



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 \(6 ページ\)](#)
- [ARP インспекションと MAC アドレス テーブルのモニタリング \(8 ページ\)](#)
- [ARP インспекションと MAC アドレス テーブルの履歴 \(9 ページ\)](#)

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 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ションを有効にします。

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спек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) 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спекションと MAC アドレス テーブルのガイドライン

- ARP インспек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спек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спек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спекションの有効化 \(6 ページ\)](#) に従って ARP インспек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 スタティック ARP エントリを追加します。

arp interface_name ip_address mac_address [alias]

例 :

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

この例では、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 応答が許可されます。

このマッピングでプロキシ ARP を有効にするには、ルーテッドモードで **alias** を指定します。ASA は、指定された IP アドレスの ARP 要求を受信すると、ASA MAC アドレスで応答します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。トランスペアレントファイアウォールモードでは、このキーワードは無視されます。ASA はプロキシ ARP を実行しません。

ステップ 2 ダイナミック ARP エントリの ARP タイムアウトを設定します。

arp timeout seconds

例：

```
ciscoasa(config)# arp timeout 5000
```

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 3 非接続サブネットを許可する

arp permit-nonconnected

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 4 ARP レート制限を設定して 1 秒あたりの ARP パケット数を制御する

arp rate-limit seconds

例：

```
ciscoasa(config)# arp rate-limit 1000
```

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。

ARP インспек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спек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

ARP インспекションをイネーブルにします。

arp-inspection interface_name enable [flood | no-flood]

例：

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

flood キーワードは、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。

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 ASA 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。

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

スタティック MAC アドレス エントリを追加します。

mac-address-table static *interface_name* *mac_address*

例：

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

interface_name は、発信元インターフェイスです。

MAC アドレス タイムアウトを設定する

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、次の手順を実行します。

手順

MAC アドレス エントリのタイムアウトを設定します。

mac-address-table aging-time *timeout_value*

例：

```
ciscoasa(config)# mac-address-table aging-time 10
```

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 ラーニングを設定するには、次の手順を実行します。

手順

ステップ 1 MAC アドレス ラーニングをディセーブルにします。

mac-learn interface_name disable

例 :

```
ciscoasa(config)# mac-learn inside 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。

ステップ 2 (ルーテッドモードのみ) 非 IP パケットのフラッディングを有効にします。

mac-learn flood

例 :

```
ciscoasa(config)# mac-learn flood
```

ARP インスペクションと MAC アドレス テーブルのモニタリング

- **show arp-inspection**

ARP インスペクションをモニターします。すべてのインターフェイスについて、ARP インスペクションの現在の設定を表示します。

- **show mac-address-table [interface_name]**

MAC アドレス テーブルをモニターします。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。

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。

```
ciscoasa# 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。

```
ciscoasa# show mac-address-table inside
interface      mac address      type      Time Left
-----
```



```
inside    0010.7cbe.6101    static    -
inside    0009.7cbe.5101    dynamic   10
```

スタティックおよびダイナミックブリッジグループのエントリの合計数を表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table count
Static      mac-address bridges (curr/max): 0/16384
Dynamic     mac-address bridges (curr/max): 0/16384
```

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、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。</p> <p>arp、arp-inspection、および show arp-inspection 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、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。</p> <p>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。</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"> • 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。 <p>arp permit-nonconnected コマンドが導入されました。</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>次のコマンドを追加しました。 arp rate-limit、show arp rate-limit</p>

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)	

機能名	プラットフォームリリース	機能情報
		<p>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。</p> <p>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、</p>

機能名	プラットフォームリリース	機能情報
		BVI ではサポートされません。 次のコマンドが変更されました。 access-group 、 access-list ethertype 、 arp-inspection 、 dhcpd 、 mac-address-table static 、 mac-address-table aging-time 、 mac-learn 、 route 、 show arp-inspection 、 show bridge-group 、 show mac-address-table 、 show mac-learn

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。