CHAPTER 19

ARP 検査およびブリッジング パラメータの設定

トランスペアレント ファイアウォール モード限定

この章では、Address Resolution Protocol（ARP; アドレス解決プロトコル）検査をイネーブルにし、FWSM 用にブリッジング動作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セキュリティ コンテキストに入力できますが、システムには入力できません。

この章では、次の内容について説明します。

ARP 検査の設定

ここでは、ARP 検査および ARP 検査をイネーブルにする方法について説明します。

ARP 検査の概要

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 検査はすべてのブリッジ グループに適用されます。

ARP 検査をイネーブルにすると、FWSM は、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック 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、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、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 テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように FWSM を設定できます。

ARP 検査によって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングは、「中間者」攻撃をイネーブルにすることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホスト トラフィックを代行受信してルータに転送できるようになります。

ARP 検査を使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

スタティック ARP エントリの追加

ARP 検査は、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。スタティック ARP エントリを追加するには、次のコマンドを入力します。

```
hostname(config)# arp interface_name ip_address mac_address
```

interface_name は、ARP パケットの送信元インターフェイスです。*ip_address* は送信元アドレスで、*mac_address* は関連 MAC アドレスです。

たとえば、外部インターフェイスで、IP アドレスが 10.1.1.1、MAC アドレスが 0009.7cbe.2100 のルータからの ARP 応答を許可するには、次のコマンドを入力します。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

（注） トランスペアレント 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 検査のイネーブル化

ARP 検査をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# arp-inspection interface_name enable [flood | no-flood]
```

interface_name は、ARP 検査をイネーブルにするインターフェイスです。**flood** キーワードは、一致しない ARP パケットをすべてのインターフェイスに転送し、**no-flood** は、一致しないパケットをドロップします。

（注） デフォルト設定では、一致しないパケットはフラッディングします。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。

たとえば、外部インターフェイスで ARP 検査をイネーブルにして、一致しないすべての ARP パケットをドロップするには、次のコマンドを入力します。

```
hostname(config)# arp-inspection outside enable no-flood
```

すべてのインターフェイス上で ARP 検査の現在の設定を表示するには、**show arp-inspection** コマンドを入力します。

MAC アドレス テーブルのカスタマイズ

ここでは、MAC アドレス テーブルについて説明します。内容は次のとおりです。

MAC アドレス テーブルの概要

FWSM は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスが FWSM を介してパケットを送信すると、FWSM が MAC アドレスをアドレス テーブルに追加します。このテーブルで MAC アドレスと送信元インターフェイスが対応付けられ、グループがブリッジングされるので、FWSM は適切なインターフェイスからデバイス宛てのパケットを送信できます。トラフィックが複数のブリッジ グループを経由して送信される場合、MAC アドレスはテーブルに、複数のエントリを持つことができます。FWSM が MAC アドレスにパケットを配信する出力インターフェイスを決定する必要があるとき、FWSM はパケットの入力インターフェイスを含んだブリッジ グループのエントリを使用します。

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含まれていなくても、通常のブリッジのように、ブリッジ グループのすべてのインターフェイスに元のパケットを FWSM がフラッディング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学習します。
- 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学習します。

元のパケットはドロップされます。

スタティック MAC アドレスの追加

MAC アドレスは通常、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届いたときに、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 MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。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、そのスタティック 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する場合、FWSM はそのトラフィックを廃棄し、システム ログ メッセージを生成します。

MAC アドレス テーブルにスタティック MAC アドレスを追加するには、次のコマンドを入力します。

```
hostname(config)# mac-address-table static interface_name mac_address
```

interface_name は、発信元インターフェイスです。

MAC アドレス タイムアウトの設定

ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分ですが、タイムアウトは変更できます。タイムアウトを変更するには、次のコマンドを入力します。

```
hostname(config)# mac-address-table aging-time timeout_value
```

timeout_value（分）は、5 ～ 720（12 時間）です。5 分がデフォルトです。

MAC アドレス ラーニングのディセーブル化

デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、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。

MAC アドレス学習をディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# mac-learn interface_name disable
```

このコマンドの **no** 形式を使用すると、MAC アドレス ラーニングが再度イネーブルになります。**clear configure mac-learn** コマンドは、すべてのインターフェイスで MAC アドレス ラーニングを再度イネーブルにします。

MAC アドレス テーブルの表示

MAC アドレス テーブル全体（スタティックおよびダイナミック エントリを含めて）、特定のインターフェイスの MAC アドレス テーブル、または特定のブリッジ グループの MAC アドレス テーブルを表示できます。MAC アドレス テーブルを表示するには、次のコマンドを入力します。

```
hostname# show mac-address-table [interface_name | bridge_group]
```

すべてのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table
interface          mac address       type      Age min)   Group
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -        Eng
inside             0010.7cbe.6101    static      -        Eng
inside             0009.7cbe.5101    dynamic     10       Eng
```

内部インターフェイスのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table inside
interface          mac address       type      Age min)   Group
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -        Eng
inside             0009.7cbe.5101    dynamic     10       Eng
```