CHAPTER 5

トランスペアレント ファイアウォールまたはルーテッド ファイアウォールの設定

この章では、ファイアウォール モードをルーテッドまたはトランスペアレントに設定する方法と、ファイアウォールが各ファイアウォール モードでどのように機能するかについて説明します。この章には、トランスペアレント ファイアウォール動作のカスタマイズに関する情報も含まれます。

マルチコンテキスト モードでは、コンテキストごとに別個にファイアウォール モードを設定できます。

この章の内容は、次のとおりです。

- 「ファイアウォール モードの設定」（P.5-1）
- 「トランスペアレント ファイアウォール用の ARP インスペクションの設定」（P.5-10）
- 「トランスペアレント ファイアウォール用の MAC アドレス テーブルのカスタマイズ」（P.5-14）

ファイアウォール モードの設定

この項では、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードについて、およびモードの設定方法について説明します。この項では、次のトピックについて取り上げます。

- 「ファイアウォール モードに関する情報」（P.5-1）
- 「ファイアウォール モードのライセンス要件」（P.5-6）
- 「デフォルト設定」（P.5-6）
- 「注意事項と制限事項」（P.5-6）
- 「ファイアウォール モードの設定」（P.5-8）
- 「ファイアウォール モードの機能履歴」（P.5-9）

ファイアウォール モードに関する情報

この項では、ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードについて説明します。次の項目を取り上げます。

- 「ルーテッド ファイアウォール モードに関する情報」（P.5-2）
- 「トランスペアレント ファイアウォール モードに関する情報」（P.5-2）

ルーテッド ファイアウォール モードに関する情報

ルーテッド モードでは、ASA はネットワーク内のルータ ホップと見なされます。ルーテッド モードは多数のインターフェイスをサポートしています。インターフェイスはそれぞれ異なるサブネット上に置かれます。コンテキスト間でインターフェイスを共有することもできます。

ASA は、接続されたネットワーク間のルータとして機能します。インターフェイスごとに、異なるサブネット上の IP アドレスが必要です。ASA は、複数のダイナミック ルーティング プロトコルをサポートします。ただし、ルーティングのニーズが広範に及ぶ場合は、ASA に依存するのではなく、アップストリームとダウンストリームのルータの高度なルーティング機能を使用することを推奨します。

トランスペアレント ファイアウォール モードに関する情報

従来、ファイアウォールはルーテッド ホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとは見なされません。

この項では、トランスペアレント ファイアウォール モードについて説明します。次の項目を取り上げます。

- 「トランスペアレント ファイアウォール ネットワーク」（P.5-2）
- 「ブリッジ グループ」（P.5-2）
- 「管理インターフェイス（ASA 5510 以降）」（P.5-3）
- 「レイヤ 3 トラフィックの許可」（P.5-3）
- 「許可される MAC アドレス」（P.5-3）
- 「ルーテッド モードで許可されないトラフィックの通過」（P.5-3）
- 「BPDU の処理」（P.5-4）
- 「MAC アドレス ルックアップと ルート ルックアップ」（P.5-4）
- 「ネットワークでのトランスペアレント ファイアウォールの使用」（P.5-5）

トランスペアレント ファイアウォール ネットワーク

ASA は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルーティングされたホップではないので、既存のネットワークに簡単に導入できます。

ブリッジ グループ

セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

（注）　ブリッジ グループにはそれぞれ管理 IP アドレスが必要です。ASA はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。別の管理方法については、「管理インターフェイス（ASA 5510 以降）」（P.5-3）を参照してください。

ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

管理インターフェイス（ASA 5510 以降）

各ブリッジ グループの管理 IP アドレスのほかに、別の管理 *スロット/ポート* インターフェイスを追加できます。このインターフェイスはどのブリッジ グループにも属さず、ASA への管理トラフィックのみを許可します。詳細については、「管理インターフェイス」（P.11-2）を参照してください。

レイヤ 3 トラフィックの許可

- IPv4 および IPv6 トラフィックは、セキュリティの高いインターフェイスから低いインターフェイスに移動する場合、アクセス リストなしで自動的にトランスペアレント ファイアウォールを通過できます。
- ARP は、アクセス リストに関係なく、両方向ともトランスペアレント ファイアウォールを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに移動するレイヤ 3 トラフィックの場合、セキュリティの低いインターフェイスで拡張アクセス リストが必要です。詳細については、第 20 章「拡張アクセス コントロール リストの追加」を参照してください。

許可される MAC アドレス

次の宛先 MAC アドレスは、トランスペアレント ファイアウォールを通過できます。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、アクセス リストで許可しても、いくつかのタイプのトラフィックは ASA を通過できません。ただし、トランスペアレント ファイアウォールは、拡張アクセス リスト（IP トラフィックの場合）または EtherType アクセス リスト（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

IP 以外のトラフィック（AppleTalk、IPX、BPDU、および MPLS など）は、EtherType アクセス リストを使用して通過するように構成できます。

（注）　トランスペアレント モードの ASA は、CDP パケットおよび 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。たとえば、IS-IS パケットは通過できません。例外として、BPDU はサポートされています。

ルーテッド モード機能のためのトラフィックの通過

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、拡張アクセス リストを使用して、DHCP トラフィック（サポートされない DHCP リレー機能の代わりに）または IP/TV によって作成されたマルチキャスト トラフィックを許可できます。また、トランスペアレント ファイアウォールを通過するルーティング プロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、または BGP トラフィックを拡張アクセス リストに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは ASA を通過できます。

BPDU の処理

スパニングツリー プロトコルを使用するときのループを防止するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、BPDU を拒否するように EtherType アクセス リストを設定する必要があります。フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチ ポートがブロッキング ステートに移行することを回避できます。詳細については、「トランスペアレント ファイアウォール モードの要件」（P.8-16）を参照してください。

MAC アドレス ルックアップと ルート ルックアップ

ASA がトランスペアレント モードで動作している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。

ただし、次のトラフィック タイプにはルート ルックアップが必要です。

- ASA で発信されたトラフィック：たとえば、syslog サーバがリモート ネットワークにある場合は、ASA がそのサブネットに到達できるようにスタティック ルートを使用する必要があります。
- NAT がイネーブルになっている ASA から 1 ホップ以上のトラフィック：ASA はルート ルックアップを実行する必要があります。管理者は、実際のホスト アドレスのためのスタティック ルートを ASA 上に追加する必要があります。
- インスペクションがイネーブルであり、エンドポイントが ASA から少なくとも 1 ホップ離れている Voice over IP（VoIP）トラフィック：たとえば、CCM と H.323 ゲートウェイの間にトランスペアレント ファイアウォールを使用し、トランスペアレント ファイアウォールと H.323 ゲートウェイの間にルータがある場合、正常にコールを完了させるには ASA に H.323 ゲートウェイ用のスタティック ルートを追加する必要があります。
- インスペクションと NAT をイネーブルにしている VoIP または DNS トラフィックで、埋め込み IP アドレスが ASA から少なくとも 1 ホップ離れている場合：VoIP および DNS パケット内部の IP アドレスを正しく変換するには、ASA でルート ルックアップを実行する必要があります。パケットに埋め込まれている実際のホスト アドレスを把握するには、ASA にスタティック ルートを追加する必要があります。

ネットワークでのトランスペアレント ファイアウォールの使用

図 5-1 に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 5-1　トランスペアレント ファイアウォール ネットワーク

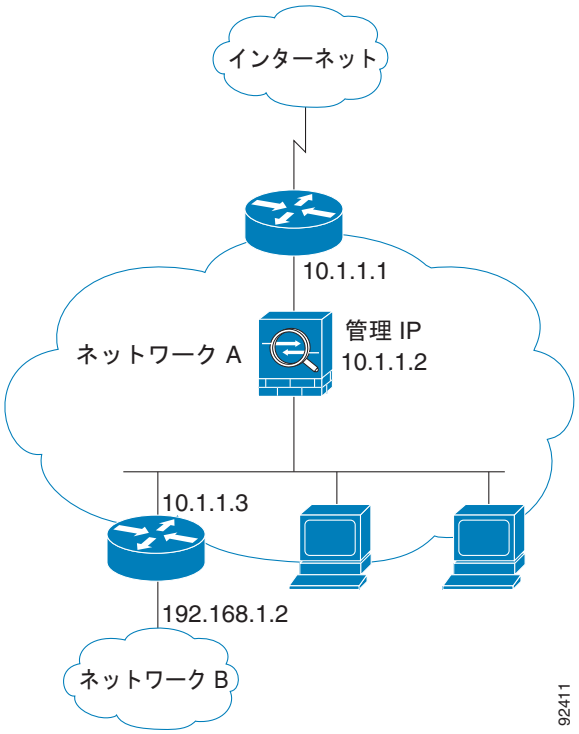
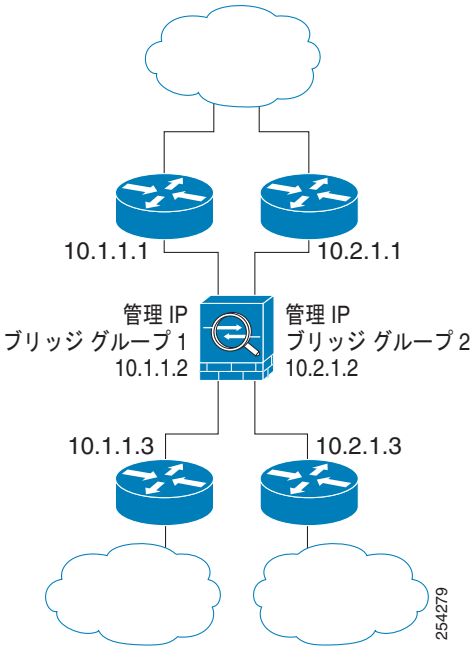


図 5-2 に、2 つのブリッジ グループを持つ、ASA に接続されている 2 つのネットワークを示します。

図 5-2　2 つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク



ファイアウォール モードのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

デフォルト設定

デフォルト モードはルーテッド モードです。

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

トランスペアレント ファイアウォール ガイドライン

トランスペアレント ファイアウォール ネットワークを計画する場合は、次のガイドラインに従ってください。

- トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Cisco Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、*管理*インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ブリッジ グループ管理 IP アドレスを、接続されたデバイスのデフォルト ゲートウェイとして指定しないでください。ASA の他方の側にあるルータをデバイスのデフォルト ゲートウェイとして指定する必要があります。
- 管理トラフィックの戻りパスを指定するために必要な、トランスペアレント ファイアウォールのデフォルト ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別するスタティック ルートを指定する必要があります。

その他のガイドラインについては、「ガイドラインと制限事項」（P.14-5）を参照してください。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドラインと制限事項

- ファイアウォール モードを変更すると、ASA は実行コンフィギュレーションをクリアします。これは、多くのコマンドが両方のモードでサポートされていないためです。スタートアップ コンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップ コンフィギュレーションがロードされて、モードは元の設定に戻ります。コンフィギュレーション ファイルのバックアップについては、「ファイアウォール モードの設定」（P.5-8）を参照してください。
- **firewall transparent** コマンドを使用してモードを変更するテキスト コンフィギュレーションを ASA にダウンロードする場合は、このコマンドをコンフィギュレーションの先頭に配置します。先頭に配置することによって、ASA でこのコマンドが読み込まれるとすぐにモードが変更され、その後引き続きダウンロードされたコンフィギュレーションが読み込まれます。このコマンドがコンフィギュレーションの後ろの方にあると、ASA はそれ以前に記述されているコンフィギュレーションの行をすべてクリアします。テキスト ファイルのダウンロードの詳細については、「使用するイメージおよびスタートアップ コンフィギュレーションの設定」（P.85-14）を参照してください。

トランスペアレント モードでサポートされていない機能

表 5-1 にトランスペアレント モードでサポートされていない機能を示します。

表 5-1　トランスペアレント モードでサポートされていない機能

機能	説明
ダイナミック DNS	—
DHCP リレー	トランスペアレント ファイアウォールは DHCP サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。2 つの拡張アクセス リストを使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、ASA で発信されたトラフィックのスタティック ルートを追加できます。拡張アクセス リストを使用して、ダイナミック ルーティング プロトコルが ASA を通過できるようにすることもできます。
マルチキャスト IP ルーティング	拡張アクセス リストで許可することによって、マルチキャスト トラフィックが ASA を通過できるようにすることができます。
QoS	—
通過トラフィック用の VPN ターミネーション	トランスペアレント ファイアウォールは、管理接続に対してのみサイトツーサイト VPN トンネルをサポートします。これは、ASA を通過するトラフィックに対して VPN 接続を終端しません。拡張アクセス リストを使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。SSL VPN もサポートされていません。
ユニファイド コミュニケーション	—

ファイアウォール モードの設定

この項では、ファイアウォール モードを変更する方法について説明します。

（注） ファイアウォール モードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォール モードを設定することをお勧めします。

前提条件

モードを変更すると、ASA は実行コンフィギュレーションをクリアします（詳細については 「注意事項と制限事項」（P.5-6）を参照してください）。

- 設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。「コンフィギュレーションまたはその他のファイルのバックアップ」（P.85-18）を参照してください。

- モードを変更するには、コンソール ポートで CLI を使用します。ASDM コマンドライン インターフェイス ツールや SSH などの他のタイプのセッションを使用すると、コンフィギュレーションがクリアされるときに切断されるので、いずれにしてもコンソール ポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。

手順の詳細

コマンド	目的
firewall transparent **例：** `hostname(config)# firewall transparent`	ファイアウォール モードをトランスペアレントに設定します。モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。 **（注）** ファイアウォール モードの変更では確認は求められず、ただちに変更が行われます。

ファイアウォール モードの機能履歴

表 5-2 に、この機能のリリース履歴を示します。

表 5-2　ファイアウォール モードの機能履歴

機能名	リリース	機能情報
トランスペアレント ファイアウォール モード	7.0(1)	トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 のファイアウォールであり、接続デバイスにはルータ ホップとして認識されません。 次のコマンドが導入されました。**firewall transparent** コマンドおよび **show firewall**。

表 5-2　ファイアウォール モードの機能履歴 （続き）

機能名	リリース	機能情報
トランスペアレント ファイアウォール ブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードでは最大 8 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 **（注）** ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。 **interface bvi**、**bridge-group**、**show bridge-group** の各コマンドが導入されました。
マルチ コンテキスト モードのファイアウォール モードの混合がサポートされます。	8.5(1)/9.0(1)	セキュリティ コンテキスごとに個別のファイアウォール モードを設定できます。したがってその一部をトランスペアレント モードで実行し、その他をルーテッド モードで実行することができます。 **firewall transparent** コマンドが変更されました。

トランスペアレント ファイアウォール用の 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 インスペクションに関する情報」（P.5-11）
- 「ARP インスペクションのライセンス要件」（P.5-11）
- 「デフォルト設定」（P.5-11）
- 「注意事項と制限事項」（P.5-12）
- 「ARP インスペクションの設定」（P.5-12）
- 「ARP インスペクションのモニタリング」（P.5-14）
- 「ARP インスペクションの機能履歴」（P.5-14）

ARP インスペクションに関する情報

デフォルトでは、すべての ARP パケットが ASA 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、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（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 インスペクションのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

デフォルト設定

デフォルトでは、すべての ARP パケットが ASA を通過できます。

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。

注意事項と制限事項

コンテキスト モードのガイドライン

- シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。
- マルチ コンテキスト モードで、各コンテキスト内の ARP インスペクションを設定します。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードでだけサポートされます。ルーテッド モードはサポートされていません。

ARP インスペクションの設定

この項では、ARP インスペクションを設定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 インスペクションの設定のタスク フロー」（P.5-12）
- 「スタティック ARP エントリの追加」（P.5-12）
- 「ARP インスペクションのイネーブル化」（P.5-13）

ARP インスペクションの設定のタスク フロー

ARP インスペクションを設定するには、次の手順を実行します。

ステップ 1　「スタティック ARP エントリの追加」（P.5-12）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。

ステップ 2　「ARP インスペクションのイネーブル化」（P.5-13）に従って、ARP インスペクションをイネーブルにします。

スタティック ARP エントリの追加

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。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、ASA 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。

手順の詳細

コマンド	目的
arp *interface_name ip_address mac_address* **例：** `hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100`	スタティック ARP エントリを追加します。

例

たとえば、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 応答を許可するには、次のコマンドを入力します。

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

次の作業

「ARP インスペクションのイネーブル化」（P.5-13）に従って、ARP インスペクションをイネーブルにします。

ARP インスペクションのイネーブル化

この項では、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。

手順の詳細

コマンド	目的
arp-inspection *interface_name* **enable** [**flood** | **no-flood**] **例：** `hostname(config)# arp-inspection outside enable no-flood`	ARP インスペクションをイネーブルにします。 **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。 **（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 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。

例

たとえば、外部インターフェイスで ARP インスペクションをイネーブルにして、一致しないすべての ARP パケットをドロップするには、次のコマンドを入力します。

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

ARP インスペクションのモニタリング

ARP インスペクションをモニタするには、次のタスクを実行します。

コマンド	目的
`show arp-inspection`	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。

ARP インスペクションの機能履歴

表 5-2 に、この機能のリリース履歴を示します。

表 5-3　ARP インスペクションの機能履歴

機能名	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。 **arp**、**arp-inspection**、および **show arp-inspection** コマンドが導入されました。

トランスペアレント ファイアウォール用の 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。次の項目を取り上げます。

- 「MAC アドレス テーブルに関する情報」（P.5-14）
- 「MAC アドレス テーブルのライセンス要件」（P.5-15）
- 「デフォルト設定」（P.5-15）
- 「注意事項と制限事項」（P.5-15）
- 「MAC アドレス テーブルの設定」（P.5-16）
- 「MAC アドレス テーブルのモニタリング」（P.5-17）
- 「MAC アドレス テーブルの機能履歴」（P.5-18）

MAC アドレス テーブルに関する情報

ASA 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 ASA 経由でパケットを送信すると、ASA 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、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。

ASA 5505 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、ブリッジMAC アドレス テーブルのみについて説明します。このテーブルは、VLAN 間のトラフィックのための、MAC アドレスから VLAN インターフェイスへのマッピングを保持します。

ASA 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、ASA 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 : ASA は宛先 IP アドレスに対して ARP 要求を生成し、ASA 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 : ASA は宛先 IP アドレスへの ping を生成し、ASA 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。

MAC アドレス テーブルのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

デフォルト設定

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。

注意事項と制限事項

コンテキスト モードのガイドライン

- シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。
- マルチ コンテキスト モードで、各コンテキスト内の MAC アドレス テーブルを設定します。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードでだけサポートされます。ルーテッド モードはサポートされていません。

その他のガイドライン

トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Cisco Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インター

フェイスではなく、*管理*インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

MAC アドレス テーブルの設定

この項では、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。次の項目を取り上げます。

- 「スタティック MAC アドレスの追加」（P.5-16）
- 「MAC アドレス タイムアウトの設定」（P.5-16）
- 「MAC アドレス ラーニングのディセーブル化」（P.5-17）

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、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、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」（P.5-12）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。

スタティック MAC アドレスを MAC アドレス テーブルに追加するには、次のコマンドを入力します。

コマンド	目的
mac-address-table static *interface_name mac_address* **例：** `hostname(config)# mac-address-table static inside 0009.7cbe.2100`	スタティック MAC アドレス エントリを追加します。 *interface_name* は、発信元インターフェイスです。

MAC アドレス タイムアウトの設定

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、次のコマンドを入力します。

コマンド	目的
mac-address-table aging-time *timeout_value* **例：** `hostname(config)# mac-address-table aging-time 10`	MAC アドレス エントリのタイムアウトを設定します。 *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 ラーニングのディセーブル化

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。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、次のコマンドを入力します。

コマンド	目的
mac-learn *interface_name* **disable** **例：** `hostname(config)# mac-learn inside disable`	MAC アドレス ラーニングをディセーブルにします。 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。

MAC アドレス テーブルのモニタリング

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。MAC アドレス テーブルを表示するには、次のコマンドを入力します。

コマンド	目的
show mac-address-table [*interface_name*]	MAC アドレス テーブルを表示します。

例

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。

```
hostname# 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。

```
hostname# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

MAC アドレス テーブルの機能履歴

表 5-2 に、この機能のリリース履歴を示します。

表 5-4　MAC アドレス テーブルの機能履歴

機能名	リリース	機能情報
MAC アドレス テーブル	7.0(1)	トランスペアレント ファイアウォール モードは MAC アドレス テーブルを使用します。 **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。