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

この章では、ARP インスペクションをイネーブルにする方法と、トランスペアレント ファイアウォール モードでセキュリティ 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。

トランスペアレント ファイアウォール モードの詳細については、第 18 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」（P.26-1）
- 「MAC アドレス テーブルのカスタマイズ」（P.26-5）

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 Inspection」（P.26-1）
- 「Edit ARP Inspection Entry」（P.26-2）
- 「ARP Static Table」（P.26-3）
- 「Add/Edit ARP Static Configuration」（P.26-4）

ARP Inspection

[ARP Inspection] ペインでは、ARP インスペクションを設定できます。

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。

フィールド

- [Interface]：インターフェイス名を示します。
- [ARP Inspection Enabled]：ARP インスペクションがイネーブルであるかどうか（[Yes] または [No]）を示します。
- [Flood Enabled]：ARP インスペクションがイネーブルの場合、アクションが不明なパケットをフラッディングするかどうか（[Yes] または [No]）を示します。ARP インスペクションがディセーブルの場合、この値は常に [No] になります。
- [Edit]：選択したインターフェイスの ARP インスペクション パラメータを編集します。

モード

次の表は、この機能を使用できるモードを示したものです。

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 インスペクション設定値を設定できます。

フィールド

- [Enable ARP Inspection]：ARP インスペクション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とも一致しないパケットをすべてのインターフェイス（発信元インターフェイスを除く）にフラッディングすることを指定します。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。このチェックボックスをオフにすると、すべての不一致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。

Management 0/0 インターフェイスまたはサブインターフェイスがある場合、これら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

次の表は、この機能を使用できるモードを示したものです。

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 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。

[ARP Static Table] パネルでは、MAC アドレスを特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せず、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ているインターフェイスを表示します。
- [IP Address]：ホスト IP アドレスを表示します。

- [MAC Address]：ホスト MAC アドレスを表示します。
- [Proxy ARP]：セキュリティ アプライアンス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。セキュリティ アプライアンスは、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]：セキュリティ アプライアンスが 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 テーブルを再構築すると、自動的に新しいホスト情報が更新され、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必要になる場合があります。このパラメータは [Static ARP Table] パネルに表示されますが、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

次の表は、この機能を使用できるモードを示したものです。

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ているインターフェイスを設定します。
- [IP Address]：ホスト IP アドレスを設定します。
- [MAC Address]：ホスト MAC アドレス（00e0.1e4e.3d8b など）を設定します。
- [Proxy ARP]：セキュリティ アプライアンス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。セキュリティ アプライアンスは、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

次の表は、この機能を使用できるモードを示したものです。

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、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 Address Table

[MAC Address Table] ペインでは、スタティック MAC アドレス 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。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 エントリに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 ARP エントリを追加するときに（「ARP Static Table」（P.26-3）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。

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。

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表示します。
- [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 MAC アドレス エントリが MAC アドレス テーブルにとどまることができる時間を設定します。有効な値は、5 ～ 720 分（12 時間）です。5 分がデフォルトです。

モード

次の表は、この機能を使用できるモードを示したものです。

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 エントリに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。

フィールド

- [Interface Name] : 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

次の表は、この機能を使用できるモードを示したものです。

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 ラーニング

[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。

フィールド

- [Interface]：インターフェイス名を表示します。
- [MAC Learning Enabled]：MAC ラーニングがイネーブルであるかどうか（[Yes] または [No]）を示します。
- [Enable]：選択したインターフェイスでの 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での MAC ラーニングをディセーブルにします。

モード

次の表は、この機能を使用できるモードを示したものです。

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
—	•	•	•	—