CHAPTER 23

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 モードのみ

この章では、ARP 検査をイネーブルにする方法と、セキュリティ アプライアンスのブリッジング 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ではなくセキュリティ コンテキストで入力します。

次の事項について説明します。

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 検査の概要

デフォルトでは、すべての ARP パケットがセキュリティ アプライアンスを通過できます。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、セキュリティ アプライアンスはすべての 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、セキュリティ アプライアンス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セキュリティ アプライアンスを設定できます。

（注）　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。

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（中間者攻撃）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。

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
```

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）　透過ファイアウォールは、セキュリティ アプライアンス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]
```

flood 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ドします。スタティック エントリにある ARP だけがセキュリティ アプライアンス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について、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

この項では、MAC アドレス テーブルについて説明します。次の事項を取り上げます。

MAC アドレス テーブルの概要

セキュリティ アプライアンスは、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。デバイスがセキュリティ アプライアンス経由でパケットを送信すると、セキュリティ アプライアンスはこの 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、セキュリティ アプライアンスは、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。

セキュリティ アプライアンス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、セキュリティ アプライアンス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：セキュリティ アプライアンスは宛先 IP アドレスに対して ARP 要求を生成し、セキュリティ アプライアンスは 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：セキュリティ アプライアンスは宛先 IP アドレスへの ping を生成し、セキュリティ アプライアンスは 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。

スタティック MAC アドレスの追加

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。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、セキュリティ アプライアンス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。

スタティック MAC アドレスを MAC アドレス テーブルに追加するには、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入っ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て、セキュリティ アプライアンス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、トラフィックがセキュリティ アプライアンスを通過できなくなります。

MAC アドレス ラーニング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

すべての MAC アドレス テーブル（両方のインターフェイスのスタティック エントリとダイナミック エントリ）を表示できます。または、あるインターフェイスの 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]
```

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      Time Left
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

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      Time Left
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```