターフェイスに適用するか、またはその両方を行うことができます。

次を参照してください。

- サービス ポリシー
- アプリケーション レイヤ プロトコル インスペクションの準備
- 基本インターネット プロトコルのインスペクション
- 音声とビデオのプロトコルのインスペクション
- モバイル ネットワークのインスペクション。

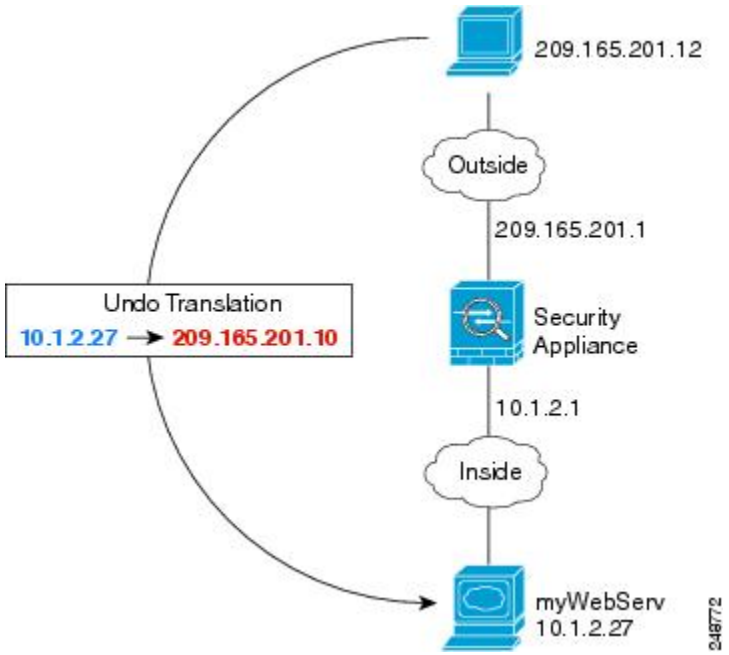
使用例：サーバの公開

一般公開されているサーバで特定のアプリケーション サービスを実行できます。たとえば、ユーザが Web ページに接続でき、それ以外のサーバへの接続を確立しないように Web ページを公開することができます。

サーバを一般公開するには、通常、接続および NAT ルールによってサーバの内部 IP アドレスと一般ユーザが使用できる外部アドレス間で変換を行うことができるアクセス ルールを作成する必要があります。さらに、外部に公開したサービスで内部サーバと同じポートを使用しない場合には、ポート アドレス変換（PAT）を使用して内部ポートを外部ポートにマッピングすることができます。たとえば、内部 Web サーバが TCP/80 で実行されていない場合、外部ユーザが容易にアクセスできるようにそのサーバを TCP/80 にマッピングできます。

次の例では、内部プライベート ネットワーク上の Web サーバをパブリック アクセスで使用可能にします。

図 *1 :* 内部 *Web* サーバのスタティック *NAT*



手順

ステップ 1 内部 Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

ステップ 2 オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

ステップ 3 外部インターフェイスに接続されているアクセス グループにアクセス ルールを追加して、サーバへの Web アクセスを許可します。

```
hostname(config)# access-list outside_access_in line 1 extended
permit tcp any4 object myWebServ eq http
```

ステップ 4 外部インターフェイスにアクセス グループがない場合は、access-group コマンドを使用してアクセス グループを適用します。

```
hostname(config)# access-group outside_access_in in interface outside
```