ファイアウォール デバイスでのブリッジング ポリシーの設定

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」のように機能するレイヤ2デバイスであり、接続されたデバイスへのルータホップとしては認識されません。セキュリティアプライアンスは、その内部および外部ポート上で同じネットワークを接続し、アクセス コントロール ブリッジとして機能します。各インターフェイスに異なる VLAN を割り当てます。IP アドレッシングは使用しません。

ファイアウォール デバイスでのブリッジングについて

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」のように機能するレイヤ2デバイスであり、接続されたデバイスへのルータホップとしては認識されません。セキュリティアプライアンスは、その内部および外部ポート上で同じネットワークを接続し、アクセス コントロール ブリッジとして機能します。各インターフェイスに異なる VLAN を割り当てます。IP アドレッシングは使用しません。

このように、既存のネットワークに簡単にトランスペアレントファイアウォールを導入できます。IP の再アドレッシングは必要ありません。また、トラブルシューティングすべき複雑なルーティング パターンも NAT 設定もないため、メンテナンスが容易になります。

トランスペアレント モードのデバイスはブリッジとして機能しますが、IP トラフィックのようなレイヤ 3 トラフィックは、特別なアクセス ルールで明示的に許可しないかぎり、セキュリティ アプライアンスを通過できません。アクセス リストなしでファイアウォールを通過できるトラフィックは ARP トラフィックだけであり、このトラフィックは ARP インスペクションおよび IPv6 ネイバー探索を使用して制御できます。

セキュリティ アプライアンスがトランスペアレント モードで実行している場合、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。ルート ステートメントは引き続き設定可能ですが、セキュリティアプライアンスから発信されたトラフィックにだけ適用されます。たとえば、syslog サーバがリモート ネットワークに配置されている場合は、セキュリティ アプライアンスがそのサブネットにアクセスできるように、スタティック ルートを使用する必要があります。

Cisco Security Manager 4.13 以降、ブリッジグループ仮想インターフェイス（BV） 機能がルーテッドファイアウォールモードに拡張されています。ルーテッドファイアウォールは、ブリッジグループを設定することによって実装されます。ユーザは、最大 8 つのブリッジグループを設定でき、ASA 9.7.1（Cisco Security Manager 4.13）では、各グループに最大 64 のインターフェイスを含めることができます。Cisco Security Manager 4.13 以前のバージョンでは、ユーザは最大 2 つのブリッジグループを設定できます。各グループには、最大 4 つのインターフェイスが含まれます。トランスペアレントモードでサポートされる BVI 機能に加えて、ルーテッド ファイアウォール モードには、次の追加の通信モードのサポートが含まれます。

- BVI 間通信
- BVI からデータポートへの通信（レイヤ 2 からレイヤ 3）およびその逆

トランスペアレント ファイアウォールを設定するには、次のポリシーを使用します。マルチコンテキスト モードの ASA/PIX/FWSM デバイスを設定する場合は、トランスペアレントのセキュリティ コンテキストごとに次のポリシーを設定します。

- **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**：アクセスルールは、拡張アクセスコントロールリストを使用して、レイヤ 3 以上のトラフィックを制御します。ルーテッド モードでは、一部のタイプのトラフィックは、アクセス リストで許可されていても、セキュリティアプライアンスを通過できません。たとえば、トランスペアレント ファイアウォールを介してルーティング プロトコルの隣接関係を確立できます。これにより、アクセス ルールに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックの通過を許可できます。同様に、HSRP または VRRP のようなプロトコルもセキュリティアプライアンスを通過できます。ただし、トランスペアレント モードのセキュリティ アプライアンスは CDP パケットを通過させません。

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については、上流および下流のルータでこれらの機能を提供できるように、トラフィックを通過させることがきます。たとえば、アクセス ルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックの通過を許可したり、IP/TV で作成されるようなマルチキャスト トラフィックの通過を許可したりできます。

詳細については、アクセスルールについておよびアクセスルールの設定を参照してください。

- **[ファイアウォール（Firewall）]>[トランスペアレントルール（Transparent Rules）]**：トランスペアレントルールは、Ethertype アクセスコントロールリストを使用して、非 IP のレイヤ 2 トラフィックを制御します。たとえば、AppleTalk、IPX、BPDU、および MPLS がデバイスを通過できるようにルールを設定できます。詳細については、トランスペアレント ファイアウォール ルールの設定を参照してください。
- **[プラットフォーム（Platform）]>[ブリッジング（Bridging）]>[ARPテーブル（ARP Table）]**、[ARPインスペクション（ARP Inspection）] および [IPv6ネイバーキャッシュ（IPv6 Neighbor Cache）]：これらのポリシーを使用して、ブリッジを通過できる ARP および IPv6 トラフィックのタイプを制御します。必要に応じて、スタティックな ARP エントリおよび IPv6 ネイバー キャッシュ エントリを設定して、これらのスタティック ルールで定義されていないトラフィックをドロップできます。MAC アドレス、IP アドレス、またはインターフェイス間に不一致がある場合に、セキュリティアプライアンスがパケットをドロップするように、ARP インスペクションをイネーブルにします。これによって、ARP スプーフィングを防ぐことができます。詳細については、[ARP Table] ページ （5 ページ）および [ARP Inspection] ページ （7 ページ）を参照してください。

（注） 非トランスペアレントの ASA/PIX/FWSM デバイスで使用できるブリッジング ポリシーは、[ARP Table] と [IPv6 Neighbor Cache] のみです。

- **[プラットフォーム（Platform）]>[ブリッジング（Bridging）]>[MACアドレステーブル（MAC Address Table）]** および [MACラーニング（MAC Learning）]：これらのポリシーを使用して、スタティックな MAC-IP アドレスマッピングを設定し、MAC 学習をイネーブルまたはディセーブルにします。MAC学習はデフォルトではイネーブルになっており、これによってアプライアンスは、トラフィックがインターフェイスを通過するときに MAC-IP アドレス マッピングを追加できます。スタティック エントリ以外のすべてのトラフィックを阻止する場合は、MAC 学習をディセーブルにできます。詳細については、[MAC Address Table] ページ （10 ページ）および [MAC Learning] ページ （12 ページ）を参照してください。
- [プラットフォーム（Platform）>[ブリッジング（Bridging）]>[管理IP（Management IP）]
- および [プラットフォーム（Platform）]>[ブリッジング（Bridging）]>[管理IPv6（Management IPv6）]：これらのポリシーを使用して、Security Manager がデバイスとの通信に使用する管理 IP アドレスを設定します。

（注） [Management IP] ページおよび [Management IPv6] ページは Catalyst 6500 サービス モジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

管理 IP アドレスを変更する場合は、デバイスまたはセキュリティ コンテキストのデバイス プロパティも更新する必要があります。次の手順に従ってください。

- 管理 IP アドレスを変更し、変更を保存して送信します。
- 変更をデバイスに展開します。
- デバイスビューで、デバイスまたはセキュリティコンテキストを選択してから、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択します。[General] ページで、新しい管理 IP アドレスを [IP Address] フィールドに入力します。[Credentials] タブで、管理インターフェイスにログインできるアカウントのクレデンシャルで、ユーザ名およびパスワードのフィールドを更新します。これで、Security Manager は、以降の展開およびデバイス通信に、このアドレスおよびユーザ アカウントを使用するようになります。

詳細については、[Management IP] ページ （13 ページ）を参照してください。

関連項目

- FWSM 3.1 のブリッジング サポート （4 ページ）
- ルーテッド モードおよびトランスペアレント モードのインターフェイス
- [Transparent Rules] ページ

FWSM 3.1 のブリッジング サポート

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

FWSM 3.1 では複数の L2 インターフェイスのペアをサポートできますが、Security Manager では 2 つの L2 インターフェイス（1 つのインターフェイス ペア）と、関連付けられた 1 つの管理 IP アドレスしか指定できません。つまり、関連付けられた 2 つの指定済みインターフェイスを含む 1 つのブリッジ グループだけが、管理 IP アドレスでプロビジョニングされます。デバイス設定に最大で 1 つのブリッジ グループと 2 つの指定済みインターフェイスが含まれている場合、このデバイス設定は検出対象になります。他のすべてのシナリオは、結果としてエラー メッセージが表示され、コマンドは検出時に拒否されます。さらに、検出では Security Manager にブリッジ グループ情報は表示されませんが、展開中にはブリッジ グループ コマンドが生成されます。ブリッジ グループがデバイス設定に存在しない場合、トランスペアレント ルール ポリシーでは、ブリッジ グループ 1 が展開および使用されます。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）

[ARP Table] ページ

[ARP Table] ページを使用して、MAC アドレスを IP アドレスにマッピングするスタティック ARP エントリを追加し、ホストに到達するために使用されるインターフェイスを識別します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [ARPテーブル（ARP Table）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [ARPテーブル（ARP Table）] を選択します。[ARPテーブル（ARP Table）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス （6 ページ）
- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Inspection] ページ （7 ページ）
- [MAC Address Table] ページ （10 ページ）
- [MAC Learning] ページ （12 ページ）
- [Management IP] ページ （13 ページ）

フィールド リファレンス

表 *1 : [ARP Table]* ページ

要素	説明
タイムアウト（秒）	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（60 ～ 4294967 秒）。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。 （注） 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。ARP テーブルに含まれているスタティックエントリではありません。
ARP テーブル	
インターフェイス	ホストが接続されるインターフェイス。

要素	説明
IPアドレス	ホストの IP アドレス。
MAC アドレス	ホストの MAC アドレス。
Alias Enabled	セキュリティ アプライアンスがこのマッピングのプロキシ ARP を実行するかどうかを示します。この設定がイネーブルにされ、指定したIPアドレスの ARP 要求をセキュリティ アプライアンスが受信した場合、セキュリティアプライアンスのMACアドレスで応答します。セキュリティアプライアンスは、このIPアドレスに属するホスト宛てのトラフィックを受信すると、このコマンドで指定したホストの MAC アドレスにそのトラフィックを転送します。この機能は、ARP を実行しないデバイスがある場合などに役立ちます。 （注） この設定は、トランスペアレント ファイアウォール モードでは無視され、セキュリティ アプライアンスはプロキシ ARP を実行しません。

[Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス

[Add ARP Configuration] と [Edit ARP Configuration] ダイアログボックスを使用して、MAC アドレスを IP アドレスにマッピングするスタティック ARP エントリを追加し、ホストに到達するために使用されるインターフェイスを識別します。

ナビゲーション パス

[Add/Edit ARP Configuration] ダイアログボックスには、[ARP Table] ページからアクセスできます。[ARP Table] ページの詳細については、を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Table] ページ （5 ページ）

フィールド リファレンス

表 2 : [Add/Edit ARP Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	ホスト ネットワークが接続されるインターフェイスの名前。
IPアドレス	ホストの IP アドレス。
MAC アドレス	ホストの MAC アドレス（00e0.1e4e.3d8b など）。

要素	説明
Enable Alias	選択すると、このマッピングのプロキシ ARP がイネーブルになります。指定した IP アドレスの ARP 要求をセキュリティ アプライアンスが受信した場合、セキュリティ アプライアンスの MAC アドレスで応答します。セキュリティ アプライアンスは、この IP アドレスに属するホスト宛てのトラフィックを受信すると、このコマンドで指定したホストの MAC アドレスにそのトラフィックを転送します。この機能は、ARP を実行しないデバイスがある場合などに役立ちます。 （注） この設定は、トランスペアレント ファイアウォール モードでは無視され、セキュリティアプライアンスはプロキシARPを実行しません。

[ARP Inspection] ページ

[ARP Inspection] ページを使用して、トランスペアレント ファイアウォールの ARP インスペクションを設定します。ARP インスペクションは、ARP スプーフィングを防ぐために使用されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [ARPインスペクション（ARP Inspection）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [ARPインスペクション（ARP Inspection）] を選択します。[ARPインスペクション（ARP Inspection）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス （6 ページ）
- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Table] ページ （5 ページ）
- [MAC Address Table] ページ （10 ページ）
- [MAC Learning] ページ （12 ページ）
- [Management IP] ページ （13 ページ）

フィールド リファレンス

表 *3 : [ARP Inspection]* ページ

要素	説明
[ARP Inspection] テーブル	
インターフェイス	ARP インスペクション設定が適用されるインターフェイスの名前。
ARP Inspection Enabled	指定した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するかどうかを示します。
Flood Enabled	スタティック ARP エントリのどの要素とも一致しないパケットが、発信元インターフェイス以外のすべてのインターフェイスからフラッドされるかどうかを示します。MAC アドレス、IP アドレス、またはインターフェイス間に不一致がある場合、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、すべての不一致パケットがドロップされます。 （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。

[Add/Edit ARP Inspection] ダイアログボックス

[Add/Edit ARP Inspection] ダイアログボックスを使用して、トランスペアレント ファイアウォール インターフェイスの ARP インスペクションをイネーブルまたはディセーブルにします。

ナビゲーション パス

[Add/Edit ARP Inspection] ダイアログボックスには、[ARP Inspection] ページからアクセスできます。[ARP Inspection] ページの詳細については、[ARP Inspection] ページ （7 ページ）を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Inspection] ページ （7 ページ）

フィールド リファレンス

表 4 : [Add ARP Inspection]/[Edit ARP Inspection] ダイアログボックス

要素	説明
インターフェイス（Interface）	ARP インスペクションをイネーブルまたはディセーブルにするインターフェイスの名前。
Enable ARP Inspection on this interface	選択すると、指定したインターフェイスで ARP インスペクションがイネーブルになります。
Flood ARP packets	選択すると、スタティック ARP エントリのどの要素とも一致しないパケットは、発信元インターフェイス以外の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に不一致がある場合、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、すべての不一致パケットがドロップされます。 （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。

IPv6 ネイバー キャッシュの管理

[IPv6 Neighbor Cache] ページを使用して、MAC アドレスを IPv6 アドレスにマッピングするスタティック IPv6 ネイバー エントリを管理します。また、ネイバー ホストに到達するために使用されるインターフェイスを識別して、IPv6 のアドレス解決機能を提供します。これは ASA 7.0 以降のデバイスでのみ使用できます。

（注） IPv6 ネイバー キャッシュ エントリは IPv6 におけるスタティック ARP エントリに相当し、[ARP Table] ページ （5 ページ）で管理されます。

指定された IPv6 アドレスのエントリがすでにネイバー探索キャッシュにある場合、つまり IPv6 ネイバー探索プロセスで取得されている場合、そのエントリは自動的にスタティック エントリに変換されます。IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

[IPv6 Neighbor Cache] ページは、Security Manager の標準のテーブルです。このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります（テーブルの使用に説明されているとおり、これらは標準のボタンです）。[行の追加（Add Row）] ボタンでは [IPv6 ネイバーキャッシュ設定の追加（Add IPv6 Neighbor Cache Configuration）] ダイアログボックスが開き、[行の編集（Edit Row）] ボタンでは [IPv6 ネイバーキャッシュ設定の編集（Edit IPv6 Neighbor Cache Configuration）] ダイアログボックスが開きます。タイトルを除き、この 2 つのダイアログボックスは同じです。

（注） 必ず少なくとも 1 つのインターフェイスで IPv6 をイネーブルにしてからネイバーを追加します。

フィールド リファレンス

表 5 : [Add Pv6 Neighbor Cache Configuration]/[Edit IPv6 Neighbor Cache Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	ネイバーを追加するインターフェイスの名前を入力または選択します。
IPアドレス	ローカルのデータリンク アドレスに対応する IPv6 アドレスを入力します（指定された IPv6 アドレスのエントリがすでにネイバー探索キャッシュにある場合、つまり IPv6 ネイバー探索プロセスで取得されている場合、そのエントリは自動的にスタティック エントリに変換されます）。
MAC アドレス	ホストのローカル データ回線（ハードウェア）の MAC アドレスを入力します（00e0.1e4e.3d8b など）。

[MAC Address Table] ページ

[MAC Address Table] ページを使用して、スタティック MAC アドレス エントリを MAC アドレス テーブルに追加します。このテーブルによって、MAC アドレスは送信元インターフェイスに関連付けられ、デバイスにアドレス指定されたパケットを正しいインターフェイスから送信することがセキュリティ アプライアンスで認識されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [MACアドレステーブル（MAC Address Table）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [MACアドレステーブル（MAC Address Table）] を選択します。[MACアドレステーブル（MAC Address Table）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス （6 ページ）

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Table] ページ （5 ページ）
- [ARP Inspection] ページ （7 ページ）
- [MAC Learning] ページ （12 ページ）
- [Management IP] ページ （13 ページ）

フィールド リファレンス

表 6 : [MAC Address Table] ページ

要素	説明
Aging Time (minutes)	MAC アドレス エントリがタイムアウトになるまでに MAC アドレス テーブル内に存在する時間を分（5 ～ 720（12 時間））で設定します。5 分がデフォルトです。
MAC アドレス テーブル	
インターフェイス	MAC アドレスを関連付けるインターフェイス。
MAC アドレス	MAC アドレス（00e0.1e4e.3d8b など）。

[Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックス

[Add MAC Table Entry] と [Edit MAC Table Entry] ダイアログボックスを使用して、スタティック MAC アドレス エントリを MAC アドレス テーブルに追加するか、MAC アドレス テーブル内のエントリを変更します。

ナビゲーション パス

[Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックスには、[MAC Address Table] ページからアクセスできます。[MAC Address Table] ページの詳細については、 [MAC Address Table] ページ （10 ページ）を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [MAC Address Table] ページ （10 ページ）

フィールド リファレンス

表 7 : [Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックス

要素	説明
インターフェイス（Interface）	MACアドレスを関連付けるインターフェイス。
MAC アドレス	MAC アドレス（00e0.1e4e.3d8b など）。

[MAC Learning] ページ

[MAC Learning] ページを使用して、インターフェイスで MAC アドレス ラーニングをイネーブルまたはディセーブルにします。デフォルトでは、各インターフェイスで入力トラフィックの MAC アドレスが学習され、対応するエントリがセキュリティ アプライアンスによって MAC アドレス テーブルに追加されます。必要な場合は、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。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックはセキュリティ アプライアンスを通過できません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [MAC ラーニング（MAC Learning）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [MAC ラーニング（MAC Learning）] を選択します。[MAC インスペクション（MAC Inspection）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add MAC Learning]/[Edit MAC Learning] ダイアログボックス （13 ページ）
- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Table] ページ （5 ページ）
- [ARP Inspection] ページ （7 ページ）
- [MAC Address Table] ページ （10 ページ）
- [Management IP] ページ （13 ページ）

フィールド リファレンス

表 8 : [MAC Learning] ページ

要素	説明
MAC Learning Table	
インターフェイス	MAC 学習設定を適用するインターフェイス。
MAC Learning Enabled	セキュリティ アプライアンスがインターフェイスに入るトラフィックから MAC アドレスを学習するかどうかを示します。

[Add MAC Learning]/[Edit MAC Learning] ダイアログボックス

[Add MAC Learning] と [Edit MAC Learning] ダイアログボックスを使用して、インターフェイスで MAC アドレス ラーニングをイネーブルまたはディセーブルにします。

ナビゲーション パス

[Add/Edit MAC Learning] ダイアログボックスには、[MAC Learning] ページからアクセスできます。[MAC Learning] ページの詳細については、[MAC Learning] ページ （12 ページ）を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [MAC Learning] ページ （12 ページ）

フィールド リファレンス

表 9 : [Add MAC Configuration]/[Edit MAC Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	MAC 学習設定を適用するインターフェイス。
MAC Learning Enabled	選択すると、セキュリティ アプライアンスはインターフェイスに入るトラフィックから MAC アドレスを学習します。

[Management IP] ページ

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。デバイスに必要な IP 設定は、管理 IP アドレスの指定のみです。管理 IP アドレスは、システム メッセージや AAA サーバとの通信など、デバイスで発信されるトラフィックの送信元アドレスとして使用されます。このアドレスは、リモート管理アクセスにも使用できます。

IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、管理 IP アドレスが必要です。

（注） デバイスの管理 IP アドレスに加えて、Management 0/0 または 0/1 の管理専用インターフェイスの IP アドレスを設定できます。この IP アドレスは、メインの管理 IP アドレスとは別のサブネットに設定できます。

[Management IP] ページを使用して、セキュリティ デバイスの管理 IP アドレス、またはトランスペアレント ファイアウォール モードのコンテキストの管理 IP アドレスを設定します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理IP（Management IP）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [管理IP（Management IP）] を選択します。[管理IP（Management IP）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Table] ページ （5 ページ）
- [ARP Inspection] ページ （7 ページ）
- [MAC Address Table] ページ （10 ページ）
- [MAC Learning] ページ （12 ページ）

フィールド リファレンス

表 10 : [Management IP] ページ

要素	説明
管理 IP アドレス（Management IP Address）	管理 IP アドレス。
サブネットマスク	管理 IP アドレスに対応するサブネット マスク。

[Management IPv6] ページ（ASA 5505）

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。デバイスに必要な IP 設定は、管理 IP アドレスの指定のみです。管理 IP アドレスは、システム メッセージや

AAA サーバとの通信など、デバイスで発信されるトラフィックの送信元アドレスとして使用されます。このアドレスは、リモート管理アクセスにも使用できます。

IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。グローバルアドレスを設定する場合、各インターフェイスにリンクローカル アドレスが自動的に設定されるため、特にリンクローカルアドレスを設定する必要はありません。ただし、グローバル管理アドレスを設定しない場合、IPv6 インターフェイスの設定（ASA/FWSM）の説明に従って、インターフェイス リンクローカル アドレスを設定する必要があります。1 つのデバイスには IPv6 管理アドレスと IPv4 管理アドレスの両方を設定できます。

トランスペアレント モードの ASA 5505 では、[Management IPv6] ページを使用して IPv6 をイネーブルにし、ネイバー送信要求を設定して、IPv6 インターフェイス アドレスを管理します。

（注） このページは、トランスペアレント モードの ASA 5505 バージョン 8.2 および 8.3 のデバイスでのみ使用できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理 IPv6（Management IPv6）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [管理 IPv6（Management IPv6）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ファイアウォール デバイスでのブリッジングについて （1 ページ）
- [ARP Table] ページ （5 ページ）
- [ARP Inspection] ページ （7 ページ）
- [MAC Address Table] ページ （10 ページ）
- [MAC Learning] ページ （12 ページ）

フィールド リファレンス

表 *11 : [Management IPv6]* ページ

要素	説明
IPv6を有効化（Enable IPv6）	IPv6 をイネーブルにして、IPv6 管理インターフェイス アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると IPv6 をディセーブルにできますが、設定情報は保持されます。
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに 0 ～ 600 の数を入力します。0 を入力すると、重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカルアドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバルアドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカルアドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカルアドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。

要素	説明
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。
Interface IPv6 Addresses	このテーブルに一覧表示される管理インターフェイスに割り当てられている IPv6 アドレス。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Address for Interface] ダイアログボックスが開きます。

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。