ARP 検査およびブリッジング パラメータの設定

透過ファイアウォール 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。

この章で説明する内容は、次のとおりです。

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 検査をイネーブルにすると、ARP パケットのフローを制御できます。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 テーブルのスタティック エントリと照合して、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 エントリと一致した場合、パケットを通過させます。
- MAC アドレス、IP アドレス、または送信元インターフェイスが一致しない場合、FWSM はそのパケットを廃棄します。
- ARP パケットのエントリがスタティック ARP テーブルのエントリと 1 つも一致しなかった場合に、FWSM がそのパケットをすべてのインターフェイスに転送するように（フラッディング）設定するか、またはパケットを廃棄するように設定できます。

ARP 検査によって、不正なユーザが他のホストまたはルータになりすます（ARP スプーフィング）ことを防止できます。ARP スプーフィングは「Man-In-The-Middle（MITM; 仲介者）」攻撃を引き起こします。たとえば、ホストからゲートウェイ ルータに ARP 要求を送ると、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。ところが、攻撃側は、ルータの MAC アドレスの代わりに攻撃側の MAC アドレスを使用して別の ARP 応答をホストに送ります。これにより、攻撃側は、ルータに転送される前にあらゆるホスト トラフィックを代行受信できるようになります。

ARP 検査により、スタティック ARP テーブルに正しい MAC アドレスとそれに対応する IP アドレスが指定されているかぎり、攻撃側が自分の MAC アドレスを使用して ARP 応答を送信できないことが保証されます。

スタティック ARP エントリの追加

ARP 検査では、ARP パケットと、ARP テーブルに登録されたスタティック ARP エントリを照合します。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、MAC アドレス 0009.7cbe.2100 を持つルータの外部インターフェイス 10.1.1.1 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）　透過ファイアウォールは、管理トラフィックなどの FWSM の間のトラフィックに関して、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** キーワードを使用すると、一致しなかった ARP パケットはすべてのインターフェイスに転送されます。**no-flood** を使用すると、一致しなかったパケットは廃棄されます。

（注）　デフォルト設定は、一致しなかったパケットをフラッディングします。FWSM 経由でスタティックエントリにのみ ARP を制限するには、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上で ARP 検査をイネーブルにして、一致しなかったすべての ARP パケットを廃棄する場合は、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。装置が 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装置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。その代わり、直接接続された装置またはリモート装置用に次のパケットを生成します。

- 直接接続装置用のパケット — FWSM は宛先 IP アドレスへの ARP 要求を生成し、FWSM に ARP 応答を受信するインターフェイスがわかるようにします。
- リモート装置用のパケット — FWSM は宛先 IP アドレスへの ping を生成し、FWSM に ping 応答を受信するインターフェイスがわかるようにします。

元のパケットは廃棄されます。

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。MAC アドレス テーブルには、必要に応じてスタティック MAC アドレスを追加できます。スタティック エントリを追加する利点の 1 つとして、MAC スプーフィングに対する防御が挙げられます。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 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 は送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 エントリのタイムアウト値は、デフォルトで 5 分です。このタイムアウト値は変更可能です。タイムアウト値を変更するには、次のコマンドを入力します。

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

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

MAC アドレス学習のディセーブル化

デフォルトでは、各インターフェイスが着信トラフィックの MAC アドレスを自動的に学習し、FWSM が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 アドレス学習をディセーブルにできます。ただし、MAC アドレスを統計的にテーブルに追加しない場合、トラフィックは FWSM を通過できません。

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
```

MAC アドレス学習を再びイネーブルにするには、このコマンドの **no** 形式を使用します。**clear configure mac-learn** コマンドは、すべてのインターフェイス上で MAC アドレス学習を再び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]
```

次に、テーブル全体を表示する **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
```

次に、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
```