



# トランスペアレントファイアウォールモードの ARP インспекションおよび MAC アドレス テーブル

この章では、MACアドレステーブルのカスタマイズ方法、およびブリッジグループのARPインспекションの設定方法について説明します。

- [ARP インспекションと MAC アドレス テーブルについて \(1 ページ\)](#)
- [デフォルト設定 \(3 ページ\)](#)
- [ARP インспекションと MAC アドレス テーブルのガイドライン \(3 ページ\)](#)
- [ARP インспекションとその他の ARP パラメータの設定 \(3 ページ\)](#)
- [トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルのカスタマイズ \(6 ページ\)](#)
- [ARP インспекションと MAC アドレス テーブルの履歴 \(8 ページ\)](#)

## ARP インспекションと MAC アドレス テーブルについて

ブリッジグループのインターフェイスでは、ARP インспекションは「中間者」攻撃を防止します。他の ARP の設定をカスタマイズすることも可能です。ブリッジグループの MAC アドレス テーブルのカスタマイズができます。これには、MAC スプーフィングに対する防御としてのスタティック ARP エントリの追加が含まれます。

## ブリッジグループのトラフィックの ARP インспекション

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インспекションをイネーブルにします。

ARP インспек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 スプーフィングが許可されていると、

「中間者」攻撃を受けることがあります。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спек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。

ARP インспекションをイネーブルにすると、ASA 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、ASA 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 ASA を設定できます。



(注) 専用の管理インターフェイスは、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。

## MAC アドレス テーブル

ブリッジ グループを使用する場合、ASA 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。デバイスがブリッジ グループ経由でパケットを送信すると、ASA が MAC アドレスをアドレス 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、ASA 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。ブリッジ グループ メンバー間のトラフィックには ASA セキュリティ ポリシーが適用されるため、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、すべてのインターフェイスに元のパケットを ASA がフラッディング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：ASA は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモートデバイスへのパケット：ASA は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

## デフォルト設定

- ARPインスペクションをイネーブルにした場合、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。
- 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。
- 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、ASA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。

## ARPインスペクションとMACアドレステーブルのガイドライン

- ARPインスペクションは、ブリッジグループでのみサポートされます。
- MACアドレステーブル構成は、ブリッジグループでのみサポートされます。
- ブリッジグループは、トランスペアレントファイアウォールモードでのみサポートされます。

## ARPインスペクションとその他のARP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のブリッジグループでは、ARPインスペクションをイネーブルにすることができます。その他のARPパラメータは、ブリッジグループとルーテッドモードのインターフェイスの両方で設定できます。

### 手順

- ステップ1** [スタティックARPエントリの追加と、他のARPパラメータのカスタマイズ \(4 ページ\)](#) に従って、スタティックARPエントリを追加します。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エントリと比較するので、この機能にはスタティックARPエントリが必要です。その他のARPパラメータも設定できます。
- ステップ2** (トランスペアレントモードのみ) [ARPインスペクションの有効化 \(5 ページ\)](#) に従ってARPインスペクションを有効にします。

## スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ

ブリッジグループのデフォルトでは、ブリッジグループ メンバー インターフェイス間の ARP パケットはすべて許可されます。ARP パケットのフローを制御するには、ARP インспекションをイネーブルにします。ARP インспек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。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は 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）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの ASA との間のトラフィックに、ASA は ARP テーブルのダイナミック ARP エントリのみを使用します。

ARP タイムアウトなどの ARP 動作を設定することもできます。

### 手順

**ステップ 1** [Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Static Table] の順に選択します。

**ステップ 2** [Add] をクリックして、スタティック ARP エントリを追加します。

[Add ARP Static Configuration] ダイアログボックスが表示されます。

- a) [Interface] ドロップダウンリストから、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選択します。
- b) [IP Address] フィールドにホストの IP アドレスを入力します。
- c) [MAC Address] フィールドにホストの MAC アドレスを入力します（00e0.1e4e.3d8b など）。
- d) このアドレスでプロキシ ARP を実行するには、[Proxy ARP] チェック ボックスをオンにします。

ASA 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。

- e) [OK] をクリックします。

**ステップ3** ダイナミック ARP エントリの ARP タイムアウトを設定するには、[ARP Timeout] フィールドに値を入力します。

このフィールドでは、ASA 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。

**ステップ4** 非接続サブネットを使用するには、[Allow non-connected subnets] チェックボックスをオンにします。ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。ARP キャッシュをイネーブルにして、間接接続されたサブネットを含めることもできます。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否 (DoS) 攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンダリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

**ステップ5** すべてのインターフェイスの1秒あたりのARPパケット数を制御するには、[ARP Rate-Limit] フィールドに値を入力します。

10 ～ 32768 の範囲で値を入力します。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。

**ステップ6** [Apply] をクリックします。

## ARP インスペクションの有効化

この項では、ブリッジグループ用に ARP インスペクションをイネーブルにする方法について説明します。

### 手順

**ステップ1** [Configuration] > [Device Management] > [Advanced] > [ARP] > [ARP Inspection] ペインの順に選択します。

**ステップ2** ARP インスペクションをイネーブルにするインターフェイス行を選択し、[Edit] をクリックします。

[Edit ARP Inspection] ダイアログボックスが表示されます。

**ステップ3** ARP インスペクションをイネーブルにするには、[Enable ARP Inspection] チェックボックスをオンにします。

**ステップ 4** (任意) 一致しない ARP パケットをフラッディングするには、[Flood ARP Packets] チェックボックスをオンにします。

デフォルトでは、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されます。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、ASA 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、一致しないパケットはすべてドロップされます。これにより、スタティック エントリにある ARP だけが ASA を通過するように制限されます。

(注) Management 0/0 または 0/1 インターフェイスあるい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。

**ステップ 5** [OK]、続いて [Apply] をクリックします。

---

## トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルのカスタマイズ

ここでは、ブリッジグループの MAC アドレス テーブルをカスタマイズする方法について説明します。

### ブリッジグループのスタティック 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、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、ASA 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 ([スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ \(4 ページ\)](#)) 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。

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、次の手順を実行します。

#### 手順

---

**ステップ 1** [Configuration] > [Device Setup] > [Bridging] > [MAC Address Table] ペインを選択します。

**ステップ 2** (オプション) MAC アドレス エントリがタイムアウトするまで MAC アドレス テーブル内に留まる時間を設定するには、[Dynamic Entry Timeout] フィールドに値を入力します。

この値は、5～720分（12時間）の範囲で指定します。5分がデフォルトです。

**ステップ3** [Add] をクリックします。

[Add MAC Address Entry] ダイアログボックスが表示されます。

**ステップ4** [Interface Name] ドロップダウンリストから、MACアドレスに関連付けられている送信元インターフェイスを選択します。

**ステップ5** [MAC Address] フィールドにMACアドレスを入力します。

**ステップ6** [OK]、続いて [Apply] をクリックします。

---

## MACアドレスラーニングのディセーブル化

デフォルトで、各インターフェイスは着信トラフィックのMACアドレスを自動的に学習し、ASA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ASA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、次の手順を実行します。

### 手順

---

**ステップ1** [Configuration] > [Device Setup] > [Bridging] > [MAC Learning] の順に選択します。

**ステップ2** MACラーニングをディセーブルにするには、インターフェイス行を選択して、[Disable] をクリックします。

**ステップ3** MACラーニングを再度イネーブルにするには、[Enable] をクリックします。

**ステップ4** [Apply] をクリックします。

---

## ARPインスペクションとMACアドレステーブルの履歴

機能名	プラットフォームリリース	機能情報
ARPインスペクション	7.0(1)	<p>ARPインスペクションは、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比較します。この機能は、トランスペアレントファイアウォールモード。</p> <p><b>arp</b>、<b>arp-inspection</b>、および <b>show arp-inspection</b> コマンドが導入されました。</p>
MACアドレステーブル	7.0(1)	<p>トランスペアレントモード。</p> <p><b>mac-address-table static</b>、<b>mac-address-table aging-time</b>、<b>mac-learn disable</b>、および <b>show mac-address-table</b> コマンドが導入されました。</p>

機能名	プラットフォーム リリース	機能情報
間接接続されたサブネットのARPキャッシュの追加	8.4(5)/9.1(2)	<p>ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。また、ARP キャッシュに間接接続されたサブネットを含めることができるようになりました。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否 (DoS) 攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。</p> <p>次の機能を使用する場合は、この機能を使用する必要がある可能性があります。</p> <ul style="list-style-type: none"> <li>• セカンダリ サブネット。</li> <li>• トラフィック転送の隣接ルートのプロキシ ARP。</li> </ul> <p>次の画面が変更されました。  <b>[Configuration] &gt; [Device Management] &gt; [Advanced] &gt; [ARP] &gt; [ARP Static Table]</b>。</p>
カスタマイズ可能な ARP レート制限	9.6(2)	<p>1 秒あたり許可される ARP パケットの最大数を設定できます。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。</p> <p>次の画面が変更されました。  <b>[Configuration] &gt; [Device Management] &gt; [Advanced] &gt; [ARP] &gt; [ARP Static Table]</b></p>

