CHAPTER 17

アクセス ルールと EtherType ルールの設定

この章では、アクセス ルールと EtherType ルール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。

（注） アクセス ルールを使用して、ルーテッド ファイアウォール モードおよび透過ファイアウォール モードの両方のネットワーク アクセスを制御します。透過モードでは、アクセス ルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

管理アクセスのために FWSM インターフェイスにアクセスする場合、ホスト IP アドレスを許可するアクセス ルールも必要ありません。ただし、第 11 章「Device Access」に従って、管理アクセスを設定する必要があります。

アクセス ルールと EtherType ルールの概要

アクセス ポリシーは、1 つのインターフェイスごとに 1 つ以上のアクセス ルールと EtherType ルールで構成されます。

ルーテッド ファイアウォール モードおよび透過ファイアウォール モードでアクセス ルールを使用して、IP トラフィックを制御できます。アクセス ルールは、プロトコル、送信元および宛先 IP アドレスまたはネットワーク、オプションで送信元および宛先ポートに基づいてトラフィックを許可または拒否します。

（注）　すべてのトラフィックが FWSM に入るのを許可するには、インターフェイスに着信アクセス ルールを設定する必要があります。設定しない場合、FWSM は、そのインターフェイスに入るすべてのトラフィックを自動的にドロップします。

透過モードでは、EtherType ルールは IP トラフィック以外のネットワーク アクセスを制御します。EtherType ルールは、EtherType に基づいてトラフィックを許可または拒否します。

ここでは、次の項目について説明します。

アクセス ルールと EtherType ルールについて

この項では、アクセス ルールと EtherType ルールの両方に関する情報を提供します。次の項目を取り上げます。

同じインターフェイスでのアクセス ルールと EtherType ルールの使用

インターフェイスの各方向に、アクセス ルールと EtherType ルールの両方を適用できます。

ルールの順序

ルールの順序は重要です。FWSM がパケットを転送するかドロップするかを決定すると、FWSM はルールが記載されている順序で各ルールに対してパケットをテストします。一致が見つかると、その後のルールはチェックされません。たとえば、最初にインターフェイスのすべてのトラフィックを明示的に許可するアクセス ルールを作成した場合、その後のルールは一切チェックされません。

ルールを非アクティブにすることで、そのルールをディセーブルにできます。

暗黙拒否

アクセス ルールまたは EtherType ルールのリストには、リストの最後に暗黙拒否があります。そのため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除いて、FWSM を経由してすべてのユーザがネットワークにアクセスできるようにする場合、特定のアドレスを拒否して、他のすべてのアドレスを許可する必要があります。

EtherType ルールでは、暗黙拒否は、IPv4 トラフィックまたは ARP に影響しません。たとえば、EtherType 8037（IPX の EtherType）を許可した場合、リストの最後の暗黙拒否は、アクセス ルールを使用して以前許可したすべての IP トラフィックをブロックしません。IPv4 および ARP トラフィックは、EtherType ルールで制御できません。

ルールのコミットメント

アクセス ルールまたは EtherType ルールを適用すると、FWSM は、そのルールをネットワーク プロセッサにコミットすることでアクティブにします。FWSM は、ルールを最後に適用した後、短時間待ってからルールをコミットします。コミットメントの開始後にルールを適用した場合、FWSM は、コミットメントを打ち切り、短時間待ってからルールを再コミットします。ルールをコミットした後、FWSM は次のようなメッセージを表示します。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

サイズによっては、約 6 万個のルールで構成される大きなリストはコミットに 3 ～ 4 分かかることがあります。

メモリの制限を超える場合については、「アクセス ルールおよび EtherType ルールの最大数」の項を参照してください。

アクセス ルールおよび EtherType ルールの最大数

FWSM では、システム全体に対して、アクセス ルールおよび EtherType ルールの最大数をサポートしています。アクセス ルールと EtherType ルール、およびその他のタイプのルールを含む、ルールの制限については P.A-7 の「ルール制限」を参照してください。

アクセス ルールによっては他のルールよりも多くのメモリを使用するものがあり、それらには、広範囲のポート番号または重複ネットワークを使用するルールが含まれます（たとえば、あるアクセス ルールで 10.0.0.0/8 を指定し、他のルールで 10.1.1.0/24 を指定すると、結果的に重複ネットワークがあるルールとなります）。アクセス ルールのタイプによっては、システムがサポートできる実際の制限は最大数よりも少なくなります。

アクセス ルールでオブジェクト グループを使用すると、入力する実際のルールの数は少なくなりますが、*拡張*ルールの数はオブジェクト グループを使用しない場合と同じになり、拡張ルールの数はシステム制限に近づきます。アクセス ルールの拡張ルール数を表示するには、CLI ツールを使用して **show access-list** コマンドを入力します。

ルールを追加して、FWSM がルールをコミットすると、コンソールに使用されたメモリ量が次のようなメッセージで表示されます。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

メモリ制限を超えた場合、エラー メッセージとシステム ログ メッセージ（106024）が表示され、そのコミットメントで追加されたすべてのアクセス ルールがコンフィギュレーションから削除されます。以前のコミットメントで正常にコミットされたルールのセットのみが使用されます。たとえば、1000 個のルールを適用し、最後のルールがメモリ制限を超えている場合、1000 個のルールがすべて拒否されます。

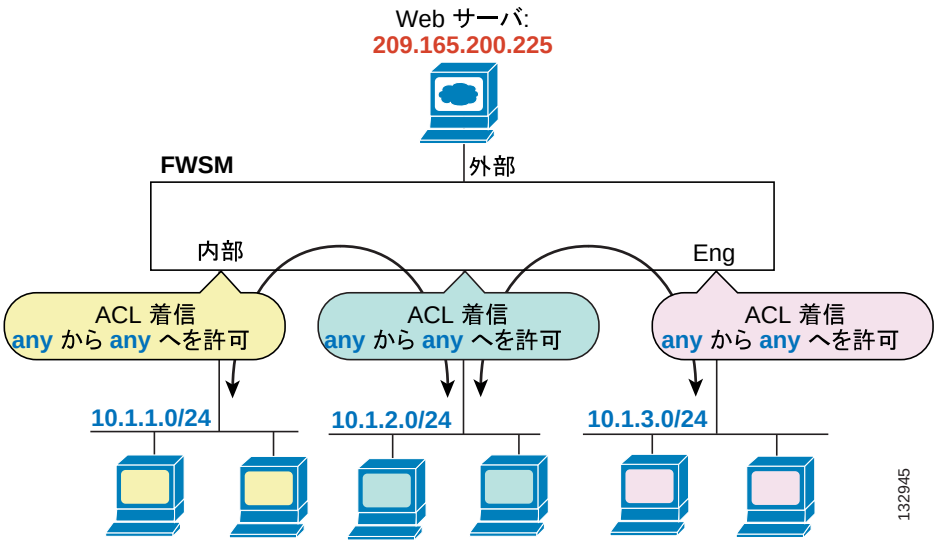
着信ルールと発信 ルール

FWSM のインターフェイスを流れるトラフィックは 2 つの方向で制御できます。FWSM に入るトラフィックは、送信元インターフェイスに着信アクセス ルールを設定することで制御できます。FWSM を出るトラフィックは、宛先インターフェイスに発信アクセス ルールを設定することで制御できます。すべてのトラフィックが FWSM に入るのを許可するには、インターフェイスに着信アクセス ルールを設定する必要があります。設定しない場合、FWSM は、そのインターフェイスに入るすべてのトラフィックを自動的にドロップします。デフォルトで、着信アクセス ルールですでに設定されているルールに制限を追加する発信アクセス ルールを使用して制限していない限り、トラフィックはすべてのインターフェイスで FWSM から出ることができます。

（注）「着信」および「発信」とは、インターフェイスでのアクセス　ルールの適用のことであり、インターフェイス上の FWSM に入るトラフィック、またはインターフェイス上の FWSM を出るトラフィックのいずれかを指します。これらの用語は、一般に着信と呼ばれる、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へのトラフィックの移動、または一般に発信と呼ばれる、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へのトラフィックの移動のことを指すものではありません。

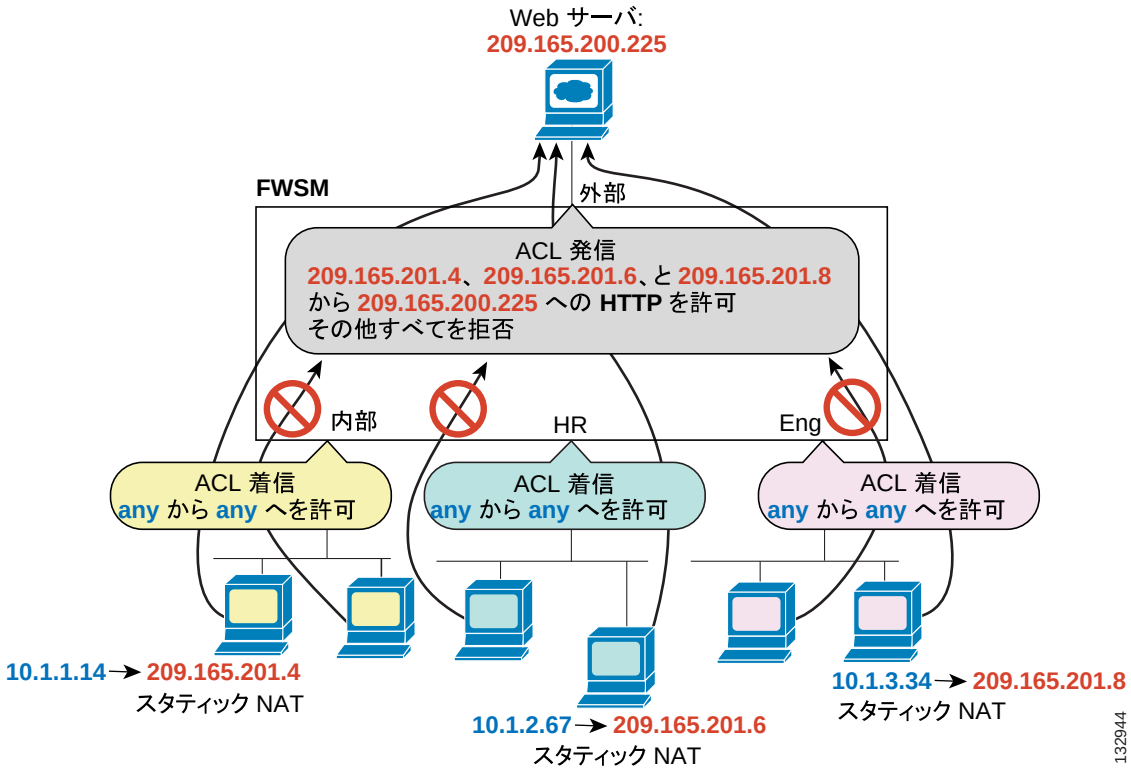
発信アクセス ルールを使用してコンフィギュレーションを単純化することも可能です。たとえば、3 つの異なるインターフェイスで 3 つの内部ネットワークの相互アクセスを許可する場合、各内部インターフェイスですべてのトラフィックを許可する単純な着信アクセス ルールを作成できます（図 17-1 を参照してください）。

図 17-1　着信アクセス ルール



内部ネットワークの特定のホストにのみ、外部ネットワークの Web サーバへのアクセスを許可する場合、指定したホストだけを許可するより限定的なアクセス ルールを作成して、外部インターフェイスの発信方向に適用することができます（図 17-2 を参照してください）。NAT および IP アドレスについては、P.17-5 の「NAT を使用する場合にアクセス ルールに使用される IP アドレス」を参照してください。発信アクセス ルールは、他のホストが外部ネットワークに到達することを防ぎます。

図 17-2　発信アクセス ルール



アクセス ルールの概要

この項では、アクセス ルールについて説明します。次の項目を取り上げます。

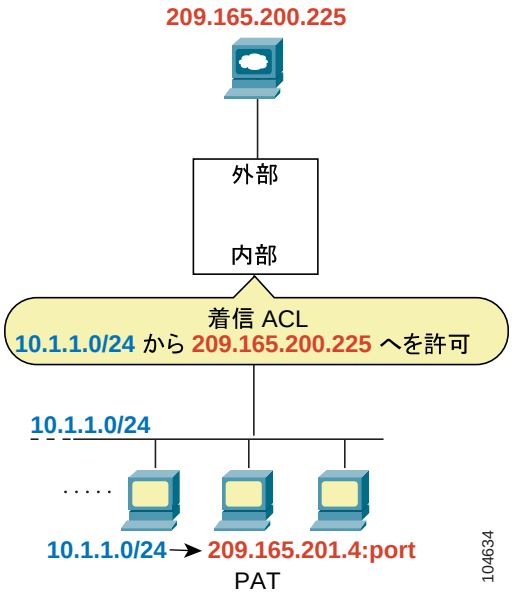
- NAT を使用する場合にアクセス ルールに使用される IP アドレス（P. 17-5）
- 戻りトラフィックのアクセス ルール（P. 17-7）
- アクセス　ルールを使用した透過ファイアウォール経由のブロードキャストおよびマルチキャスト トラフィックの許可（P. 17-7）

NAT を使用する場合にアクセス ルールに使用される IP アドレス

NAT を使用する場合、アクセス ルールに指定する IP アドレスは、アクセス ルールを設定するインターフェイスによって異なります。つまり、インターフェイスに接続されているネットワークで有効なアドレスを使用する必要があります。このガイドラインは、着信アクセス ルールと発信アクセス ルールの両方に適用されます。したがって、使用されるアドレスは方向によって決まりません。インターフェイスによってのみ決まります。

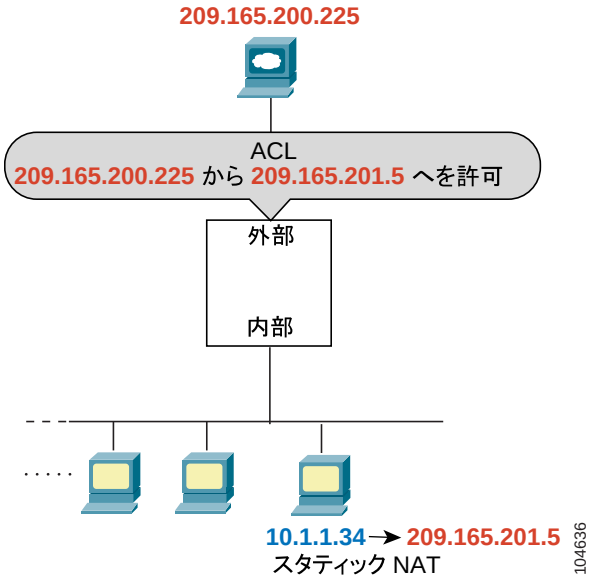
たとえば、内部インターフェイスの着信方向にアクセス ルールを適用するとします。この場合、内部送信元アドレスが外部アドレスにアクセスするときに、それらのアドレス上で NAT を実行するように FWSM を設定します。アクセス ルールは内部インターフェイスに適用されるため、送信元アドレスは元の変換されていないアドレスになります。外部アドレスは変換されていないため、アクセス ルールで使用される宛先アドレスは実際のアドレスになります（図 17-3 を参照してください）。

図 17-3　アクセス ルールの IP アドレス：送信元アドレスに使用される NAT



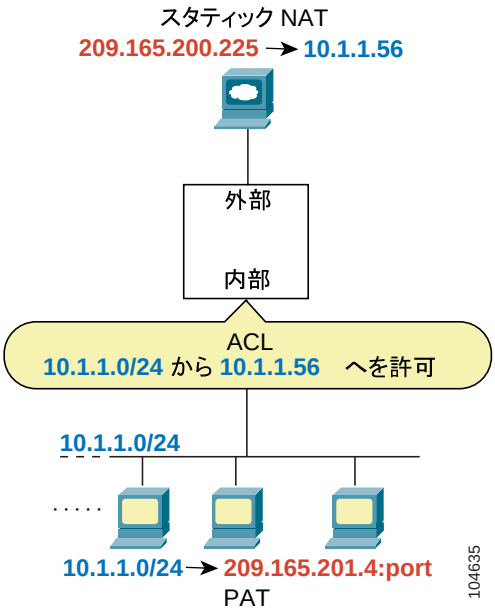
外部ホストが内部ホストにアクセスできるようにすると、外部インターフェイスで着信アクセス ルールを適用できます。内部ホストの変換済みアドレスは外部ネットワークで使用可能なアドレスであるため、アクセス ルールにそのアドレスを指定する必要があります（図 17-4 を参照してください）。

図 17-4　アクセス ルールの IP アドレス：宛先アドレスに使用される NAT



両方のインターフェイスで NAT を実行する場合、所定のインターフェイスから見えるアドレスに留意してください。図 17-5 では、変換済みアドレスが内部ネットワークに表示されるように、外部サーバはスタティック NAT を使用しています。

図 17-5　アクセス ルールの IP アドレス：送信元アドレスおよび宛先アドレスで使用される NAT



戻りトラフィックのアクセス ルール

ルーテッド モードと透過モードの両方の TCP 接続および UDP 接続で、FWSM は、確立された双方向接続に対してすべての戻りトラフィックを許可するため、戻りトラフィックを許可するためのアクセスリストは不要です。ただし、ICMP などのコネクションレス型プロトコルでは、FWSM は、単方向セッションを確立します。したがって、双方向での ICMP を許可するアクセスリストを使用するか（送信元インターフェイスおよび宛先インターフェイスにアクセスリストを適用することによって）、または ICMP 検査エンジンをイネーブルにする必要があります。ICMP 検査エンジンは、ICMP セッションを双方向接続として扱います。

アクセス ルールを使用した透過ファイアウォール経由のブロードキャストおよびマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードで、アクセス ルールで許可している場合でも、サポートされていないダイナミック ルーティング プロトコルおよび DHCP を含めて（DHCP リレーを設定している場合を除く）、ブロードキャスト トラフィックとマルチキャスト トラフィックはブロックされます。透過ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。この機能は、たとえばダイナミック ルーティングを許可しないマルチコンテキスト モードで特に便利です。

（注）　これらの特殊なタイプのトラフィックはコネクションレス型であり、拡張アクセスリストを両方のインターフェイスに適用する必要があるため、戻りトラフィックの通過が可能です。

表 17-1 に、透過ファイアウォールを通過させることができる一般的なトラフィック タイプを示します。

表 17-1　透過ファイアウォールの特殊なトラフィック

トラフィック タイプ	プロトコルまたはポート	注意
DHCP	UDP ポート 67 および 68	DHCP サーバをイネーブルにした場合、FWSM は DCHP パケットを通過させません。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートはアプリケーションによって異なります。	マルチキャスト ストリームは、常にクラス D アドレス（224.0.0.0 ～ 239.x.x.x）を宛先とします。
RIP（v1 または v2）	UDP ポート 520	—

EtherType ルールの概要

この項では、EtherType ルールについて説明します。次の項目を取り上げます。

- サポートされている EtherType（P. 17-8）
- 双方向での EtherType ルールの適用（P. 17-8）
- MPLS の許可（P. 17-9）

サポートされている EtherType

EtherType ルールは、16 ビットの 16 進数で識別されるすべての EtherType を制御します。

EtherType ルールは、イーサネット V2 フレームをサポートします。

802.3 フォーマットのフレームは、タイプ フィールドではなく長さフィールドを使用するため、EtherType ルールでは処理されません。

唯一の例外は、EtherType ルールで処理する BPDU です。BPDU は、SNAP でカプセル化され、FWSM は特に BPDU を処理できるように設計されています。

FWSM のポートはトランク ポート（シスコ独自）であるため、FWSM はトランク ポート BPDU を受信します。トランク BPDU にはペイロード内に VLAN 情報があるため、BPDU を許可した場合、FWSM は発信 VLAN を使用してペイロードを変更します。

（注） フェールオーバーを使用する場合、ブリッジング ループを防止するために、EtherType ルールを使用して両方のインターフェイスの BPDU を許可する必要があります。

双方向での EtherType ルールの適用

EtherType はコネクションレス型であるため、トラフィックを双方向に通過させる場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合、Label Distribution Protocol（LDP; ラベル配布プロトコル）および Tag Distribution Protocol（TDP; タグ配布プロトコル）の TCP 接続が FWSM を経由して確立されるようにする必要があります。これは、FWSM に接続された両方の MPLS ルータが、LDP または TDP セッションの ルータ ID として FWSM インターフェイスの IP アドレスを使用するように設定することによって行います（LDP および TDP によって、MPLS ルータはパケット転送用ラベル（アドレス）をネゴシエートできます）。

Cisco IOS ルータで、使用しているプロトコル（LDP または TDP）に応じたコマンドを入力します。*interface* は、FWSM に接続されたインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

アクセス ルールの設定

Access Rules ウィンドウには、ルールで表現されたネットワーク全体のセキュリティ ポリシーが表示されます。

Access Rules オプションを選択するとき、このウィンドウでは、使用可能なプロトコルやポートなど、特定ホストまたはネットワークによる別のホストまたはネットワークへのアクセスを制御するアクセスリストを定義できます。

テーブル セルをダブルクリックして（またはクリックして F2 を押す）、カラムの内容を編集できます。入力を開始すると、ASDM はドロップダウンに一致する可能性のあるものを表示します。また、サイド ペインから選択したアクセス ルールの送信元または宛先に追加するネットワーク オブジェクトおよびグループをドラッグすることもできます。

アクセス ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

フィールド

注 : カーソルをカラムの線に重ねて二重矢印になったら、その矢印を動かしてテーブル カラムの幅を調整できます。カラムの線をクリックして希望のサイズにドラッグします。

- Add : 新しいアクセス ルールを追加します。
- Edit : アクセス ルールを編集します。
- Delete : アクセス ルールを削除します。
- Move Up : ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複するルールがあると順序によって評価が異なります。
- Move Down : ルールを下に移動します。
- Cut : ルールを切り取ります。
- Copy : ルールのパラメータをコピーし、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。
- Paste : コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。
- Find : 表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter ドロップダウン リスト : フィルタリングする基準を、Interface、Source、Destination、Source or Destination、Destination Service、または Rule Query のいずれかから選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用できます。
  - Condition ドロップダウン リスト : 基準の Source、Destination、Source or Destination、および Destination Service に対して、**is** または **contains** のいずれかの条件を選択します。**is** は完全一致を意味します。Source/Destination の場合、**contains** は、指定したアドレスが含まれるネットワークに一致します。また、サービス タイプの場合は、指定したサービスが含まれるネットワークに一致します。たとえば、10.1.1.1/32 は 10.1.1.1 を含むため、10.1.1.0/24 や 10.0.0.0/8 または「any」に一致します。tcp port 80 は、「tcp」または「any」に一致します。これは、両方とも tcp port 80 を含むためです。
  - Filter フィールド : Interface タイプの場合は、このフィールドがドロップダウン リストになります。リストからインターフェイス名を選択できます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開いてアドレスを参照します。Destination Service タイプとしては、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリッ

クして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。Filter フィールドは、カンマまたはスペースで区切って、複数のエントリを受け入れます。また、ワイルドカードも受け入れます。

  - Filter：フィルタリングを実行します。
  - Clear：一致内容および表示内容をすべてクリアします。
  - Define Query：このボタンは、Flter ドロップダウン リストから Query を選択したときに表示されます。

- Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図には、ネットワーク、トラフィックのタイプ、インターフェイス名、フロー方向、およびアクションが表示されます。
- Export：ファイルをカンマ区切り値または HTML 形式のいずれかでエクスポートします。
- Show：Real-Time Log Viewer に、選択したアクセス ルールによって生成された syslog を表示します。

次の説明では、Access Rules テーブルのカラムをまとめています。ルールは、実行順に表示されます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- No：ルールの評価順序を示します。
- Enabled：ルールがイネーブルかディセーブルかを示します。
- Source：Destination Type フィールドで指定された宛先へのトラフィックが許可または拒否される IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（inside: any など）。これは、内部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。
- Destination：Source Type フィールドで指定した送信元からのトラフィックを許可または拒否する IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。アドレス カラムには、単語 any が付いたインターフェイス名が含まれることがあります（outside: any など）。これは、外部インターフェイスのすべてのホストが、このルールの影響を受けるという意味です。また、詳細モードでは、アドレス カラムに角カッコで囲まれた IP アドレスが含まれることもあります（[209.165.201.1-209.165.201.30] など）。これらのアドレスは、変換済みアドレスです。内部ホストが外部ホストへの接続を作成すると、ファイアウォールは内部ホストのアドレスをプールのアドレスにマッピングします。ホストが発信接続を作成した後、ファイアウォールはこのアドレス マッピングを維持します。アドレス マッピング構造は xlate と呼ばれ、一定の時間、メモリに保持されます。アクセス ルールで許可されていれば、この時間内に、外部ホストはプールの変換済みアドレスを使用して、内部ホストへの接続を開始できます。通常、内部ホストは常に同じ IP アドレスを使用するので、外部から内部への接続にはスタティック変換が必要です。
- Service：ルールで指定されるサービスまたはプロトコルを示します。
- Action：ルールに適用されるアクションです（Permit または Deny）。
- Hits：ルールのヒット数を示します。このカラムは、Preferences ダイアログボックスの頻度設定に応じて、ダイナミックにアップデートされます。ヒット数は、明示的なルールにのみ適用されます。Access Rules テーブルには、暗黙のルールのヒット数は表示されません。
- Logging：アクセス ルールのロギングをイネーブルにしている場合、このカラムには、ロギング レベル、およびログ メッセージ間の間隔が秒数で表示されます。
- **Time：**ルールを適用する時間範囲が表示されます。
- Description：ルールを追加したときに入力した説明が表示されます。暗黙のルールには、「Implicit outbound rule.」という説明が付けられます。
- Addresses：IP 名またはネットワーク オブジェクト グループを追加、編集、削除、または検索できるタブです。IP アドレス オブジェクトは、その後のルール作成で簡単に選択できるように、ルール作成の間、送信元エントリおよび宛先エントリに基づいて自動的に作成されます。手動では追加、編集、または削除できません。

- Services：サービスを追加、編集、削除、または検索できるタブです。
- Time Ranges：時間範囲を追加、編集、または削除できるタブです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Define Query

Define Query ダイアログボックスでは、ルールを検索するときに Filter フィールドで使用できる名前付きルール クエリーを追加または編集できます。

フィールド

- Name：ルール クエリーの名前を入力します。
- Description：ルール クエリーの説明を入力します。
- Match Criteria：この領域には、フィルタリングのための基準が一覧表示されます。
  - any of the following criteria：一覧表示された任意の基準に一致するようにルール クエリーを設定します。
  - all of the following criteria：一覧表示されたすべての基準に一致するようにルール クエリーを設定します。
  - Field：基準のタイプを一覧表示します。インターフェイスまたは送信元などです。
  - Value：「inside」など、基準の値を一覧表示します。
  - Remove：選択した基準を削除します。
- Define New Criteria：この領域では、新しい基準を定義して、照合基準に追加します。
  - Field：ルール クエリーにネストされる Interface、Source、Destination、Service、Action、または他の Rule Query などの基準のタイプを選択します。
  - Value：検索する値を入力します。Interface タイプの場合、このフィールドはドロップダウン リストになり、インターフェイス名を選択できます。Action タイプの場合、ドロップダウン リストには Permit と Deny が表示されます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開いてアドレスを参照します。Service タイプには、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリックして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。
  - Add：Match Criteria テーブルに基準を追加します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Access Rule

Add/Edit Access Rule ダイアログボックスでは、新しいルールの作成、または既存のルールの変更が実行できます。

アクセス ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

フィールド

- Interface：ルールを適用するインターフェイスを指定します。
- Action：新しいルールのアクション タイプを決めます。Permit または Deny のいずれかを選択します。
  - Permit：すべての一致したトラフィックを許可します。
  - Deny：すべての一致したトラフィックを拒否します。
- Source：Destination フィールドで指定された宛先へのトラフィックが許可または拒否される IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  ...：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはすべてを選択、追加、編集、削除、または検索できます。
- Destination：Source Type フィールドで指定した送信元からのトラフィックを許可または拒否する IP アドレス、ネットワーク オブジェクト グループ、インターフェイス IP、または any を指定します。

  ...：既存の IP アドレス オブジェクト、IP 名、ネットワーク オブジェクト グループ、またはすべてを選択、追加、編集、削除、または検索できます。
- Service：サービスのリストから、ポート番号、ポート範囲、またはウェルノウン サービス名またはグループを指定するには、このオプションを選択します。

  ...：事前に設定されたリストから既存のサービスを選択、追加、編集、削除または検索できます。
- Description：（オプション）アクセス ルールの説明を入力します。
- Enable Logging：アクセス ルールのロギングをイネーブルにします。
  - Logging Level：default、emergencies、alerts、critical、errors、warnings、notifications、informational、または debugging を指定します。
- More Options：ルールの追加の設定オプションが表示されます。
  - Enable Rule：ルールをイネーブルまたはディセーブルにします。
  - Traffic Direction：どちらの方向のトラフィックにルールを適用するかを決定します。オプションは incoming または outgoing のいずれかです。
  - Source Service：送信元のプロトコルおよびサービスを指定します（TCP または UDP サービスのみ）。

    ...：事前に設定されたリストから送信元サービスを選択、追加、編集、削除または検索できます。
  - Logging Interval：ロギングが設定されている場合、ロギングの間隔を秒数で指定します。
  - Time Range：このルールに定義されている時間範囲をドロップダウン リストから指定します。

    ...：事前に設定されたリストから時間範囲を選択、追加、編集、削除または検索できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Service Groups

Manage Service Groups ダイアログボックスでは、名前付きグループにある複数の TCP、UDP、または TCP-UDP サービス（ポート）を関連付けます。以後、アクセスや、IPSec ルール、コンジットなどの ASDM および CLI 内の機能でサービス グループを使用できます。

用語のサービスは、ウェルノウン ポート番号と「リテラル」名（ftp、telnet、smtp など）を持つ、アプリケーション レベル サービスと関連付けられた上位レイヤ プロトコルを指します。

FWSM は、次の TCP リテラル名を許可します。

bgp、chargen、cmd、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、ident、irc、klogin、kshell、lpd、nntp、pop2、pop3、pptp、smtp、sqlnet、sunrpc、tacacs、talk、telnet、time、uucp、whois、www。

サービス グループの名前は、オブジェクト グループの 4 つすべてのタイプで、一意である必要があります。たとえば、サービス グループとネットワーク グループで、同じ名前を共有することはできません。

複数のサービス グループを「グループのグループ」にネストして、単一グループとして使用できます。サービス オブジェクト グループを削除すると、使用されているすべてのサービス オブジェクト グループから削除されます。

アクセス ルールで使用しているサービス グループは、削除しないでください。アクセス ルールで使用されているサービス グループを空にすることはできません。

フィールド

- TCP : TCP サービスまたはポート番号をオブジェクト グループに追加するには、このオプションを選択します。
- UDP : UDP サービスまたはポート番号をオブジェクト グループに追加するには、このオプションを選択します。
- TCP-UDP : TCP および UDP に共通のサービスまたはポート番号をオブジェクト グループに追加するには、このオプションを選択します。
- Service Group table : このテーブルには、各サービス オブジェクト グループの記述名を含みます。このリストのグループを変更または削除するには、グループを選択して **Edit** または **Delete** をクリックします。新しいグループをこのリストに追加するには、**Add** をクリックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Service Group

Add/Edit Service Group ダイアログボックスでは、TCP および UDP サービスまたはポートのグループを管理できます。

フィールド

- Service Group Name：サービス グループの名前を指定します。重複するオブジェクト グループ名は指定できません。サービス グループ名はネットワーク グループと名前を共有できません。
- Description：サービス グループの説明を指定します。
- Service：事前に定義されたドロップダウン リストからサービス グループのサービスを選択できます。
- Range/Port #：サービス グループのポートの範囲を指定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Advanced Access Rule Configuration

Advanced Access Rule Configuration ダイアログボックスでは、グローバル アクセス ルールのロギング オプションを設定できます。

ロギングがイネーブルで、パケットがアクセス ルールと一致した場合、FWSM はフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します（「ログ オプション」を参照）。FWSM は、最初のヒットがあったとき、および各間隔の終わりにシステム ログ メッセージを生成し、その間隔におけるヒットの合計数を示します。各間隔の終わりに、FWSM はヒット数を 0 にリセットします。1 つの間隔内でアクセス ルールと一致するパケットがなかった場合、FWSM はそのフロー エントリを削除します。

どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU リソースが無制限に消費されないようにするために、FWSM は同時拒否フロー数に制限を設定します。この制限は、拒否フローに対してのみ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、FWSM は既存の拒否フローが期限切れになるまで新しい拒否フローを作成しません。DoS 攻撃（サービス拒絶攻撃）が開始された場合、FWSM は非常に大量の拒否フローをごく短時間のうちに作成する可能性があります。拒否フロー数を制限することにより、メモリおよび CPU リソースが無制限に消費されないようにします。

アクセス ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

前提条件

アクセス ルールのアクセス コントロール エントリ（ルールとも呼ばれます）に対して、さらに新しいロギング メカニズムをイネーブルにする場合にのみ、この設定が適用されます。詳細については、「Log Options」を参照してください。

フィールド

- Maximum Deny-flows：FWSM がロギングを停止する前に許可される拒否フローの最大数で、1 とデフォルト値の間です。デフォルトは 4096 です。
- Alert Interval：拒否フローの最大数に達したことを識別するシステム ログ メッセージ（番号 106101）の間の時間（1 ～ 3600 秒）です。デフォルトは 300 秒です。
- Per User Override table：ユーザごとの上書き機能の状態を指定します。着信アクセス ルールでユーザごとの上書き機能がイネーブルになっている場合、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルールに置き換えられます。ユーザごとの上書き機能がディセーブルになっている場合、RADIUS サーバによって提供されるアクセス ルールは、そのインターフェイス上で設定されたアクセス ルールに結合されます。インターフェイスに着信アクセス ルールが設定されていない場合、ユーザごとの上書きは設定できません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Log Options

Log Options ダイアログボックスでは、各アクセス ルールのロギング オプションを設定できます。グローバル ロギング オプションの設定については、P.17-15 の「Advanced Access Rule Configuration」を参照してください。

このダイアログボックスでは、旧式のロギング メカニズム（拒否されたトラフィックだけが記録される）を使用したり、新しいロギング メカニズム（許可および拒否されたトラフィックがパケットのヒット数などの追加情報と共に記録される）を使用したり、ロギングをディセーブルにしたりできます。

Log オプションをイネーブルにすると、一定量のメモリを消費します。潜在的な DoS 攻撃のリスクを制御するには、Access Rules ウィンドウの **Advanced** を選択して、Maximum Deny-flow 設定を実行すると役立ちます。

フィールド

- Use default logging behavior：旧式のアクセス ルール ロギング メカニズムを使用します。FWSM は、パケットが拒否されるとシステム ログ メッセージ番号 106023 を記録します。デフォルト設定に戻すには、このオプションを選択します。
- Enable logging for the rule：新しいアクセス ルール ロギング メカニズムをイネーブルにします。FWSM は、パケットがアクセス ルール（許可または拒否のいずれか）に一致したとき、システム ログ メッセージ番号 106100 を記録します。

  パケットがアクセス ルールと一致した場合、FWSM はフロー エントリを作成して、指定された間隔で受信したパケットの数を追跡します（Logging Interval フィールドを参照）。FWSM は、最初のヒットがあったとき、および各間隔の終わりにシステム ログ メッセージを生成し、その間隔におけるヒットの合計数を示します。各間隔の終わりに、FWSM はヒット数を 0 にリセットします。1 つの間隔内でアクセス ルールと一致するパケットがなかった場合、FWSM はそのフロー エントリを削除します。

- Logging Level：syslog サーバに送信されるロギング メッセージのレベルをドロップダウン リストから選択します。レベルは次のように定義されています。

  Emergencies（レベル 0）：FWSM では、このレベルは使用しません。

  Alert（レベル 1、即時対処が必要）

  Critical（レベル 2、クリティカル条件）

  Error（レベル 3、エラー条件）

  Warning（レベル 4、警告条件）

  Notification（レベル 5、正常だが顕著な条件）

  Informational（レベル 6、情報メッセージのみ）

  Debugging（レベル 7、デバッグ中のみ表示）

- Logging Interval : FWSM がフロー統計情報を syslog に送信する前に待機する時間を秒数（1 ～ 600 秒）で設定します。この設定は、アクセス ルールと一致するパケットがない場合にフローを削除するタイムアウト値としても機能します。デフォルトは 300 秒です。

- Disable logging for the rule：アクセス ルールのすべてのロギングをディセーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

EtherType ルールの設定（透過モードのみ）

EtherType Rules ウィンドウには、パケット EtherType に基づくアクセス ルールが表示されます。EtherType ルールは、透過モードで動作するときに FWSM で非 IP 関連トラフィック ポリシーを設定するのに使用されます。透過モードでは、拡張アクセス ルールと EtherType アクセス ルールの両方をインターフェイスに適用できます。EtherType ルールは、拡張アクセス ルールに優先されます。

EtherType ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

フィールド

- Add：新しい EtherType ルールを追加します。ドロップダウン リストから、追加するルールのタイプを選択します。
- Edit：EtherType ルールを編集します。
- Delete：EtherType ルールを削除します。
- Move Up：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複するルールがあると順序によって評価が異なります。
- Move Down：ルールを下に移動します。
- Cut：ルールを切り取ります。
- Copy：ルールのパラメータをコピーし、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。
- Paste：コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。

次の説明では、EtherType Rules テーブルのカラムをまとめています。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- No：ルールの評価順序を示します。
- Action：このルールの Permit または Deny アクションです。
- Ethervalue：EtherType 値で、IPX、BPDU、MPLS-Unicast、MPLS-Multicast、または 16 ビットの 16 進数値 0x600（1536）～ 0xffff のいずれかとなります。この値により EtherType が識別されます。
- Interface：ルールが適用されるインターフェイスです。
- Direction Applied：このルールの方向で、着信トラフィックまたは発信トラフィックです。
- Description：テキストによるルールの説明で、オプションです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Add/Edit EtherType Rule

Add/Edit EtherType Rules ダイアログボックスでは、EtherType ルールを追加または編集できます。

EtherType ルールの詳細については、P.17-2 の「アクセス ルールと EtherType ルールの概要」を参照してください。

フィールド

- Action：このルールの Permit または Deny アクションです。
- Interface：このルールのインターフェイス名です。
- Apply rule to：このルールの方向で、着信トラフィックまたは発信トラフィックです。
- Ethervalue：EtherType 値で、BPDU、IPX、MPLS-Unicast、MPLS-Multicast、any（0x600 ～ 0xffff の間の任意の値）、または 16 ビットの 16 進数値 0x600（1536）～ 0xffff のいずれかとなります。この値により EtherType が識別されます。
- Description：テキストによるルールの説明で、オプションです。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—