トランスペアレントファイアウォールルールの管理

トランスペアレント ファイアウォール ルールは、非 IP レイヤ 2 トラフィックのアクセス コントロール ルールです。これらのルールを使用して、レイヤ 2 パケット内の Ethertype 値に基づいてトラフィックを許可またはドロップできます。

この章は次のトピックで構成されています。

トランスペアレント ファイアウォール ルールの設定

トランスペアレント ファイアウォール ルールは、非 IP レイヤ 2 トラフィックのアクセス コントロール ルールです。これらのルールを使用して、レイヤ 2 パケット内の Ethertype 値に基づいてトラフィックを許可またはドロップできます。これらのルールによって、デバイス上に Ethertype アクセス コントロール リストが作成されます。トランスペアレント ルールを使用すると、デバイスでの非 IP トラフィック フローを制御できます（IP トラフィックを制御するには、アクセス ルールを使用します。アクセス ルールについてを参照してください）。

トランスペアレント ファイアウォールは、ブリッジ経由のトラフィック フローを制御するために単一のサブネット内に配置するデバイスです。トランスペアレントファイアウォールを使用すると、ネットワークに番号を付け直すことなく、サブネット上にファイアウォールを配置できます。

トランスペアレント ルールは、次のタイプのインターフェイス上でだけ設定できます。

- **IOS 12.3(7)T 以降のデバイスの場合**：ブリッジグループの一部であるレイヤ 3 インターフェイス上：
  - [インターフェイス（Interfaces）] > [インターフェイスポリシー（Interfaces policy）] で、ブリッジするインターフェイスをレイヤ 3 として設定します。
  - [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）] ポリシーで、2 つ以上のレイヤ 3 インターフェイスが含まれるブリッジ

グループを設定します（Cisco IOS ルータにおけるブリッジングおよびブリッジ グループの定義を参照）。

- このブリッジ グループと同じ番号を使用して、Bridge-group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）を作成します（ブリッジ グループ仮想インターフェイスを参照）。たとえば、ブリッジ グループ 12 を作成する場合は、BVI12 を作成します。

- **ASA、PIX 7.0 以降、FWSM デバイスの場合**：デバイスがトランスペアレント モードで実行されている場合の任意のインターフェイス上。複数のコンテキストを使用する場合は、個々のセキュリティ コンテキストでルールを設定します。

[プラットフォーム（Platform）] > [ブリッジング（Bridging）] ポリシーグループで設定できるその他のブリッジングポリシーには、ARP テーブルと ARP インスペクション、MAC テーブルと MAC 学習ディセーブル化機能、およびデバイスのリモート管理を可能にするための管理 IP アドレスの設定機能があります。トランスペアレント ファイアウォールの詳細については、ファイアウォール デバイスでのブリッジング ポリシーの設定およびルーテッド 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を参照してください。

ヒント トランスペアレント モードの ASA、PIX、および FWSM では、すべての IP トラフィックがデバイスを通過できるようにアクセス ルールを設定する必要があります。トランスペアレント ルールでは、レイヤ 2 の非 IP トラフィックだけが制御されます。

また、セキュリティ デバイスでネットワーク アドレス変換を使用する方法については、トランスペアレント モードの NATを参照してください。

これらのインターフェイス上に、他のタイプのファイアウォール ルールを設定することもできます。その他のタイプのルールは、レイヤ 3 以上のトラフィックに適用されます。

ヒント トランスペアレントルールを設定すると、暗黙的な **deny all** ルールが、各インターフェイスのルールリストの最後に追加されます。必要なトラフィックをすべて許可していることを確認してください。特定のタイプのトラフィックだけを許可するのではなく、単に特定のタイプのトラフィックを拒否する場合は、**permit any**（ASA/PIX/FWSM デバイスの場合）または **permit 0x0000 0xFFFF**（IOS デバイスの場合）ルールをテーブル内の最後のルールとして含めることができます。

関連項目

- ルールの追加および削除
- ルールの編集
- ルールのイネーブル化とディセーブル化

ステップ 1 次のいずれかを実行して、[Transparent Rules] ページ （4 ページ）を開きます。

- （デバイスビュー）サポートされているデバイスタイプのポリシーセレクタから [ファイアウォール（Firewall）] > [トランスペアレントルール（Transparent Rules）] 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 [ファイアウォール（Firewall）]>[トランスペアレントルール（Transparent Rules）] を選択します。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。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （6 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （6 ページ）を参照してください。

- 許可または拒否：ルールに一致したトラフィックを許可するか、またはドロップするか。
- インターフェイス：ルールを設定するインターフェイスまたはインターフェイス ロール。
- このルールを適用するトラフィックの方向（[in] または [out]）。デフォルトは [in] です。
- EtherType：トラフィックを識別する 16 進コードまたはキーワード（ASA/PIX/FWSM の場合だけ）。コードのリストについては、https://www.ietf.org/rfc/rfc1700.txtで RFC 1700 を参照し、「EtherType」を検索してください。ASA/PIX/FWSM の場合、キーワードを選択して一部の EtherType を識別できます。ASA/PIX/FWSM の場合、このコードは少なくとも 0x0600 である必要があります。
- マスク：IOS デバイスに適用するルールの場合は、EtherType に適用するマスクも指定する必要があります。EtherType が文字どおり解釈されるようにするには、0xFFFF を使用します。

EtherType のグループに適用する単一のルールを作成する場合は、EtherType を 2 進数に変換し、適切なマスクを計算します。この場合、1 は、EtherType を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します。次に、マスクを 16 進数に変換する必要があります。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性を参照してください。

ステップ 5 （IOS デバイスだけ）IOS デバイスでトランスペアレント ルールを設定する場合、DHCP トラフィックを検査せずにブリッジ経由で転送できます。これを設定するには、[ファイアウォール（Firewall）] > [設定（Settings）]>[検査（Inspection）] ポリシーを選択し、[DHCPパススルーを許可（トランスペアレントファイアウォール）（Permit DHCP Passthrough (Transparent Firewall)）] オプションを選択します。この設定は、

一部の IOS バージョンではサポートされていないため、検証結果をよく調べて、使用しているデバイスで設定できるかどうかを確認してください。

[Transparent Rules] ページ

[Transparent Rules] ページを使用して、非 IP レイヤ 2 トラフィックのアクセスを制御します（IP トラフィック アクセスを制御するには、アクセス ルールを使用します。アクセス ルールについてを参照してください）。

トランスペアレント ルールの対象は、トランスペアレント ファイアウォール（トランスペアレント モードで動作する ASA、PIX 7.0+、および FWSM の各デバイス）またはレイヤ 3 インターフェイス（IOS 12.3(7)T+ デバイス上のブリッジ グループに属している）に限定されます。展開されたトランスペアレント ルールは、Ethertype アクセス コントロール リストになります。

トラフィックをデバイス経由で両方向に渡せるようにするには、すべてのブリッジ インターフェイスに同じルールを設定します。

トランスペアレント ファイアウォールの設定の詳細について、およびこれらのルールを展開するためのデバイス要件については、トランスペアレント ファイアウォール ルールの設定 （1 ページ）を参照してください。

ヒント　ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。

ナビゲーション パス

トランスペアレント ルールにアクセスするには、次のいずれかを実行します。

- （デバイス ビュー）サポートされているデバイス タイプのポリシー セレクタから [ファイアウォール（Firewall）] > [トランスペアレント ルール（Transparent Rules）] 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 [ファイアウォール（Firewall）] > [トランスペアレント ルール（Transparent Rules）] を選択します。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。
- （マップ ビュー）デバイスを右クリックし、[ファイアウォール ポリシーの編集（Edit Firewall Policies）] > [トランスペアレント ルール（Transparent Rules）] を選択します。

関連項目

- 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
- 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

- Cisco IOS ルータにおけるブリッジング
- ブリッジ グループの定義
- ブリッジ グループ仮想インターフェイス
- テーブルのフィルタリング

フィールド リファレンス

表 *1 : [Transparent Rules]* ページ

要素	説明
番号	順序が付けられたルール番号。
許可（Permit）	設定された次の条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。
EtherType	Ethernet パケット タイプ。パケット内の EtherType 値です。16 進コードまたはキーワードとなります。
Mask	EtherType の 16 ビットの 16 進マスク（IOS デバイスだけ）。0xFFFF のマスクは、EtherType がリテラルであることを示します。それ以外のマスクはすべて、EtherType 内の対応するビットを無視することを示します。マスクを完全に解釈するには、16 進数を 2 進数に変換する必要があります（2 進数 1 は、対応する EtherType 値を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します）。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。インターフェイス ロール オブジェクトについてを参照してください。
Dir.	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
説明	ルールの説明（ある場合）。
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページを参照）。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性を参照してください。
[Add Row] ボタン	[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （6 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス

[Add Transparent Firewall Rule] および [Edit Transparent Firewall Rule] の各ダイアログボックスを使用して、デバイス上で EtherType アクセス コントロール リストとして設定されているトランスペアレント ファイアウォール ルールを追加および編集します。トランスペアレント ルールを設定する前に、 トランスペアレント ファイアウォール ルールの設定 （1 ページ）を読んでください。

ナビゲーション パス

[Transparent Rules] ページ （4 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- 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
- 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

- Cisco IOS ルータにおけるブリッジング
- ブリッジ グループの定義
- ブリッジ グループ仮想インターフェイス
- ルールの編集
- ルールの追加および削除

フィールド リファレンス

表 2 : [Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルールテーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。
操作	定義した条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。ブリッジングされたトランスペアレント インターフェイスだけを選択する必要があります（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 （1 ページ）を参照してください）。 インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについてを参照してください。
トラフィックの方向	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。

要素	説明
EtherType	パケット内の EtherType 値に基づいたトラフィックを識別する 16 進のコードまたはキーワード（ASA/PIX/FWSM 専用）。次の内容を入力または選択します。 • 16 進の EtherType 値。コードのリストについては、http://www.ietf.org/rfc/rfc1700.txt「Ether Type」の RFC 1700 を参照してください。 • IOS デバイス：0x0000 ～ 0xFFFF の任意の値を入力できます。 • ASA/PIX/FWSM デバイス：値は 0x0600 以降である必要があります。 • ASA/PIX/FWSM デバイスの場合、次のキーワードも選択できます。 • bpdu：スパニング ツリー ブリッジ プロトコル データ ユニット • ipx：インターネット パケット交換 • mpls-unicast：マルチプロトコル ラベル スイッチング、ユニキャスト。 • mpls-multicast：MPLS マルチキャスト。 • isis：IS-IS パススルー • any：EtherType に関係なく、すべてのパケット。 • eii-ipx • raw-ipx ヒント　上記のリストのキーワード「isis」は、Security Manager 4.4 の新機能である IS-IS パススルーサポートを指します。「IS-IS パススルーサポート」とは、IS-IS トラフィックが透過モードで ASA を通過できることを意味します。 （注）　4.16 以降、ethertype dsap CLI を使用して、インストールされた ACE を、ether タイプ bpdu、ipx、または isis で作成されたかどうかに関係なく、ether タイプ dsap フォーマットで解釈します。この機能は、ASA 9.9(1) 以降のデバイスでサポートされています。
Wildcard Mask (IOS)	マスクは、EtherType コードの解釈方法を決定する 16 ビットの 16 進数です。 0xFFFF のマスクは、EtherType がリテラルであることを示します。それ以外のマスクはすべて、EtherType 内の対応するビットを無視することを示します。マスクを完全に解釈するには、16 進数を 2 進数に変換する必要があります（2 進数 1 は、対応する EtherType 値を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します）。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。

[Edit Transparent EtherType] ダイアログボックス

[Edit Transparent EtherType] 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 ルールの EtherType を編集します。トラフィックを識別する 16 進コードを入力します。ASA/PIX/FWSM デバイスの場合、一部のタイプのトラフィックには、キーワードを選択することもできます。コードのリストについては、http://www.ietf.org/rfc/rfc1700.txtで RFC 1700 を参照し、「EtherType」を検索してください。EtherType の詳細については、[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （6 ページ）を参照してください。

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 （1 ページ）を参照してください。

ナビゲーション パス

トランスペアレントルール（[Transparent Rules] ページ （4 ページ））の [EtherType] セルを右クリックし、[EtherTypeの編集（Edit EtherType）] を選択します。一度に 1 つの行の EtherType を編集できます。

[トランスペアレントマスクの編集（Edit Transparent Mask）] ダイアログボックス

[Edit Transparent Mask] ダイアログボックスを使用して、IOS デバイス用のトランスペアレント ファイアウォール ルールのマスクを編集します。マスクは、EtherType コードの解釈方法を決定する 16 ビットの 16 進数です。

0xFFFF のマスクは、EtherType がリテラルであることを示します。それ以外のマスクはすべて、EtherType 内の対応するビットを無視することを示します。マスクを完全に解釈するには、16 進数を 2 進数に変換する必要があります（2 進数 1 は、対応する EtherType 値を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します）。

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 （1 ページ）を参照してください。

ナビゲーション パス

トランスペアレントルール（ [Transparent Rules] ページ （4 ページ）） の [マスク（Mask）] セルを右クリックし、[マスクの編集（Edit Mask）] を選択します。一度に 1 つの行のマスクを編集できます。

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。