ARP インスペクションおよび 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インスペクションの設定方法について説明します。

ARP インスペクションと 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 インスペクションは「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 トラフィックの ARP インスペクション

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。

ARPインスペクションを有効化すると、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 Management 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。

ルーテッドモードでは、すべてのインターフェイスで非 IP パケットのフラッディングをオプションで有効にできます。

デフォルト設定

- ARPインスペクションを有効にした場合、デフォルト設定では、一致しないパケットはフラッディングします。
- ダイナミック MAC アドレス テーブル エントリ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。

（注） Secure Firewall ASA はリセットパケットを生成し、ステートフル検査エンジンによって拒否された接続をリセットします。リセットパケットでは、パケットの宛先 MAC アドレスが ARP テーブルのルックアップに基づいて決定されるのではなく、拒否されるパケット（接続）から直接取得されます。

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。

ARP インスペクションとその他の ARP パラメータの設定

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 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。

- セカンデリ 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 [適用（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

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設定

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。ルーテッドモードでは、すべてのインターフェイスで非 IP パケットのフラッディングを有効にできます。

MAC アドレスラーニングを設定にするには、次の手順を実行します。

手順

ステップ 1 **[構成（Configuration）]** > **[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ブリッジング（Bridging）]** > **[MACラーニング（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 非IPパケットのフラッディングを有効にするには、[非IPv4-IPv6パケットの不明なMACアドレスのフラッディングを有効にする（Enable flooding for unknown MAC address for non IPv4-IPv6 packets）] をオンにします。

ステップ 5 [適用（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)	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、および9.7(1) で始まるトランスペアレントモードとルーテッドモードのブリッジグループのインターフェイスで利用できます。 **arp**、**arp-inspection**、および **show arp-inspection** コマンドが導入されました。
MAC アドレス テーブル	7.0(1)	トランスペアレント モード、および9.7(1) で始まるトランスペアレントモードとルーテッドモードのブリッジグループのインターフェイスの MAC アドレス テーブルをカスタマイズすることもできます。 **mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable**、および **show mac-address-table** コマンドが導入されました。
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)	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。 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。 • セカンデリ 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。 次の画面が変更されました。[Configuration] > [Device Management] > [Advanced]> [ARP] > [ARP Static Table]。

機能名	プラットフォーム リリース	機能情報
カスタマイズ可能な ARP レート制限	9.6(2)	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。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[ARP]** > **[ARP Static Table]**

機能名	プラットフォーム リリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASA がルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバーなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッドモードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** **[Configuration] > [Device Setup] > [Routing] > [Static Routes]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Server]** **[Configuration] > [Firewall] > [Access Rules]** **[Configuration] > [Firewall] > [EtherType Rules]**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。