CHAPTER 23

ARP 検査およびブリッジング パラメータの設定

この章では、ARP 検査をイネーブルにする方法と、透過ファイアウォール モードでのセキュリティ 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。

透過ファイアウォール モードの詳細については、第 16 章「ファイアウォール モードの概要」を参照してください。

この章には、次の項があります。

- ARP 検査の設定（P.23-2）
- MAC アドレス テーブルのカスタマイズ（P.23-6）

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 Inspection（P.23-2）
- Edit ARP Inspection Entry（P.23-3）
- ARP Static Table（P.23-4）
- Add/Edit ARP Static Configuration（P.23-5）

ARP Inspection

Configuration > Properties > ARP > ARP Inspection

ARP Inspection ペインでは、ARP 検査を設定できます。

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 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（介入者攻撃）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。

フィールド

- Interface：インターフェイス名を示します。
- ARP Inspection Enabled：ARP 検査がイネーブルになっているかどうかを Yes または No で示します。
- Flood Enabled：ARP 検査がイネーブルになっている場合には、アクションで未知のパケットをフラッドするようになっているかどうかを Yes または No で示します。ARP 検査がディセーブルになっている場合は、この値は常に No です。

- Edit：選択したインターフェイスの ARP 検査パラメータを編集します。

モード

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > ARP > ARP Inspection > Edit ARP Inspection Entry

Edit ARP Inspection Entry ダイアログボックスでは、ARP 検査の設定値を設定できます。

フィールド

- Enable ARP Inspection：ARP 検査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にも一致しないパケットが、送信元のインターフェイスを除くすべてのインターフェイスからフラッドするように指定します。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。このチェックボックスをオフにすると、一致しないすべての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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > ARP > ARP Static Table

ホストは、パケットの宛先を IP アドレスで識別しますが、イーサネット上でパケットが実際にどこに配信されるかは、イーサネットの MAC アドレスで決まります。ルータやホストが直接接続されているネットワークにパケットを配信する場合は、そのパケットの IP アドレスに関連付けられている MAC アドレスを尋ねる ARP 要求を送信します。次に、ARP 応答に従って、MAC アドレスにパケットを配信します。ホストやルータは、パケットを配信するたびに ARP 要求を送信しなくてもよいように、ARP テーブルを保持しています。ARP テーブルは、ARP 応答がネットワークに送信されるたびにダイナミックに更新され、一定の期間使用されなかったエントリはタイムアウトになります。エントリが正しくなくなった場合（IP アドレスに関連付けられていた MAC アドレスが変更された場合など）は、更新される前にタイムアウトになります。

（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 Static Table パネルでは、MAC アドレスを所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しないため、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たインターフェイスを示します。
- IP Address：ホストの IP アドレスを示します。
- MAC Address：ホストの MAC アドレスを示します。
- 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 テーブルが再構築されると、新しいホスト情報に自動的に更新され、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できます。このパラメータは ARP Static 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

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > ARP > ARP Static Table > 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るインターフェイスを設定します。
- IP Address：ホストの IP アドレスを設定します。
- MAC Address：ホストの MAC アドレスを設定します（00e0.1e4e.3d8b など）。
- 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

次の表に、この機能を使用できるモードを示します。

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 Address Table（P.23-6）
- Add/Edit MAC Address Entry（P.23-7）
- MAC Learning（P.23-8）

MAC Address Table

Configuration > Properties > Bridging > MAC Address Table

MAC Address Table ペインでは、スタティック MAC アドレスの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。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。ARP のスタティック エントリを追加すると（P.23-4 の「ARP Static Table」を参照）、スタティック MAC アドレス エントリが 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、内蔵スイッチがあります。このスイッチの MAC アドレス テーブルには、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が登録されています。この項では、複数の VLAN を通るトラフィックの 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示します。
- MAC Address：MAC アドレスを示します。
- 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に、MAC アドレス エントリが MAC アドレス テーブルに残る時間を 5 ～ 720 分（12 時間）の範囲で設定します。5 分がデフォルトです。

モード

次の表に、この機能を使用できるモードを示します。

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

Configuration > Properties > Bridging > MAC Address Table > 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。

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設定します。
- MAC Address：MAC アドレスを設定します。

モード

次の表に、この機能を使用できるモードを示します。

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 Learning

Configuration > Properties > Bridging > MAC Learning

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。デフォルトにより、各インターフェイスは送信され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、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示します。
- MAC Learning Enabled：MAC ラーニングがイネーブルになっているかどうかを Yes または No で示します。
- Enable：選択したインターフェイスに対する 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に対する MAC ラーニングをディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
—	•	•	•	—