CHAPTER 5

IPv4 および IPv6 のアクセス コントロール リストの設定

Cisco MDS 9000 ファミリ スイッチ製品は、イーサネットとファイバ チャネル インターフェイスの間で IP バージョン 4（IPv4）トラフィックをルーティングできます。IP スタティック ルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリ スイッチは、ネットワーク管理システム（NMS）に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス（mgmt0）での IP 転送
- IP over Fibre Channel（IPFC）機能を使用したインバンド ファイバ チャネル インターフェイス上の IP 転送：IPFC は、IP フレームをカプセル化手法を利用してファイバ チャネル上で転送するための方法を定義しています。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング（デフォルト ルーティングおよびスタティック ルーティング）：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

スイッチは仮想ルータ冗長プロトコル（VRRP）機能の RFC 2338 標準に準拠します。VRRP は、冗長な代替パスをゲートウェイ スイッチに提供する、再起動可能なアプリケーションです。

IPv4 Access Control List（IPv4-ACL および IPv6-ACL）は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

この章では、次の事項について説明します。

IPv4 および IPv6 のアクセス コントロール リストの概要

Cisco MDS 9000 ファミリ スイッチ製品は、イーサネットとファイバ チャネル インターフェイスの間で IP バージョン 4（IPv4）トラフィックをルーティングできます。IP スタティック ルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリ スイッチは、ネットワーク管理システム（NMS）に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス（mgmt0）での IP 転送
- IP over Fibre Channel（IPFC）機能を使用したインバンド ファイバ チャネル インターフェイス上の IP 転送：IPFC は、IP フレームをカプセル化手法を利用してファイバ チャネル上で転送するための方法を定義しています。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング（デフォルト ルーティングおよびスタティック ルーティング）：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

IPv4 Access Control List（IPv4-ACL および IPv6-ACL）は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

ここでは、次の内容について説明します。

フィルタの内容について

IP フィルタには、プロトコル、アドレス、ポート、ICMP タイプ、およびサービス タイプ（ToS）に基づく IP パケットの一致規則が含まれます。

プロトコル情報

各フィルタには、プロトコル情報が必要です。この情報により、IP プロトコルの名前または番号を識別します。IP プロトコルは、次のいずれかの方法で指定できます。

- 0 ～ 255 の整数を指定します。この番号は IP プロトコルを表します。

- プロトコルの名前を指定しますが、Internet Protocol（IP）、伝送制御プロトコル（TCP）、User Datagram Protocol（UDP）、および Internet Control Message Protocol（ICMP）には限定されません。

（注）　ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL を設定する場合は、TCP または ICMP オプションだけを使用してください。

アドレス情報

各フィルタには、アドレス情報が必要です。アドレス情報により、次の詳細を識別します。

- 送信元：パケット送信元のネットワークまたはホストのアドレス
- 送信元ワイルドカード：送信元に適用されるワイルドカード ビット
- 宛先：パケットの送信先となるネットワークまたはホストの番号
- 宛先ワイルドカード：宛先に適用されるワイルドカード ビット

送信元/送信元ワイルドカードおよび宛先/宛先ワイルドカードは、次のいずれかの方法で指定します。

- 4 つに区切られたドット付き 10 進表記の 32 ビット数を使用します（10.1.1.2/0.0.0.0 はホスト 10.1.1.2 と同じ）。
  - 各ワイルドカード ビットをゼロに設定する場合には、パケットの IPv4 アドレス内の対応するビット位置と送信元の対応するビット位置で、ビット値が正確に一致している必要があります。
  - 各ワイルドカード ビットを 1 に設定する場合は、パケットの IPv4 または IPv6 アドレス内の対応する位置のビット値が 0 および 1 のいずれであっても、現在のアクセス リスト エントリと一致すると見なされます。無視するビット位置に 1 を入れます。たとえば、0.0.255.255 の場合、送信元の最初の 16 ビットだけが完全に一致する必要があります。複数のワイルドカード ビットを 1 に設定する場合、これらのビットが送信元ワイルドカード内で連続している必要はありません。たとえば、送信元ワイルドカード 0.255.0.64 は有効です。
- 送信元/送信元ワイルドカードまたは宛先/宛先ワイルドカード（0.0.0.0/255.255.255.255）の短縮形として、**any** オプションを使用します。

ポート情報

ポート情報はオプションです。送信元ポートと宛先ポートを比較するためには、**eq**（等号）オプション、**gt**（より大きい）オプション、**lt**（より小さい）オプション、または **range**（ポート範囲）オプションを使用します。ポート情報は次のいずれかの方法で指定できます。

- ポート番号を指定します。ポート番号の範囲は 0 ～ 65535 です。表 5-1 に、関連 TCP ポートおよび UDP ポートについて、Cisco NX-OS ソフトウェアが認識するポート番号を示します。
- TCP または UDP ポートの名前を次のように指定します。
  - TCP ポート名は、TCP をフィルタリングする場合にかぎって使用できます。
  - UDP ポート名は、UDP をフィルタリングする場合にかぎって使用できます。

表 5-1　TCP および UDP のポート番号

プロトコル	ポート	番号
UDP	dns	53
	tftp	69
	ntp	123
	radius アカウンティング	1646 または 1813
	radius 認証	1645 または 1812
	snmp	161
	snmp-trap	162
	syslog	514
TCP[1]	ftp	20
	ftp-data	21
	ssh	22
	telnet	23
	smtp	25
	tasacs-ds	65
	www	80
	sftp	115
	http	143
	wbem-http	5988
	wbem-https	5989

1. TCP コネクションが確立済みの場合は、**established** オプションを使用して適合するものを探してください。TCP データグラムが ACK、FIN、PSH、RST または URG のコントロール ビット セットを持つ場合は、適合と見なされます。

ICMP 情報

オプションとして IP パケットは次の ICMP 条件に基づいて選別できます。

- icmp-type：ICMP メッセージ タイプは 0 から 255 の番号から 1 つ選びます。
- icmp-code：ICMP メッセージ コードは 0 から 255 の番号から 1 つ選びます。

表 5-2 に各 ICMP タイプの値を示します。

表 5-2　ICMP タイプの値

ICMP タイプ[1]	コード
echo	8
echo-reply	0
destination unreachable	3
traceroute	30
time exceeded	11

1. ICMP リダイレクト パケットは必ず拒否されます。

ToS 情報

オプションとして IP パケットは次の ToS 条件に基づいて選別できます。

- ToS レベル：レベルは 0 から 15 の番号で指定します。
- ToS 名：max-reliability、max-throughput、min-delay、min-monetary-cost、および normal から選択できます。

注意事項と制限

Cisco MDS 9000 ファミリのスイッチまたはディレクタに IPv4-ACL または IPv6-ACL を設定する場合は、次の注意事項に従ってください。

- IPv4-ACL または IPv6-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。

ヒント ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL がすでに設定されている場合は、このインターフェイスをイーサネット ポートチャネル グループに追加できません。IPv4-ACL の設定に関する注意事項については、『*IP Services Configuration Guide, Cisco DCNM for SAN*』を参照してください。

注意 IPv4-ACL または IPv6-ACL は、ポートチャネル グループ内の 1 つのメンバーだけに適用しないでください。IPv4-ACL または IPv6-ACL はチャネル グループ全体に適用します。

- 条件の順序は正確に設定してください。IPv4-ACL または IPv6-ACL フィルタは IP フローに順番に適用されるので、最初の一致によって動作が決定されます。以降の一致は考慮されません。最も重要な条件を最初に設定してください。いずれの条件とも一致しなかった場合、パケットは廃棄されます。
- IP ACL を適用する IP ストレージのギガビット イーサネット ポートでは、暗黙的な deny は有効にならないため、明示的な deny を設定してください。

IPv4-ACL または IPv6-ACL の設定

ここでは、次の内容について説明します。

IP-ACL Wizard を使用した IPv4-ACL または IPv6-ACL の作成

スイッチに入ったトラフィックは、スイッチ内でフィルタが現れる順番に従って IPv4-ACL または IPv6-ACL のフィルタと比較されます。新しいフィルタは IPv4-ACL または IPv6-ACL の末尾に追加されます。スイッチは合致するまで照合を続けます。フィルタの最後に達して合致するものがなかった場合、そのトラフィックは拒否されます。そのため、フィルタの最上部にはヒットする確率の高いフィルタを置く必要があります。許可されないトラフィックに対して、*implied deny* が用意されています。1 つの拒否エントリしか持たないシングルエントリの IPv4-ACL または IPv6-ACL には、すべてのトラフィックを拒否する効果があります。

手順の詳細

IPv4-ACL または IPv6-ACL を設定する手順は次のとおりです。

ステップ 1　IPv4-ACL または IPv6-ACL の作成には、フィルタ名と 1 つ以上のアクセス条件を指定します。フィルタには、条件に合致する発信元と宛先のアドレスが必要です。適切な粒度を設定するために、オプションのキーワードを使用できます。

（注）　フィルタのエントリは順番に実行されます。エントリは、リストの最後にだけ追加できます。正しい順番でエントリを追加するように注意してください。

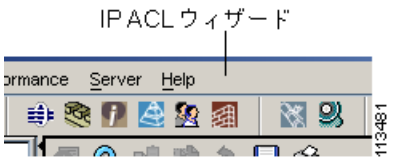
ステップ 2　指定したインターフェイスにアクセス フィルタを適用します。

IPv4-ACL Wizard を使用して、IPv4-ACL または IPv6-ACL の名前付きプロファイルの中に順番に並べた IP フィルタのリストを作成する手順は、次のとおりです。

手順の詳細

ステップ 1　DCNM-SAN ツールバーで **IP ACL Wizard** アイコンをクリックします（図 5-1 を参照）。

図 5-1　IP ACL Wizard



IP ACL Wizard が表示されます。

ステップ 2　IP-ACL の名前を入力します。

（注）　IPv6-ACL を作成する場合は IPv6 チェックボックスにチェックを入れます。

ステップ 3　[Add] をクリックし、この IP-ACL に新しいルールを追加します。テーブルに新しい規則とデフォルト値が表示されます。

ステップ 4　必要に応じて、フィルタ送信元 IP および送信元マスクを修正します。

（注）　IP-ACL Wizard で作成できるのは、着信 IP フィルタだけです。

ステップ 5　[Application] ドロップダウン リストで、適切なフィルタ タイプを選択します。

ステップ 6　[Action] ドロップダウン リストで [permit] または [deny] を選択します。

ステップ 7　追加する IP フィルタに対して、ステップ 3 ～ステップ 6 を繰り返します。

ステップ 8　[Up] または [Down] をクリックして、IP-ACL フィルタの順序を決定します。

ヒント　IP フィルタの順序は慎重に決定してください。トラフィックは、指定された順序で IP フィルタと比較されます。最初の一致が適用され、以降のフィルタは無視されます。

ステップ 9　[Next] をクリックします。

この IP-ACL を適用できるスイッチのリストが表示されます。

ステップ 10　この IP-ACL を適用しないスイッチのチェックボックスをオフにします。

ステップ 11　この IP-ACL を適用する**インターフェイス**を選択します。

ステップ 12　[Finish] をクリックして、この IP-ACL を作成し、選択したスイッチに適用します。

IPv4-ACL または IPv6-ACL の作成

手順の詳細

Device Manager を使用して既存の IPv4-ACL または IPv6-ACL にエントリを追加する手順は次のとおりです。

ステップ 1　[Security] > [IP ACL] を選択します。

ステップ 2　[Create] をクリックして、IP-ACL プロファイルを作成します。

[IP ACL Profiles] ダイアログボックスが表示されます。IP-ACL プロファイルの名前を入力します。

ステップ 3　[Create] をクリックしてから [Close] をクリックします。

新しい IP-ACL プロファイルが作成されます。

ステップ 4　作成した IP-ACL をクリックし、[Rules] をクリックします。

Device Manager を利用している場合は、IPv4-ACL または IPv6-ACL の作成後に、続く IP フィルタを IPv4-ACL または IPv6-ACL の最後に追加できます。DCNM-SAN を利用すると、1 つのプロファイルに対する既存のルールを並び替えることができます。IPv4-ACL または IPv6-ACL の中間にはフィルタを挿入できません。設定された各エントリは、自動的に IPv4-ACL または IPv6-ACL の最後に追加されます。

ステップ 5　[Create] をクリックして、IP フィルタを作成します。

ステップ 6　[Action] に対して [permit] または [deny] のいずれかを選択し、[Protocol] フィールドに IP 番号を設定します。ドロップダウン メニューには、一般的なフィルタリングされたプロトコルが提供されています。

ステップ 7　フィルタを適用する送信元 IP アドレスおよびワイルドカード マスクを設定します。すべての IP アドレスに対してフィルタを適用する場合には、[any] チェックボックスをオンにします。

これにより、フレームの送信元 IP アドレスをチェックする IP フィルタが作成されます。

（注）　ワイルドカード マスクは、照合する IP アドレスのサブネットを示します。これによって、あるアドレス範囲がこのフィルタに照合されます。

ステップ 8　TCP または UDP のプロトコルを選択した場合には、トランスポート層の送信元ポート範囲を設定します。

ステップ 9　宛先 IP アドレスおよびポート範囲について、ステップ 7 ～ステップ 8 を繰り返します。

これにより、フレームの宛先 IP アドレスをチェックする IP フィルタが作成されます。

ステップ 10　必要に応じて、ToS、ICMPType、および ICMPCode フィールドを設定します。

ステップ 11　ACK、FIN、PSH、RST、SYN、または URG 制御ビット セットを含む TCP 接続を一致させる場合には、[TCPEstablished] チェックボックスをオンにします。

ステップ 12　この IP フィルタと一致する全フレームのログを作成する場合には、[LogEnabled] チェックボックスをオンにします。

ステップ 13　[Create] をクリックしてこの IP フィルタを作成し、IP-ACL に追加します。

既存の IPv4-ACL または IPv6-ACL からの IP フィルタの削除

手順の詳細

Device Manager を使用して既存の IPv4-ACL または IPv6-ACL から、設定したエントリを削除する手順は次のとおりです。

ステップ 1　[Security] > [IP ACLs] を選択します。

[IP ACL] ダイアログボックスが表示されます。

ステップ 2　修正する IP-ACL をクリックしてから [Rules] をクリックします。

この IP-ACL に関連する IP フィルタのリストが表示されます。

ステップ 3　削除するフィルタを選択してから [Delete] をクリックしてその IP フィルタを削除します。

IP-ACL の削除

前提条件

IP-ACL を削除する前に、IP-ACL とインターフェイスの関連付けを削除する必要があります。

手順の詳細

IP-ACL を削除するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IP ACL] を選択します。

[Information] ペインに、IP-ACL の設定が表示されます。

ステップ 2　[Profiles] タブをクリックします。

スイッチ、ACL、およびプロファイル名のリストが表示されます。

ステップ 3　削除する行を選択します。複数の行を削除する場合は、Shift キーを押しながら行を選択します。

ステップ 4　[Delete Row] をクリックします。IP-ACL が削除されます。

IP-ACL ログ ダンプの読み取り

このフィルタに合致するパケットに関する情報をログに記録するには、IP フィルタ作成の際に LogEnabled チェックボックスを使用します。ログ出力には ACL の番号、許可または拒否のステータス、およびポート情報が表示されます。

入力 ACL に対しては、ログは無加工の MAC 情報を表示します。キーワード「MAC=」は、MAC アドレス情報を持つイーサネットの MAC フレームの表示は意味しません。ログにダンプされるレイヤ 2 の MAC レイヤ情報を意味します。出力 ACL に対しては、無加工のレイヤ 2 情報はログに記録されません。

入力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:00:08:00:45:00:00:54:00
:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02:01
:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24
:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

出力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.12 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280
```

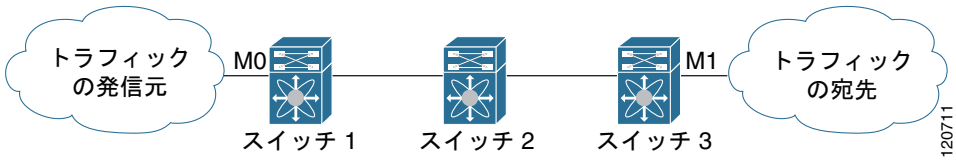
インターフェイスへの IP-ACL の適用

IP-ACL は適用しなくても定義できます。しかし、IP-ACL はスイッチのインターフェイスに適用されるまで効果は出ません。IP-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。

ヒント　トラフィックの送信元に一番近いインターフェイスに IP-ACL を適用してください。

送信元から宛先へ流れるトラフィックを遮断しようとする場合は、スイッチ 3 の M1 に対するアウトバンド フィルタの代わりに、スイッチ 1 の M0 にインバウンド IPv4-ACL を適用できます（図 5-2 を参照）。

図 5-2　インバウンド インターフェイス上のトラフィックの拒否



access-group オプションによりインターフェイスへのアクセスを規制できます。各インターフェイスは、1 つの方向につき 1 つの IP-ACL にしか関連付けできません。入力方向には、出力方向とは異なる IP-ACL を持たせることができます。IP-ACL はインターフェイスに適用されたときにアクティブになります。

ヒント　IP-ACL の中の条件は、インターフェイスに適用する前にすべて作成しておいてください。

注意　IP-ACL を作成前にインターフェイスに適用すると、IP-ACL が空白であるため、そのインターフェイスのすべてのパケットが排除されます。

スイッチにおいては、用語としての*イン*、*アウト*、*送信元*、*宛先*は次の意味になります。

- イン：インターフェイスに到達してスイッチ内を通過するトラフィック。送信元はそのトラフィックが発信された場所で、宛先は送信される先（ルータの反対側で）を意味します。

ヒント　入力トラフィック用インターフェイスに適用された IP-ACL はローカルおよびリモート両方のトラフィックに作用します。

- アウト：スイッチを通過済みで、インターフェイスから離れたトラフィック。送信元はこれが送信された場所であり、宛先は送信先を意味します。

ヒント　出力トラフィック用インターフェイスに適用された IP-ACL はローカル トラフィックにだけ作用します。

mgmt0 への IP-ACL の適用

mgmt0 と呼ばれるシステムのデフォルト ACL は、mgmt0 インターフェイス上に存在します。この ACL はユーザに表示されないため、mgmt0 は、ユーザが使用できない予約された ACL 名です。mgmt0 ACL はほとんどのポートをブロックし、許可されたセキュリティ ポリシーに準拠した必須のポートへのアクセスだけを可能にします。

手順の詳細

インターフェイスに IP-ACL を適用する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IP ACL] を選択します。

[Information] ペインに、IP-ACL の設定が表示されます。

ステップ 2　[Interfaces] タブをクリックします。

インターフェイスおよび関連 IP-ACL のリストが表示されます。

ステップ 3　[Create Row] をクリックします。

ステップ 4　（任意）IP-ACL に含めないスイッチを削除する場合は、スイッチ アドレス横のチェックボックスをオフにします。

IPv4-ACL または IPv6-ACL に関連付けたい**インターフェイス**を [Interface] フィールドで設定します。

ステップ 5　[ProfileDirection] を選択します（[inbound] または [outbound] のいずれか）。

ステップ 6　[Profile Name] フィールドに IP-ACL の名前を入力します。

（注）　この IP-ACL 名は、すでに [Create Profiles] ダイアログボックスを使用して作成済みでなければなりません。作成されていない場合、[Create Profiles] ダイアログボックスを開いてプロファイルを作成するまで、どのフィルタもイネーブルになりません。

ステップ 7　[Create] をクリックして IP-ACL を関連付けます。

新しく関連付けたアクセス リストが IP-ACL のリストの中に表示されます。

IP-ACL の設定例

Device Manager を使用して、管理アクセスを規制する IP-ACL を定義する手順は次のとおりです。

ステップ 1　[Security] > [IP ACL] を選択します。

[IP ACL] ダイアログボックスが表示されます。

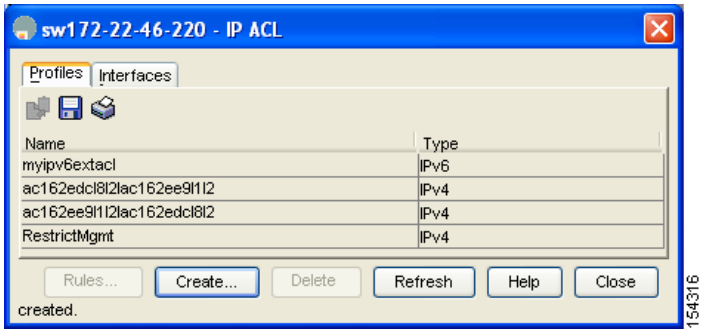
ステップ 2　[Create] をクリックして IP-ACL を 1 つ作成します。

[IP ACL Profiles] ダイアログボックスが表示されます。

ステップ 3　プロファイル名として **RestrictMgmt** と入力してから [Create] をクリックします。

RestrictMgmt という名前が付いた空の IP-ACL が作成されます（図 5-3 を参照）。

図 5-3　リストに追加された RestrictMgmt プロファイル



ステップ 4　**RestrictMgmt** を選択してから [Rules] をクリックします。

この IP-ACL に関連する IP フィルタの空のリストが表示されます。

ステップ 5　[Create] をクリックして最初の IP フィルタを作成します。

[Create IP Filter] ダイアログボックスが表示されます。

ステップ 6　信頼できるサブネットからの管理コミュニケーションを許すための IP フィルタを作成します。

a. [permit] アクションを選択して、[Protocol] ドロップダウン メニューで [0 IP] を選択します。

b. 送信元 IP アドレスを 10.67.16.0 に、ワイルドカード マスクを 0.0.0.255 に設定します。

（注） ワイルドカード マスクは、照合する IP アドレスのサブネットを示します。これによって、あるアドレス範囲がこのフィルタに照合されます。

c. 宛先アドレスとして [any] チェックボックスをオンにします。

d. [Create] をクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

ステップ a からステップ d までの繰り返して、10.67.16.0/24 サブネットのすべてのアドレスに通信を許可する IP フィルタを作成します。

ステップ 7　ICMP ping コマンドを許可するフィルタを次の手順で作成します。

a. [permit] アクションを選択して、[Protocol] ドロップダウン メニューで [1 ICMP] を選択します。

b. 送信元アドレスとして [any] チェックボックスをオンにします。

c. 宛先アドレスとして [any] チェックボックスをオンにします。

d. [ICMPType] ドロップダウン メニューで [8 echo] を選択します。

e. [Create] をクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

ステップ a からステップ e までを繰り返して、ICMP ping を許可する IP フィルタを作成します。

ステップ 8　他のすべてのトラフィックを遮断する最後の IP フィルタを次の手順で作成します。

a. [deny] アクションを選択して、[Protocol] ドロップダウン メニューで [0 IP] を選択します。

b. 送信元アドレスとして [any] チェックボックスをオンにします。

c. 宛先アドレスとして [any] チェックボックスをオンにします。

d. [Create] をクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

e. [Close] をクリックして、[Create IP Filter] ダイアログボックスを閉じます。

ステップ a からステップ d までを繰り返して、他のすべてのトラフィックを遮断する IP フィルタを作成します。

ステップ 9　次の手順で mgmt0 インターフェイスに RestrictMgmt IP ACL を適用します。

a. [Security] をクリックし､[IP ACL] を選択してから [IP ACL] ダイアログボックスで [Interfaces] タブをクリックします。

b. [Create] をクリックします。

[Create IP-ACL Interfaces] ダイアログボックスが表示されます。

c. [Interfaces] ドロップダウン メニューで [mgmt0] を選択します。

d. [ProfileDirection] から [inbound] を選択します。

e. [ProfileName] ドロップダウン メニューで [RestrictMgmt] を選択します。

f. [Create] をクリックして RestrictMgmt IP-ACL を mgmt0 インターフェイスに適用します。

ステップ a からステップ f までを繰り返して、新しい IP-ACL を mgmt0 インターフェイスに適用します。

IPv4 および IPv6 のアクセス コントロール リストのフィールドの説明

ここでは、IPv4 および IPv6 のアクセス コントロール リストのフィールドについて説明します。

IP ACL プロファイル

フィールド	説明
Name	固有の IP プロトコル フィルタ プロファイル識別子です。
Type	このオブジェクトは、このフィルタ プロファイルの使用タイプを決定します。この使用タイプは、プロファイルの作成後には変更できません。

IP ACL インターフェイス

フィールド	説明
ProfileName	固有の IP プロトコル フィルタ プロファイル識別子です。

IP フィルタ プロファイル

フィールド	説明
Action	deny に設定すると、このフィルタに一致するすべてのフレームが廃棄され、フィルタ リスト残りの部分のスキャンが中止されます。permit に設定すると、後続のブリッジングまたはルーティング処理に対して、このフィルタに一致するすべてのフレームが許可されます。
Protocol	このフィルタ プロトコル値は、フレーム内のインターネット プロトコル番号と照合されます。これらの IP 番号は、Network Working Group の Request for Comments（RFC）ドキュメントで定義されています。これを「-1」に設定すると、フィルタリングで任意の IP 番号が一致します。
Address	このフィルタで照合される送信元 IP アドレス。0 を設定すると、すべての送信元アドレスが一致します。
Mask	一致する必要がある SrcAddress ビットに対するワイルドカード マスクです。このマスクの 0 ビットは、照合に成功するために一致する必要がある SrcAddress の対応するビットを示します。1 ビットは、照合に無関係のビットです。0 を設定すると、SrcAddress と同じ送信元アドレスの IP フレームだけが一致します。
PortLow	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の送信元ポート範囲の下限を指定します。それ以外の場合は、照合中に無視されます。この値は、この SrcPortHigh のエントリに指定した値以下である必要があります。

フィールド	説明
PortHigh	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の送信元ポート範囲の上限を指定します。それ以外の場合は、照合中に無視されます。この値は、この SrcPortLow のエントリに指定した値以上である必要があります。この値が「0」の場合は、照合中に UDP または TCP ポート番号が無視されます。
Address	このフィルタで照合される宛先 IP アドレス。0 を設定すると、すべての送信元アドレスが一致します。
Mask	一致させる必要がある DestAddress ビットに対するワイルドカード マスクです。このマスクの 0 ビットは、照合に成功するために一致する必要がある DestAddress の対応するビットを示します。1 ビットは、照合に無関係のビットです。0 を設定すると、SrcAddress と同じ送信元アドレスの IP フレームだけが一致します。
PortLow	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の宛先ポート範囲の下限を指定します。それ以外の場合は、照合中に無視されます。この値は、PortHigh でこのエントリに指定した値以下である必要があります。
PortHigh	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の宛先ポート範囲の上限を指定します。それ以外の場合は、照合中に無視されます。この値は、この DestPortLow のエントリに指定した値以上である必要があります。この値が「0」の場合は、照合中に UDP または TCP ポート番号が無視されます。
Precedence	各フレーム内の IP トラフィックの優先度パラメータは、特定のネットワークを通じてデータグラムを送信するときに、実際のサービス パラメータの選択を案内するために使用されます。ほとんどのネットワークは、高い優先度のトラフィックを他のトラフィックよりも重要なものとして扱います。IP Precedence 値の範囲は「0」～「7」ですが、「7」が最も優先度が高く、「0」が最も優先度が低くなります。値「-1」は、任意の IP precedence のフレームと一致することを意味します。つまり、この値が「-1」の場合、IP precedence パラメータはチェックされません。優先レベルは次のとおりです。 • routine(0)：ルーティング トラフィックの優先度 • priority(1)：プライオリティ トラフィックの優先度 • immediate(2)：即時トラフィックの優先度 • flash(3)：フラッシュ トラフィックの優先度 • flashOverride(4)：フラッシュ オーバーライド トラフィックの優先度 • critical(5)：クリティカルな優先度 • internet(6)：インターネットワーク制御トラフィックの優先度 • network(7)：ネットワーク制御トラフィックの優先度
TOS	フレームのサービス タイプ（ToS）。TOS 値の範囲は「0」～「15」です。値「-1」は、任意の TOS 値と一致します。
ICMPType	このフィルタは、照合される ICMP メッセージを指定します。この値を「-1」に設定すると、フィルタリングで任意の ICMP メッセージ タイプが一致します。

フィールド	説明
ICMPCode	このフィルタは、照合される ICMP メッセージ コードを指定します。この値を「-1」に設定すると、フィルタリングで任意の ICMP コードが一致します。
TCPEstablished	このフィルタが true の場合は、TCP プロトコルで接続が確立されているときに、TCP データグラムが ACK、FIN、PSH、RST、SYN、または URG のコントロール ビット セットを持っていると一致と見なされます。false の場合は、任意の TCP データグラムで一致と見なされます。
LogEnabled	フィルタリング サブシステムによってフィルタリングされたフレームが記録されるかどうかを指定します。true の場合は、すべてのフレームが記録されます。false の場合は、いずれのフレームも記録されません。