CHAPTER 16

ファイアウォール モードの概要

この章では、ファイアウォール モードの設定方法と各ファイアウォール モードでファイアウォールがどのように機能するかを説明します。ファイアウォール モードは、マルチコンテキスト モードのコンテキストごとに個別に設定できます。

FWSM（またはマルチモードの各コンテキスト) は、2 つのファイアウォール モードのいずれかで動作できます。

- ルーテッド モード
- 透過モード

この章には、次の項があります。

ルーテッド モードの概要

ルーテッド モードでは、FWSM はネットワーク内のルータ ホップと見なされます。（シングルコンテキスト モードでは）OSPF または受動 RIP を使用できます。ルーテッド モードは、多数のインターフェイスをサポートしており、各インターフェイスは、それぞれ異なるサブネット上に置かれます。コンテキスト間でインターフェイスを共有することもできますが、いくつかの制限事項があります。

FWSM は、接続されたネットワーク間のルータとして機能します。インターフェイスごとに、異なるサブネット上の IP アドレスが必要です。シングルコンテキスト モードでは、ルーテッド ファイアウォールは OSPF および RIP をサポートします（パッシブ モードで）。マルチコンテキスト モードでは、スタティック ルートだけがサポートされます。過度なルーティングのニーズを FWSM に頼るのではなく、アップストリーム ルータとダウンストリーム ルータの拡張ルーティング機能を使用することをお勧めします。

透過モードの概要

透過ファイアウォールは、「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 ホップとは見なされません。

ここでは、透過ファイアウォール モードについて説明します。次の項目を取り上げます。

透過ファイアウォール ネットワーク

FWSM 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ルーティングされたホップではないので、既存のネットワークに簡単に導入できます。IP 再アドレッシングは必要ありません。

透過ファイアウォールに接続されているホストの NAT をオプションでイネーブルにできます。

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を避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、ブリッジ グループと呼ばれる最大 8 つのペアのインターフェイスを設定できます。各ブリッジ グループは別々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、他のブリッジ グループから隔離され、トラフィックは FWSM 内の他のブリッジ グループにルーティングされません。また、トラフィックは、外部ルータから FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。ブリッジング機能はブリッジ グループごとに別々のものですが、他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、すべてのブリッジ グループはシステム ログ サーバまたは AAA サーバ コンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキストで単一ブリッジ グループを持つセキュリティ コンテキストを使用します。

透過ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。IP 再アドレッシングは必要ありません。トラブルシューティングが必要な複雑なルーティング パターンがないため、メンテナンスが容易です。

（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、接続されているネットワークと同じサブネット内にある必要があります。

レイヤ 3 トラフィックの許可

透過モードはブリッジとして機能しますが、IP トラフィックなどのレイヤ 3 トラフィックは、拡張アクセスリストで明示的に許可されない限り、FWSM を通過できません。アクセスリストなしで透過ファイアウォールを通過できるトラフィックは ARP トラフィックだけです。ARP トラフィックは ARP 検査によって制御されます。

許可された MAC アドレス

次の宛先 MAC アドレスは、透過ファイアウォールから許可されます。このリストにない MAC アドレスはすべてドロップされます。

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

ルーテッド モードで許可されていないトラフィックの通過

ルーテッド モードでは、アクセスリストで許可しても、いくつかのタイプのトラフィックは FWSM を通過できません。一方、透過ファイアウォールは、拡張アクセスリスト（IP トラフィックの場合）または EtherType アクセスリスト（IP 以外のトラフィックの場合）を使用して、ほとんどのタイプのトラフィックを通過させることができます。

（注）　透過モードの FWSM は、CDP パケット、または 0x600 以上の有効な EtherType を持たないパケットは通過させません。たとえば、IS-IS パケットを通過させることはできません。サポートされている BPDU は例外です。

たとえば、透過ファイアウォールでルーティング プロトコルの隣接関係を確立できます。つまり、拡張アクセスリストに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックを許可することができます。同様に、HSRP や VRRP などのプロトコルは FWSM を通過できます。

IP 以外のトラフィック（AppleTalk、IPX、BPDU、および MPLS など）は、EtherType アクセスリストを使用して通過するように構成できます。

透過ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートでき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して、（サポートされない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV によって作成されたマルチキャスト トラフィックを許可したりできます。

MAC アドレスとルート ルックアップ

FWSM が NAT を使用せずに透過モードで動作している場合、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 ルックアップを実行することによって決定されます。この場合もルート文を設定することはできますが、FWSM から発信されたトラフィックだけに適用されます。たとえば、syslog サーバがリモート ネットワークにある場合は、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、音声検査を使用している場合とエンドポイントが FWSM から少なくとも 1 ホップ離れている場合です。たとえば、CCM と H.323 ゲートウェイの間に透過ファイアウォールを使用し、透過ファイアウォールと H.323 ゲートウェイの間にルータがあり、コールをうまく完了するために 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る場合です。

NAT を使用する場合は、FWSM は MAC アドレス ルックアップではなく、ルート ルックアップを使用します。場合によっては、スタティック ルートが必要になります。たとえば、実際の宛先アドレスが FWSM に直接接続されていない場合は、ダウンストリーム ルータをポイントする実際の宛先アドレスの FWSM にスタティック ルートを追加する必要があります。

ネットワークでの透過ファイアウォールの使用

図 16-1 に、外部デバイスが内部デバイスと同じサブネット上にある一般的な透過ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 16-1　透過ファイアウォール ネットワーク

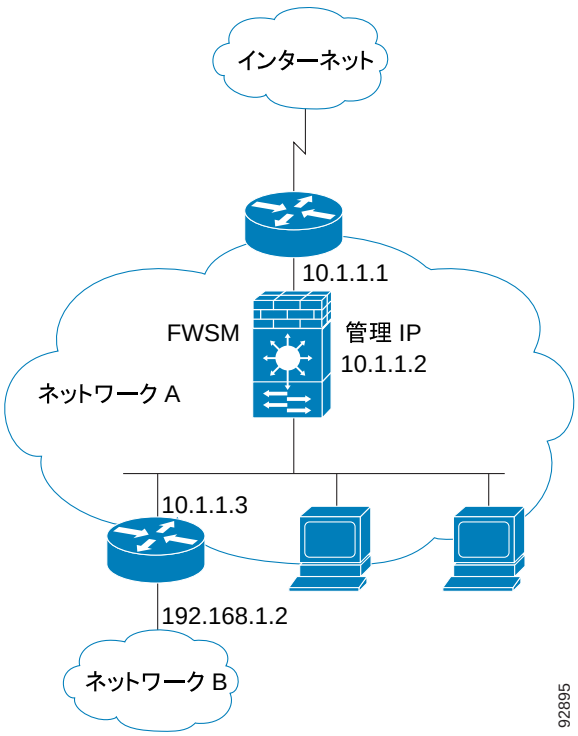
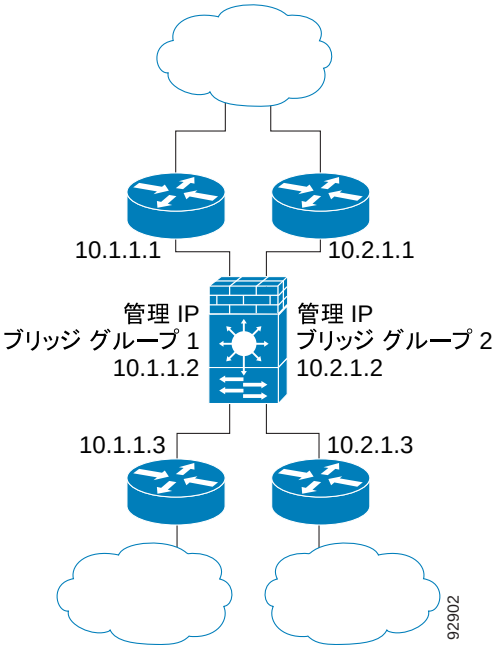


図 16-2 は、2 つのブリッジ グループを持つ FWSM に接続された 2 つのネットワークを示しています。

図 16-2　2 つのブリッジ グループを持つ透過ファイアウォール ネットワーク



透過ファイアウォール ガイドライン

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

- ブリッジ グループごとに管理 IP アドレスが必要です。

  インターフェイスごとに IP アドレスが必要なルーテッド モードと異なり、透過ファイアウォールではブリッジ グループ全体に IP アドレスが割り当てられます。FWSM は、この IP アドレスを、システム メッセージや AAA 通信など、FWSM で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、接続されているネットワークと同じサブネット内にある必要があります。管理 IP サブネットの詳細については、P.5-7 の「ブリッジ グループの追加または編集」を参照してください。
- 各ブリッジ グループは、内部インターフェイスと外部インターフェイスだけを使用します。
- 直接に接続された各ネットワークは同一のサブネット上にある必要があります。
- 接続されたデバイス用のデフォルト ゲートウェイとしてブリッジ グループ管理 IP アドレスを指定しないでください。デバイスは FWSM の他方の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。
- 透過ファイアウォールのデフォルト ルートは、管理トラフィックにリターンパスを提供しなければならないため、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にだけ適用されます。デフォルト ルートがブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定するため、デフォルト ルートを 1 つしか定義できません。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ある場合は、そこからの管理トラフィックを想定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 モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間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 モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。
- 拡張アクセスリストを使用し、IP トラフィックなどのレイヤ 3 トラフィックが FWSM を通過できるようにする必要があります。

  オプションで、EtherType アクセスリストを使用して IP 以外のトラフィックの通過を許可することもできます。

透過モードでサポートされていない機能

表 16-1 に透過モードでサポートされていない機能を示します。

表 16-1　透過モードでサポートされていない機能

サポートされていない機能	説明
ダイナミック ルーティング プロトコル	ただし、FWSM で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 プロトコルが FWSM を通過できるように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 を通過させることができます。
DHCP リレー	透過ファイアウォールは DHCP サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。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 リレーは不要です。
スイッチのループガード	FWSM が透過モードの場合は、スイッチの LoopGuard 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、EtherChannel が err-disable 状態になると、フェールオーバーおよびフェールバック後にセカンダリ装置がループガードによって切断されます。
マルチキャスト	ただし、拡張アクセスリストで許可することによって、マルチキャスト トラフィックが FWSM を通過できるようにすることができます。
管理用リモート アクセス VPN	管理用サイトツーサイト VPN を使用できます。

CLI での透過またはルーテッド ファイアウォール モードの設定

ASDM のシングルモードでは、モードの変更はできません。マルチモードでは、ASDM の管理コンテキストモードでのモード変更はできません。CLI でモードの変更をする必要があります。

モードを変更すると、FWSM はコンフィギュレーションをクリアします。これは、多くのコマンドが両方のモードでサポートされていないためです。すでに実装済みのコンフィギュレーションがある場合は、モードを変更する前に必ずコンフィギュレーションのバックアップを作成してください。新しくコンフィギュレーションを作成するときにこのバックアップを参照する場合があります。

firewall transparent コマンドでモードを変更する FWSM にテキスト コンフィギュレーションをダウンロードする場合は、必ずこのコマンドをコンフィギュレーションの最上部に置いてください。これによって、FWSM は、このコマンドを読み取り次第すぐにモードを変更し、その後は、ダウンロードしたコンフィギュレーションの読み取りを続けます。このコマンドがコンフィギュレーションの後ろの方にあると、FWSM はそれ以前に記述されているコンフィギュレーションの行をすべてクリアします。

- 透過モードに設定するには、各コンテキストで次のコマンドを入力します。

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

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

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