CHAPTER 26

ARP インスペクション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、ARP インスペクションをイネーブルにし、セキュリティ アプライアンス 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。

この章は、次の項で構成されています。

ARP インスペクションの設定

この項では、ARP インスペクションについて説明し、これをイネーブルにする方法について説明します。次の項目を取り上げます。

ARP インスペクションの概要

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 インスペクションをイネーブルにします。

ARP インスペクション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、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（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、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 インスペクションを使用すると、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 インスペクションは、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。ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

（注）　トランスペアレント 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。

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
```

ARP インスペクションのイネーブル化

ARP インスペクション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 インスペクション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 インスペクション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

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。

ASA 5505 適応型セキュリティ アプライアンスには、組み込みスイッチがあります。このスイッチの MAC アドレス テーブルは、各 VLAN 内のトラフィックの MAC アドレスとスイッチ ポートのマッピングを維持します。この項では、VLAN 間のトラフィックの MAC アドレスと VLAN インターフェイスのマッピングを維持する、ブリッジの MAC アドレス テーブルについて説明します。

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。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、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 によってトラフィックがドロップされ、システム メッセージが生成されます。スタティック ARP エントリを追加するときに（「スタティック ARP エントリの追加」（P.26-2）を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

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トラフィックに入る MAC アドレスを自動的に学習し、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
```