ファイアウォール サービス モジュールのトランスペアレント ファイアウォールの設定例

目次

概要

従来、ファイアウォールはルーテッド ホップであり、分割されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして動作するものです。 これに対し、トランスペアレント ファイアウォールは、*Bump In The Wire* または*ステルス ファイアウォール*のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。 Firewall Service Module（FWSM; ファイアウォール サービス モジュール）には、Inside インターフェイスと Outside インターフェイスで同じネットワークに接続します。 ファイアウォールはルーティング ホップではないので、透過型ファイアウォールを既存のネットワークに簡単に導入できます。 IP アドレスの再設定は必要ありません。

トラブルシューティングを行うための複雑なルーティング パターンが存在せず、NAT 設定も存在

しないため、メンテナンスは簡易化されます。

トランスペアレント モードはブリッジとして動作しますが、拡張アクセス リストを使用して明示的に許可しない限り、IP トラフィックなどのレイヤ 3 トラフィックは FWSM を通過できません。 アクセス リストを使用せずに透過型ファイウォールの通過を許可されている唯一のトラフィックは、ARP トラフィックです。 ARP トラフィックは、ARP インスペクションによって制御できます。

ルーテッド モードでは、アクセス リスト内で許可した場合でも、一部のタイプのトラフィックは FWSM を通過できません。 これに代わる方法として、拡張アクセス リスト（IP トラフィック用）または EtherType アクセス リスト（非 IP トラフィック用）を使用することで、透過型ファイアウォールによるトラフィックの通過の許可が可能になります。

たとえば、透過ファイアウォールを通してルーティング プロトコルの隣接関係を確立できます。拡張アクセス リストに基づいて、VPN（IPSec）、OSPF、RIP、EIGRP、または BGP トラフィックの通過が許可されます。 同様に、HSRP または VRRP などのプロトコルは、FWSM を通過できます。

非 IP トラフィック（たとえば、AppleTalk、IPX、BPDU、および MPLS）を EtherType アクセス リストを使用して通過するように設定できます。

透過型ファイアウォール上で直接サポートされない機能の場合、上流および下流のルータによって機能がサポートされるように、トラフィックの通過を許可することができます。 たとえば、拡張アクセス リストを使用すると、（サポートされない DHCP リレー機能ではなく）DHCP トラフィックまたは IP/TV によって作成されるようなマルチキャスト トラフィックを許可できます。

FWSM がトランスペアレント モードで実行されている場合、パケットの発信インターフェイスはルート ルックアップではなく MAC アドレスのルックアップによって判断されます。 route 文の設定は可能ですが、これらは FWSM から発信されたトラフィックにだけ適用されます。 たとえば、syslog サーバがリモート ネットワークに置かれている場合、FWSM がそのサブネットに到達できるように、スタティック ルートを使用する必要があります。

このルールの例外は、音声検査を使用する場合、およびエンドポイントが FWSM から 1 ホップ以上離れている場合です。 たとえば、CCM と H.323 ゲートウェイの間でトランスペアレント ファイアウォールを使用し、さらにトランスペアレント ファイアウォールと H.323 ゲートウェイの間にルータが存在する場合は、正常にコール完了するために、H.323 ゲートウェイの FWSM にスタティック ルートを追加する必要があります。

注: トランスペアレント モードの FWSM では、CDP パケットまたは 0x600 以上の有効な EtherType を含まないパケットは受け渡されません。 たとえば、IS-IS パケットは通過できません。 サポートされている BPDU の場合は例外となります。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、FWSM バージョン 3.x に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

トランスペアレント ファイアウォール

ブリッジ グループ

セキュリティ コンテキストのオーバーヘッドが不要な場合、またはセキュリティ コンテキストを最大限使用する場合は、ブリッジ グループと呼ばれる最大 8 ペアのインターフェイスを設定できます。 各ブリッジ グループは個別のネットワークに接続します。 ブリッジ グループのトラフィックは、その他のブリッジ グループからは分離されます。 トラフィックは FWSM 内のその他のブリッジ グループにはルーティングされません。そのため、外部ルータにより FWSM 内のその他のブリッジ グループにルーティングされる前に、トラフィックは FWSM を出る必要があります。 ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループで共有されています。 たとえば、システム ログ サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。 セキュリティ ポリシーを完全に分離するには、各コンテキストに 1 つのブリッジ グループを設定したセキュリティ コンテキストを使用します。

ファイアウォールはルーティング ホップではないので、透過型ファイアウォールを既存のネットワークに簡単に導入できます。 IP アドレスの再設定は必要ありません。 トラブルシューティングを行うための複雑なルーティング パターンが存在せず、NAT 設定も存在しないため、メンテナンスは簡易化されます。

注: 各ブリッジ グループには、管理 IP アドレスが必要です。 FWSM は、この IP アドレスをブリッジ グループから発信されるパケットの送信元アドレスとして使用します。 管理 IP アドレスは接続されたネットワークと同じサブネット上に配置される必要があります。

ガイドライン

透過型ファイアウォール ネットワークを計画する場合には、次のガイドラインに従ってください。

- 管理 IP アドレスは、各ブリッジ グループに必要です。各インターフェイスに IP アドレスが必要なルーテッド モードとは異なり、トランスペアレント ファイアウォールにはブリッジ グループ全体に割り当てられた IP アドレスがあります。 FWSM では、この IP アドレスをシステム メッセージまたは AAA 通信などの FWSM から発信されるパケットの送信元アドレスとして使用します。管理 IP アドレスは接続されたネットワークと同じサブネット上に配置される必要があります。 サブネットをホスト サブネット（255.255.255.255）に設定することはできません。 FWSM はセカンダリ ネットワークのトラフィックをサポートしていません。 管理 IP アドレスと同じネットワークのトラフィックのみがサポートされます。 管理 IP サブネットの詳細については、「ブリッジ グループへの IP アドレスの割り当て」を参照してください。

- 各ブリッジ グループでは、Inside インターフェイスと Outside インターフェイスだけが使用されます。
- 直接接続された各ネットワークは、同じサブネット上にある必要があります。
- ブリッジ グループの管理 IP アドレスは、接続されているデバイスのデフォルト ゲートウェイとして指定しないでください。 デバイスは、FWSM の相手側のルータをデフォルト ゲートウェイとして指定する必要があります。
- 管理トラフィックのリターン パスを提供する必要のあるトランスペアレント ファイアウォールのデフォルト ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックのみに適用されます。 これは、デフォルト ルートはブリッジ グループのインターフェイスだけでなく、ブリッジ グループ ネットワークのルータ IP アドレスも指定するため、1 つのデフォルト ルートしか定義できないためです。 複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、使用する管理トラフィックを送信するネットワークを識別するスタティック ルートを指定する必要があります。
- マルチ コンテキスト モードの場合、各コンテキストが異なるインターフェイスを使用する必要があります。 コンテキストをまたいでインターフェイスを共有することはできません。
- マルチ コンテキスト モードの場合、一般的に各コンテキストでは異なるサブネットが使用されます。 オーバーラップするサブネットを使用できますが、ルーティングの観点からは、この実現にはネットワーク トポロジにルータおよび NAT の設定が必要です。IP トラフィックなどのレイヤ 3 トラフィックの FWSM の通過を許可するには、拡張アクセス リストを使用する必要があります。 オプションとして、非 IP トラフィックの通過を許可するには、EtherType アクセス リストを使用することもできます。

許可された MAC アドレス

次の宛先 MAC アドレスは、透過なファイアウォールを通過することが許可されています。 このリストに含まれていない MAC アドレスは廃棄されます。

- FFFF.FFFF.FFFF に等しい TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ~ 0100.5EFE.FFFF の IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ~ 3333.FFFF.FFFF の IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD に等しい BPDU マルチキャスト アドレス
- 0900.0700.0000 ~ 0900.07FF.FFFF の Appletalk マルチキャスト MAC アドレス

サポートされない機能

次の機能は、透過モードではサポートされていません。

- NAT/PATNAT は上流のルータで実行されます。**注:** NAT/PAT は、FWSM バージョン 3.2 以降のリリースのトランスペアレント ファイアウォールでサポートされています。
- ダイナミック ルーティング プロトコル (RIP、EIGRP、OSPF など) FWSM から発信されたトラフィックのスタティック ルートを追加できます。 拡張アクセス リストを使用して、ダイナミック ルーティング プロトコルの FWSM の通過を許可することもできます。
- ブリッジ グループ IP アドレスの IPv6ただし、EtherType アクセス リストを使用して、IPv6 EtherType を渡すことはできます。
- DHCP リレートランスペアレント ファイアウォールは DHCP サーバとして動作できますが、DHCP リレー コマンドはサポートされません。 拡張アクセス リストを使用して DHCP トラフィックの通過を許可できるため、DHCP リレーは必要ありません。
- Quality of Service (QoS)

- マルチキャスト拡張アクセス リスト内で許可すると、マルチキャスト トラフィックによる FWSM の通過を許可できます。 詳細は、「トラフィックの通過」セクションを参照してください。
- 通過するトラフィックの VPN 終端透過型ファイアウォールでは、管理接続専用のサイト間 VPN トンネルがサポートされています。 FWSM を通過するトラフィックの VPN 接続は終端されません。 拡張アクセス リストを使用して FWSM を通過する VPN トラフィックを許可できますが、非管理接続は終端されません。
- スイッチのループガードFWSM がトランスペアレント モードの場合は、スイッチでループガードをグローバルにイネーブルにしないでください。 ループガードは、スイッチと FWSM 間の内部 EtherChannel に自動的に適用されます。そのため、フェールオーバーおよびフェールバックの後は、ループガードによりセカンダリ ユニットが切断されます（EtherChannel が err-disable ステートになるため）。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

次のネットワーク図は、外部デバイスが内部デバイスと同じサブネットにある一般的な透過型ファイアウォール ネットワークを示しています。 Inside ルータおよびホストは、Outside ルータに直接接続されているように表示されています。

設定

各コンテキストは、ルーテッド ファイアウォール モード（デフォルト）またはトランスペアレント ファイアウォール モードで実行するように設定できます。

多くのコマンドが両方のモードではサポートされないため、モードを変更すると FWSM によって設定がクリアされます。 すでにデータが入力された設定が用意されている場合、モードを変更する前に必ずその設定をバックアップしてください。 新しい設定を作成する際に、このバックアップ設定を参照用に使用できます。

firewall transparent コマンドを使用してモードを変更した FWSM にテキスト設定をダウンロードする場合は、必ず設定の一番上にコマンドを入力してください。 FWSM でコマンドが読み込まれると、モードがただちに変更され、その後ダウンロードした設定の読み込みが続行されます。 設定の後ろの方にコマンドが入力されていると、FWSM により、設定内のこのコマンドよりも前の行がすべてクリアされます。

モードをトランスペアレントに設定するには、各コンテキストに次のコマンドを入力します。

```
hostname(config)#firewall transparent
```

モードをルーテッドに設定するには、各コンテキストに次のコマンドを入力します。

```
hostname(config)#no firewall transparent
```

さまざまなシナリオにおける透過型ファイアウォールを通過する

データ

Inside ユーザの Outside 電子メール サーバへのアクセス

Inside ネットワーク上のユーザがインターネット（Outside）に配置された電子メール サーバへアクセスします。 FWSM によってパケットが受信され、必要な場合は送信元 MAC アドレスが MAC アドレス テーブルに追加されます。 これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、または AAA）の条件に従ってパケットが許可されていることが確認されます。

注: マルチ コンテキスト モードの場合、一意のインターフェイスに従って、まず FWSM によってパケットが分類されます。

FWSM によってセッションが確立したことが記録されます。 宛先 MAC アドレスがそのテーブル内に存在する場合、FWSM によってパケットが Outside インターフェイスから転送されます。 宛先 MAC アドレスは、上流のルータ 192.168.1.2 の宛先 MAC アドレスです。 宛先 MAC アドレスが FWSM テーブル内に存在しない場合、ARP 要求と ping の送信時に FWSM によって MAC アドレスの検索が試行されます。 最初のパケットはドロップされます。

電子メール サーバが要求に応答します。 セッションがすでに確立されているため、パケットによって新しい接続に関連付けられている多くのルックアップがバイパスされます。 FWSM によってパケットが Inside ユーザに転送されます。

内部ユーザは NAT の電子メールサーバを参照します

インターネット ルータで NAT を有効にすると、インターネット ルータを通過するパケットのフローがわずかに変わります。

Inside ネットワーク上のユーザがインターネット（Outside）に配置された電子メール サーバへアクセスします。 FWSM によってパケットが受信され、必要な場合は送信元 MAC アドレスが MAC アドレス テーブルに追加されます。 これは新しいセッションであるため、セキュリティ ポリシー（アクセス リスト、フィルタ、または AAA）の条件に従ってパケットが許可されていることが確認されます。

注: マルチ コンテキスト モードの場合、一意のインターフェイスに従って、まず FWSM によってパケットが分類されます。

インターネット ルータは、Host A のリアル アドレス（192.168.1.5）を、インターネット ルータのマッピングされたアドレス（172.16.1.1）に変換します。 マッピングされたアドレスは、Outside インターフェイスと同じネットワーク上には存在しないため、FWSM をポイントするマッピングされたネットワークへのスタティック ルートが上流のルータに含まれていることを確認してください。

FWSM によってセッションが確立したことが記録され、Outside インターフェイスからパケットが転送されます。 宛先 MAC アドレスがそのテーブル内に存在する場合、FWSM によってパケットが Outside インターフェイスから転送されます。 宛先 MAC アドレスは、上流のルータ 172.16.1.1 の宛先 MAC アドレスです。 宛先 MAC アドレスが FWSM テーブル内に存在しない場合、ARP 要求と ping の送信時に FWSM によって MAC アドレスの検索が試行されます。 最初のパケットはドロップされます。

電子メール サーバが要求に応答します。 セッションがすでに確立されているため、パケットによ

って新しい接続に関連付けられている多くのルックアップがバイパスされます。 FWSM は NAT を実行して、マッピングされたアドレスをリアル アドレスである 192.168.1.5 に変換します。

Inside ユーザによる Inside Web サーバへのアクセス

ホストA が内部Webサーバにアクセスすることを試みれば（ 10.1.1.1 ）、ホストA （ 192.168.1.5 ）内部からの外部に FWSM によってインターネットルータに要求パケットを（ それがデフォルト ゲートウェイであるので ）送ります。 それからパケットは Webサーバにリダイレクトされます（ 10.1.1.1 ） FWSM （ 外部で内部に ）および内部ルータを通して。

注: 要求パケットは Webサーバに FWSM に外部からの内部へのトラフィックを許可するアクセスリストがあるときだけ戻ります。

この問題を解決するには、Host A（ 10.1.1.1 ）のデフォルト ゲートウェイをインターネット ルータ（ 192.168.1.2 ）ではなく、内部ルータ（ 192.168.1.3 ）へ変更します。 これによって、Outside ゲートウェイに送信される不必要なトラフィックが回避され、Outside ルータ（ インターネット ルータ ）上での発生がリダイレクトされます。 また、逆方向、つまり内部ルータの Inside に存在する Web サーバまたは任意のホスト（ 10.1.1.0/24 ）がホスト A（ 192.168.1.5 ）にアクセスしようとする場合も解決されます。

Outside ユーザによる Inside ネットワーク上の Web サーバへのアクセス

次の手順では、データが FWSM をどのように通過するのかを説明しています。

1. Outside ネットワーク上のユーザが、Inside Web サーバに Web ページを要求します。 FWSM によってパケットが受信され、必要な場合は送信元 MAC アドレスが MAC アドレス テーブルに追加されます。 これは新しいセッションであるため、セキュリティ ポリシー（ アクセス リスト、フィルタ、または AAA ）の条件に従ってパケットが許可されていることが確認されます。**注:** マルチ コンテキスト モードの場合、一意のインターフェイスに従って、まず FWSM によってパケットが分類されます。
2. Outside ユーザが内部 Web サーバへの有効なアクセス権を持っている場合のみ、FWSM によってセッションが確立したことが記録されます。 アクセス リストは、Outside ユーザによる Web サーバへのアクセスを許可するように設定する必要があります。
3. 宛先 MAC アドレスがそのテーブル内に存在する場合、FWSM によってパケットが Inside インターフェイスから転送されます。 宛先 MAC アドレスは、下流のルータ 192.168.1.3 の宛先 MAC アドレスです。
4. 宛先 MAC アドレスが FWSM テーブル内に存在しない場合、ARP 要求と ping の送信時に FWSM によって MAC アドレスの検索が試行されます。 最初のパケットはドロップされます。
5. Web サーバが要求に応答します。 セッションがすでに確立されているため、パケットによって新しい接続に関連付けられている多くのルックアップがバイパスされます。 FWSM によってパケットが Outside ユーザに転送されます。

Outside ユーザによる Inside ホストへのアクセスの試行

Outside ネットワーク上のユーザが Inside ホストへアクセスしようとします。 FWSM によってパケットが受信され、必要な場合は送信元 MAC アドレスが MAC アドレス テーブルに追加されます。 これは新しいセッションであるため、セキュリティ ポリシー（ アクセス リスト、フィルタ、または AAA ）の条件に従ってパケットが許可されているかどうかが確認されます。

注: マルチ コンテキスト モードの場合、一意のインターフェイスに従って、まず FWSM によってパケットが分類されます。

パケットが拒否され、Outside ユーザが Inside ホストへのアクセス権を持っていないため、FWSM によってパケットがドロップされます。 Outside ユーザが Inside ネットワークを攻撃しようとする場合、FWSM ではさまざまなテクノロジーを利用して、パケットがすでに確立されたセッションに有効であるかどうかが判断されます。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

```
cisco(config)#show firewall Firewall mode: Transparent
```

トラブルシューティング

トラフィックの通過

トランスペアレント ファイアウォールでマルチキャスト トラフィックを受け渡すには、high から low および low から high のアクセス リストが必要です。 通常のファイアウォールでは、high から low は必要ありません。

注: マルチキャスト アドレス（224.0.0.9）は、リターン トラフィックの送信元アドレスになることはないため、リターン トラフィックの戻りは許可されません。そのため、In から Out、Out から In への ACL が必要になります。

たとえば、RIP トラフィックを通過させるには、トランスペアレント ファイアウォールのアクセス リストは次の例のようになります。

RIP

Outside ACL（Out から In）：

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

Inside ACL（Inside から Outside）：

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

実行する EIGRP：

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
 access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

OSPF の場合：

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
```

```
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
 access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside sourec ) host ( inside source )
access-group outside in interafce outside
```

MSFC VLAN と FWSM VLAN

トランスペアレント モードでは、VLAN がブリッジングのタイプとなるため、MSFC インターフェイスと FWSM で同じ VLAN を持つ必要があります。

関連情報

- Cisco PIX Firewall ソフトウェア
- Requests for Comments (RFC)
- セキュリティ製品に関する Field Notice (PIX を含む)
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- PIX/ASA： 透過型ファイアウォールの設定例
- テクニカルサポートとドキュメント - Cisco Systems