CHAPTER 22

ARP 検査およびブリッジング パラメータの設定

この章では、ARP 検査をイネーブルにする方法と、透過ファイアウォール モードでの FWSM のブリッジング オペレーションをカスタマイズする方法について説明します。マルチコンテキスト モードでは、この章のコマンドはシステム実行スペースではなくセキュリティ コンテキストで入力できます。

透過ファイアウォール モードの詳細については、第 16 章「ファイアウォール モードの概要」を参照してください。

この章には、次の項があります。

ARP 検査の設定

この項では、ARP 検査について説明し、これをイネーブルにする方法について説明します。次の事項を取り上げます。

ARP Inspection

ARP Inspection ペインでは、ARP 検査を設定できます。

デフォルトでは、すべての ARP パケットが FWSM を通過できます。ARP パケットのフローを制御するには、ARP 検査をイネーブルにします。

ARP 検査をイネーブルにすると、FWSM はすべての ARP パケットの MAC アドレス、IP アドレス、および発信元インターフェイスを ARP テーブルのスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および発信元インターフェイスが ARP エントリと一致した場合、パケットは通過します。
- MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、FWSM はパケットをドロップします。
- ARP パケットがスタティック ARP テーブルのどのエントリとも一致しない場合は、パケットをすべてのインターフェイスに転送するか（フラッド）、パケットをドロップするように FWSM を設定できます。

ARP 検査は、悪意のあるユーザが他のホストまたはルータになりすますこと（ARP スプーフィング）を防ぎます。ARP スプーフィングは、「man-in-the-middle」攻撃（介入者攻撃）を可能にすることがあります。たとえば、ホストは ARP 要求をゲートウェイ ルータに送信し、ゲートウェイ ルータはゲートウェイ ルータ MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスの代わりに攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これによって、攻撃者は、すべてのホスト トラフィックを傍受してからルータに転送できます。

ARP 検査を行うと、正しい MAC アドレスとそれに関連付けられている IP アドレスがスタティック ARP テーブルにある限り、攻撃者は、攻撃者の MAC アドレスで ARP 応答を送信することができなくなります。

フィールド

- Interface：インターフェイス名を示します。
- ARP Inspection Enabled：ARP 検査がイネーブルになっているかどうかを Yes または No で示します。
- Flood Enabled：ARP 検査がイネーブルになっている場合には、アクションで未知のパケットをフラッドするようになっているかどうかを Yes または No で示します。ARP 検査がディセーブルになっている場合は、この値は常に No です。
- Edit：選択したインターフェイスの ARP 検査パラメータを編集します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Edit ARP Inspection Entry

Edit ARP Inspection Entry ダイアログボックスでは、ARP 検査の設定値を設定できます。

フィールド

- Enable ARP Inspection：ARP 検査をイネーブルにします。
- Flood ARP Packets：スタティック ARP エントリのどの要素にも一致しないパケットが、送信元のインターフェイスを除くすべてのインターフェイスからフラッドするように指定します。MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、FWSM はパケットをドロップします。このチェックボックスをオフにすると、一致しないすべてのパケットがドロップされます。

（注） デフォルト設定では、一致しないパケットはフラッドします。スタティック エントリにある ARP だけが FWSM を通過するように制限するには、このコマンドを **no-flood** に設定します。

専用の管理インターフェイスがある場合、このインターフェイスは、このパラメータがフラッドに設定されていてもパケットをフラッドしません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

ARP Static Table

ホストは、パケットの宛先を IP アドレスで識別しますが、イーサネット上でパケットが実際にどこに配信されるかは、イーサネットの MAC アドレスで決まります。ルータやホストが直接接続されているネットワークにパケットを配信する場合は、そのパケットの IP アドレスに関連付けられている MAC アドレスを尋ねる ARP 要求を送信します。次に、ARP 応答に従って、MAC アドレスにパケットを配信します。ホストやルータは、パケットを配信するたびに ARP 要求を送信しなくてもよいように、ARP テーブルを保持しています。ARP テーブルは、ARP 応答がネットワークに送信されるたびにダイナミックに更新され、一定の期間使用されなかったエントリはタイムアウトになります。エントリが正しくなくなった場合（IP アドレスに関連付けられていた MAC アドレスが変更された場合など）は、更新される前にタイムアウトになります。

（注）　透過ファイアウォールは、FWSM との間のトラフィック（管理トラフィックなど）に、ARP テーブルのダイナミック ARP エントリを使用します。

ARP Static Table ペインでは、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするスタティック ARP エントリを追加できます。スタティック ARP エントリはタイムアウトしないため、ネットワーク問題の解決に役立つ場合があります。

フィールド

- Interface：ホスト ネットワークに接続されたインターフェイスを示します。
- IP Address：ホストの IP アドレスを示します。
- MAC Address：ホストの MAC アドレスを示します。
- Proxy ARP：FWSM が、このアドレスでプロキシ ARP を実行するかどうかを示します。FWSM は、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。
- Add：スタティック ARP エントリを追加します。
- Edit：スタティック ARP エントリを編集します。
- Delete：スタティック ARP エントリを削除します。
- ARP Timeout：FWSM が ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは 14400 秒です。ARP テーブルが再構築されると、新しいホスト情報に自動的に更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることができます。このパラメータは ARP Static Table ペインに表示されますが、タイムアウトはダイナミック ARP テーブルに適用されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ARP Static Configuration

Add/Edit ARP Static Configuration ダイアログボックスでは、スタティック ARP エントリを追加または編集できます。

フィールド

- Interface：ホスト ネットワークに接続されるインターフェイスを設定します。
- IP Address：ホストの IP アドレスを設定します。
- MAC Address：ホストの MAC アドレスを設定します（00e0.1e4e.3d8b など）。
- Proxy ARP：FWSM がこのアドレスでプロキシ ARP を実行できるようにします。FWSM は、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MAC アドレス テーブルのカスタマイズ

ここでは、次の項目について説明します。

概要

通常、ファイアウォールはルーティングされたホップであり、スクリーニング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機能します。一方、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。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。

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 syslog サーバまたは AAA サーバの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 パターンや NAT コンフィギュレーションがないので、メンテナンスが容易です。

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。

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、すべてのトラフィックを許可することができます。

（注）　透過モードの FWSM は、CDP パケットを通過させません。

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、DHCP トラフィック（サポートされない DHCP リレー機能の代わりに）または 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できます。

FWSM が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。

ブリッジングの下に、たとえば、スタティック MAC アドレス エントリを追加するか、または ARP 検査をイネーブルにすることで、透過ファイアウォールをカスタマイズできます。

前提条件

マルチコンテキスト モードの ASDM で、管理外コンテキストに対してファイアウォール モードを変更できます。シングルモードで、または管理コンテキストに対して、ルーテッドから透過にモードを変更するには、FWSM CLI にアクセスして **firewall transparent** コマンドを入力します。透過からルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

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。

MAC Address Table

MAC Address Table ペインでは、スタティック MAC アドレスのエントリを追加できます。通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。必要に応じて、スタティック MAC アドレスを MAC アドレス テーブルに追加できます。

FWSM は、通常のブリッジやスイッチと同様の方法で、MAC アドレス テーブルをラーニングし、構築します。デバイスが FWSM 経由でパケットを送信すると、FWSM はこの MAC アドレスをテーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、FWSM は、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。

FWSM はファイアウォールなので、パケットの宛先 MAC アドレスがテーブルにない場合、FWSM は通常のブリッジとは異なり、元のパケットをすべてのインターフェイスにフラッドすることはありません。代わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット:FWSM は宛先 IP アドレスに対して ARP 要求を生成し、FWSM は ARP 応答を受信したインターフェイスをラーニングします。
- リモート デバイスへのパケット : FWSM は宛先 IP アドレスへの ping を生成し、FWSM は ping 応答を受信したインターフェイスをラーニングします。

元のパケットはドロップされます。

フィールド

- Interface：MAC アドレスに関連付けられたインターフェイスを示します。
- MAC Address：MAC アドレスを表示します。
- Add：スタティック MAC アドレス エントリを追加します。
- Edit：スタティック MAC アドレス エントリを編集します。
- Delete：スタティック MAC アドレス エントリを削除します。
- Dynamic Entry Timeout：タイムアウトするまでに、MAC アドレス エントリが MAC アドレス テーブルに残る時間を 5 ～ 720 分（12 時間）の範囲で設定します。5 分がデフォルトです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Add/Edit MAC Address Entry

Add/Edit MAC Address Entry ダイアログボックスでは、スタティック MAC アドレス エントリを追加または編集できます。通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック エントリを追加する利点の 1 つとして、MAC スプーフィングの防止があります。スタティック エントリと同じ MAC アドレスを持つクライアントが、スタティック エントリと一致しないインターフェイスにトラフィックを送信しようとした場合、FWSM はトラフィックをドロップし、システム メッセージを生成します。

フィールド

- Interface：MAC アドレスに関連付けられたインターフェイスを設定します。
- MAC Address：MAC アドレスを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

MAC Learning

MAC Learning ペインでは、インターフェイスでの MAC アドレス ラーニングをディセーブルにすることができます。デフォルトにより、各インターフェイスは送信されてきたトラフィックの MAC アドレスを自動的にラーニングし、FWSM は、対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MAC アドレスをテーブルにスタティックに追加しないと、トラフィックが FWSM を通過できなくなります。

フィールド

- Interface：インターフェイス名を示します。
- MAC Learning Enabled：MAC ラーニングがイネーブルになっているかどうかを Yes または No で示します。
- Enable：選択したインターフェイスに対する MAC ラーニングをイネーブルにします。
- Disable：選択したインターフェイスに対する MAC ラーニングをディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—