IP ACL の設定

この章の内容は、次のとおりです。

ACL について

ACLは、トラフィックをフィルタリングするための順番に並べられた一連のルールです。デバイスは、パケットを適用する ACL を決定する際に、パケットをルールに対してテストしていきます。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するルールがない場合は、そのデバイスでのデフォルトルールが適用されます。デバイスは、許可されたパケットは処理し、拒否されたパケットは廃棄します。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACLを使用して、厳重にセキュリティ保護されたネットワークからインターネットに HyperText Transfer Protocol（HTTP; ハイパー テキスト トランスファ プロトコル）トラフィックが流入するのを禁止できます。 また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ACL のタイプと適用

ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。

レイヤ 2 トラフィックのフィルタリングでは、次のポート ACL のタイプがサポートされます。

- IP ACL：IPv4 ACL は IP トラフィックだけに適用されます。
- MAC ACL：MAC ACL は非 IP トラフィックにだけ適用されます。

ACL の適用順序

ACL は次の順序で適用されます。

1. 着信ポート ACL
2. 発信ポート ACL

ルール

ACLによるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。 ルールは実行コンフィギュレーション内に表示されます。 ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。

アクセス リスト コンフィギュレーション モードで permit または deny コマンドを使用すると、ACLにルールを作成できます。 これにより、デバイスは許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。 ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。 指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。 送信元と宛先の指定方法は、IP ACL と MAC ACL のどちらを設定するかによって異なります。

プロトコル

IP ACL および MAC ACL では、トラフィックをプロトコルで識別できます。 一部のプロトコルは名前で指定できます。 たとえば、IP ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。 MAC ACL では、プロトコルをそのプロトコルの Ethertype 番号（16 進数）で指定できます。 たとえば、MAC ACL ルールの IP トラフィックの指定に 0x0800 を使用できます。

IP ACL では、インターネット プロトコル番号を表す整数でプロトコルを指定できます。 たとえば、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を指定するには、115 を使用します。

暗黙のルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にデバイスがトラフィックに適用するルールです。 ACL のルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IP ACL には、不一致の IP トラフィックを拒否する次の暗黙ルールがあります。

```
deny ip any any
```

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny any any
```

この暗黙ルールによって、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックが確実に拒否されます。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。これらのオプションは、ACLのタイプによって異なります。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- IP ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 4 プロトコル
  - TCP/UDP ポート
  - ICMP タイプおよびコード
  - IGMP タイプ
  - 優先レベル
  - DiffServ コード ポイント（DSCP）値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- MAC ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 3 プロトコル
- VLAN ID
- サービス クラス（CoS）

シーケンス番号

デバイスはルールのシーケンス番号をサポートしています。 入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。 シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。 たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

  ```
  switch(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。 この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。 たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

さらに、ACL内のルールにシーケンス番号を再割り当てすることも可能です。 シーケンス番号の再割り当ては、ACL内に、100、101のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

統計情報

デバイスは IPv4 ACL および MAC ACL に設定する各ルールのグローバル統計を維持できます。 1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計数が維持されます。

（注） インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。 たとえば、すべての IPv4 ACL の末尾にある暗黙の deny ip any any ルールと一致するパケットのカウントはデバイスに維持されません。 暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。

ACL ロギング

アクセス コントロール リスト（ACL）のロギングを使用して、特定の ACL に影響するフローをモニタできます。 ACL は、アクセス コントロール エントリ（ACE）でそのオプションのログ キーワードを設定できます。 オプションを設定すると、入力した ACL の許可条件または拒否条件に一致する各フローの統計情報がソフトウェアで記録されます。

次のコマンドを入力して、ACL にログ オプションを適用できます。

```
switch(config)# ip access-list [name]
switch(config-acl)# permit tcp any 156.10.3.44/24 log
```

暗黙拒否ルールは ACL のデフォルト アクションです。 暗黙拒否ルールに一致するパケットを記録するには、明示的な拒否ルールを作成し、ログ キーワードを追加する必要があります。

ACL のロギングが適用されるのは、ip access-list コマンドで設定された ACL だけです。 仮想スーパーバイザ モジュール（VSM）の管理インターフェイスやセレクタ（aaa authen match、qos match など）のような他のトラフィックは、記録されません。

統計情報およびロギングはフローごとに提供されます。 フローは次の IP フローによって定義されます。

- VSM ID
- 仮想イーサネット モジュール（VEM）ID
- 送信元インターフェイス
- プロトコル
- 送信元 IP アドレス
- 送信元ポート
- 宛先 IP アドレス
- 宛先ポート

スケーラビリティは次の機能によって提供されます。

- 各 Cisco Nexus 1000V スイッチで最大 64 個の VEM をサポートできます。
- 各 VEM では最大 5000 の許可フローおよび 5000 の拒否フローをサポートできます。 許可/拒否フローの最大数は設定可能なオプションです。

- フローのレポート インターバルは 5 ～ 86,400 秒（1 日）の範囲で設定できます。
- 設定フローの Syslog レベルは 0 ～ 7 の範囲で指定できます。
- 最大 3 台の Syslog サーバがサポートされます。

ACL フロー

ACL ロギングに関連する ACL フローには次の特性があります。

- 同一の ACL アクションを実行する同じパケット ヘッダー（SrcIP、DstIP、Protocol、SrcPort、DstPort）を持つ IPv4 パケットのストリームを表します。 各フロー エントリがフローと一致するパケットの数を追跡します。
- ロギングが対応する入力/出力 ACL ポリシーでイネーブルになっている場合にだけ作成されます。 入力および出力フローは個別に追跡されます。
- 各 VEM で最大 10,000 の ACL フローを追跡します。フローのスペースは許可/拒否フロー間で共有され、それぞれの最大値は 5000 ですが、これは設定可能です。
- 各フロー エントリは、次の要素で構成されます。
  - パケットのタプル
  - ACL アクション
  - 方向
  - パケット数
- ACL フローのライフ サイクルは次のとおりです。
  - フローは、単一方向ストリーム内の最初のパケットがレイヤ 3 ACL ポリシーと一致すると作成されます。 新しいフロー通知が Syslog サーバに送信されます。
  - フローのタプルと一致するタプルを持つ後続のすべてのパケットにより、フローあたりのパケット カウンタが増加します。
  - 各フローは、設定されたレポート間隔に基づいて、定期的に追跡されます。 それぞれの定期的なレポートによって、最後の定期的なレポート以降に出現したすべてのアクティブ フローおよび対応するパケット カウントが、Syslog サーバに報告されます。
  - 1 回の完全な間隔で、フローと一致するパケットが出現しなかった場合、フロー エントリが削除されます。 これは、唯一のフロー エージング方式です。
  - フローはステートフルではありません。 TCP フローの接続トラッキングはありません。
- フローを報告するプロセスは、次のように発生します。
  - フローが作成されるたびに、新しいフローの通知メッセージが Syslog サーバに送信されます。

- 次に、各アクティブフローごとの定期的なレポートが届きます。最後の定期的なレポート以降に、フローと一致するパケットが出現すると、フローはアクティブになります。
- パケットのタプル、ACL アクション、方向、VEM ID、VSM ID、パケット数を含むフロー情報が Syslog サーバにエクスポートされます。
- 定期的な時間のデフォルト設定は 5 分で、最小は 5 秒です。 新しいユーザ空間の ACL ロギング スレッドが、定期的なポーリングおよびレポート機能を処理します。
- フローのスペース使用量を識別する Syslog メッセージが、最大しきい値の 75 パーセント、90 パーセント、および 100 パーセントになったときに、各間隔で一度だけ Syslog サーバに送信されます。

Syslog メッセージ

Syslog メッセージの特性は次のとおりです。

- フロー情報が含まれている Syslog メッセージは各 VEM からエクスポートされます。
- Syslog クライアント機能は RFC-5424 に準拠しており、UDP ポート（514）を使用してサーバと通信します。
- ホストは、リモート Syslog サーバに到達できる vmknic インターフェイスを使用して設定する必要があります。
- ESXi-5.0 ホストでは、Syslog メッセージはファイアウォールによってブロックされます。Cisco Nexus 1000V には、ポート 514 のファイアウォールを開くインストール スクリプトがあります。

IP ACL の前提条件

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。
- ACL を設定するインターフェイス タイプについての知識が必要です。

IP ACL の注意事項と制約事項

- ほとんどの場合、IP パケットの ACL 処理は、I/O モジュール上で実行されます。 管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。この場合、速度は遅くなります。
- ACL は、ポート チャネルではサポートされていません。

IP ACL のデフォルト設定

パラメータ	デフォルト
IP ACL	デフォルトの IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

IP ACL の設定

IP ACL の作成

デバイスに IPv4 ACL を作成し、これにルールを追加できます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ip access-list** {*name* | **match-local-traffic**}	名前付き IP ACL（最大 64 文字）を作成し、IP ACL コンフィギュレーション モードを開始します。 match-local-traffic オプションは、ローカルに生成されたトラフィックのマッチングをイネーブルにします。 no オプションは指定されたアクセス リストを削除します。
ステップ 3	switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*	IP ACL 内にルールを作成します。 多数のルールを作成できます。 sequence-number 引数には、1 ～ 4294967295 の整数を指定できます。 **permit** キーワードと **deny** キーワードには、トラフィックを識別するための多くの方法が用意されています。

	コマンドまたはアクション	目的
ステップ 4	switch(config-acl)# **statistics per-entry**	（任意） その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	switch(config-acl)# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 6	switch(config-acl)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

IP ACL の変更

既存の IPv4 ACL に対してルールの追加または削除を行うことができます。 既存のルールは変更できません。 ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip access-list** *name*	指定した ACL の IP ACL コンフィギュレーション モードを開始します。
ステップ 3	switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*	（任意） IP ACL 内にルールを作成します。 シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。 シーケンス番号を指定しないと、ルール

	コマンドまたはアクション	目的
		はACLの末尾に追加されます。 sequence-number引数には、1 ～ 4294967295 の整数を指定できます。 **permit** キーワードと **deny** キーワードには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination}*	（任意） 指定したルールを IP ACL から削除します。 **permit** キーワードと **deny** キーワードには、トラフィックを識別するための多くの方法が用意されています。
ステップ 5	switch(config-acl)# [**no**] **statistics per-entry**	（任意） その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 no オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	switch(config-acl)# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 7	switch(config-acl)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# 100 permit ip 192.168.2.0/24 any
switch(config-acl)# no 80
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

IP ACL の削除

ACLを削除しても、適用されているインターフェイスの設定には影響しません。デバイスは削除された ACL を空であると見なします。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- ACL がインターフェイスに適用されているかどうかがわかっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no ip access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	switch(config)# **show ip access-list** *name* **summary**	（任意） IP ACL の設定を表示します。 ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# no ip access-list acl-01
switch(config)# show ip access-lists acl-01 summary
switch(config)# copy running-config startup-config
```

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。 後続の各ルールには、直前のルールよりも大きい番号が付けられます。 番号の間隔は、指定した増分によって決まります。 starting-sequence-number 引数と increment 引数は、1 ～ 4294967295 の整数で指定します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 4	switch(config)# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# resequence access-list ip acl-01 100 10
switch(config)# show ip access-lists acl-01
switch(config)# copy running-config startup-config
```

IP ACL のポート ACL としての適用

IPv4 または ACL をレイヤ 2 インターフェイスの物理ポートに適用してポート ACL を設定するには、次の手順を実行します。

IP ACL はポート プロファイルに設定することもできます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- EXEC モードで CLI にログインしていること。
- 1 つのインターフェイスに 1 つのポート ACL を適用できます。
- 適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface vethernet** *port*	指定された vEthernet インターフェイスをインターフェイス コンフィギュレーション モードにします。
ステップ 3	switch(config-if)# **ip port access-group** *access-list* [**in** | **out**]	インバウンドまたはアウトバウンド IPv4 ACL をインターフェイスに適用します。1 つのインターフェイスに 1 つのポート ACL を適用できます。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **show running-config aclmgr**	（任意） ACL の設定を表示します。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# interface vethernet 40
switch(config-if)# ip port access-group acl-l2-marketing-group in
switch(config-if)# show running-config aclmgr
switch(config-if)# copy running-config startup-config
```

IP ACL のポート プロファイルへの追加

IP ACL をポート プロファイルに追加するには、次の手順を実行します。

次の情報を知っている必要があります。

- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびプロファイルに指定する名前。
- このポート プロファイルに対して設定する IP アクセス コントロール リストの名前。
- アクセス リストのパケット フローの方向。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- このポート プロファイルに追加する IP ACL が作成され、名前がわかっていること。
- 既存のポートプロファイルを使用する場合は、それが作成され、名前がわかっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*	名前付きポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-port-prof)# **ip port access-group** *name* { **in** | **out** }	着信トラフィックまたは発信トラフィックのポートプロファイルに名前付き ACL を追加します。
ステップ 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	（任意） 確認のためにコンフィギュレーションを表示します。
ステップ 5	switch(config-port-prof)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# ip port access-group allaccess4 out
switch(config-port-prof)# show port-profile name AccessProf
switch(config-port-prof)# copy running-config startup-config
```

管理インターフェイスへの IP ACL の適用

管理インターフェイス mgmt0 に IPv4 または ACL を適用するには、次の手順を実行します。

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface mgmt0**	管理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# [**no**] **ip access-group***access-list* [**in** | **out**]	指定したインバウンド IPv4 ACL またはアウトバウンド IPv4 ACL をインターフェイスに適用します。 no オプションは指定された設定を削除します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **show ip access-lists** *access-list*	（任意） ACL の設定を表示します。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# interface mgmt0
switch(config-if)# ip access-group telnet in
switch(config-if)# show ip access-lists telnet summary
IP access list telnet
statistics per-entry
Total ACEs Configured:2

Configured on interfaces:
mgmt0 - ingress (Router ACL)

Active on interfaces:
mgmt0 - ingress (Router ACL)
switch(config-if)# copy running-config startup-config
```

ACL ロギングの設定

ACL ロギングは、すべての仮想イーサネット モジュール（VEM）で、デフォルトでイネーブルになっています。 また、次の事項も ACL ロギングの設定に適用されます。

- ログ キーワードを追加することによって、ロギングについて任意のルールをイネーブルにできます。
- ログ キーワードがイネーブルのルールに当てはまるパケットだけが記録されます。

ACL ロギングのディセーブル化

次のコマンドを入力して、VEM での ACL ロギングをディセーブルにできます。

コマンド	目的
[**no**] **logging ip access-list cache module** *vem*	指定された VEM での ACL ロギングをディセーブルにします。

パケット カウンタを累積する時間間隔の設定

Syslog サーバにレポートする前にパケット カウンタを累積する時間間隔を設定できます。 5 ～ 86,400 秒（1 日）の範囲の時間を秒単位で入力します。 デフォルトは 300 秒（5 分）です。

次のいずれかのコマンドを入力して、パケット カウンタを累積する時間を設定できます。

コマンド	目的
logging ip access-list cache interval *secs*	Syslog サーバにレポートする前にパケット カウンタを累積する時間間隔を秒単位で設定します。num は秒数を示します。
[**no**] **logging ip access-list cache interval** *secs*	デフォルトの時間間隔の設定である 300 秒（5 分）に設定を戻します。num は秒数を示します。

次に、時間間隔が経過すると定期的に送信される時間間隔の Syslog メッセージのフォーマットの例を示します。

```
ACL-LOGGING-6-PERMIT-FLOW-INTERVAL <VSM-id> <VEM-id> <protocol> <source-interface>
 <source-ip/source-port)> <destination-ip/destination-port> Hit-count = <nnn>

ACL-LOGGING-6-DENY-FLOW-INTERVAL <VSM-id> <VEM-id> <protocol> <source-interface>
<source-ip/source-port)> <destination-ip/destination-port> Hit-count = <nnn>
```

次に、時間間隔の条件が満たされると送信される時間間隔の Syslog メッセージのフォーマットの例を示します。

```
ACL-LOGGING-6-MAX-PERMIT-FLOW-REACHED: The number of ACL log permit-flows has reached 75%
limit (<n>)
ACL-LOGGING-6-MAX-PERMIT-FLOW-REACHED: The number of ACL log permit-flows has reached 90%
limit (<n>)
ACL-LOGGING-6-MAX-PERMIT-FLOW-REACHED: The number of ACL log permit-flows has reached 100%

limit (<n>)

ACL-LOGGING-6-MAX-DENY-FLOW-REACHED: The number of ACL log deny-flows has reached 75%
limit (<n>)
ACL-LOGGING-6-MAX-DENY-FLOW-REACHED: The number of ACL log deny-flows has reached 90%
limit (<n>)
ACL-LOGGING-6-MAX-DENY-FLOW-REACHED: The number of ACL log deny-flows has reached 100%
limit (<n>)
```

フローの設定

VEM あたりの拒否フローおよび許可フローの数を設定できます。 有効な範囲は 0 ～ 5000 フローです。 デフォルトは 3000 です。 Syslog メッセージは、フローが最大しきい値に近づくと送信されます。 最初のメッセージはフローの数が最大しきい値の 75 パーセントに到達すると送信され、次のメッセージはフローの数が最大しきい値の 90 パーセントに到達すると送信されます。 最後のメッセージはフローの数が 100 パーセントの最大しきい値に到達すると送信されます。

許可フローの設定

次のいずれかのコマンドを入力して、許可フローを設定できます。

コマンド	目的
logging ip access-list cache max-permit-flows *num*	num はフロー数で、許可フロー数を設定します。
[**no**] **logging ip access-list cache max-permit-flows**	デフォルトの許可フロー値である 3000 に設定を戻します。

次に、許可フローの Syslog メッセージの例を示します。

- 新しいフロー通知メッセージ

```
-  Aug 28 04:17:19 fish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-ecology -
ACLLOG-PERMIT-FLOW-CREATE VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.21, Source Port: 42196, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1
```

- 定期的にフローをレポートするメッセージ

```
-  Aug 28 04:17:20 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.21, Source Port: 42196, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1245
```

- しきい値超過アラーム メッセージ

```
-  Aug 28 04:17:22 sfish-231-157.cisco.com 1 2011-08-28T11:14:24 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 75 percent

limit (3969)
-  Aug 28 04:17:26 sfish-231-157.cisco.com 1 2011-08-28T11:14:26 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 90 percent

limit (4969)
-  Aug 28 04:17:27 sfish-231-157.cisco.com 1 2011-08-28T11:14:31 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 100
percent
limit (5000)
```

拒否フローの設定

次のいずれかのコマンドを入力して、拒否フローを設定できます。

コマンド	目的
logging ip access-list cache max-deny-flows *num*	num はフロー数で、拒否フロー数を設定します。
[**no**] **logging ip access-list cache max-deny-flows**	デフォルトの拒否フロー値である 3000 に設定を戻します。

次に、拒否フローの Syslog メッセージの例を示します。

- 新しいフロー通知メッセージ

```
-  Aug 28 04:17:19 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-DENY-FLOW-CREATE VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.100, Source Port: 48528, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1
```

- 定期的にフローをレポートするメッセージ

```
-  Aug 28 04:17:20 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-DENY-FLOW-INTERVAL VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.100, Source Port: 47164, Destination Port: 8029, Source Interface: Veth2,

Protocol: "TCP"(6), Hit-count = 1245
```

- しきい値超過アラーム メッセージ

```
-  Aug 28 04:17:27 sfish-231-157.cisco.com 1 2011-08-28T11:14:31 - n1k-acllog -
ACLLOG-MAX-DENY-FLOW-REACHED The number of ACL log deny-flows has reached 75 percent
limit
(4330)
-  Aug 28 04:18:27 sfish-231-157.cisco.com 1 2011-08-28T11:15:31 - n1k-acllog -
ACLLOG-MAX-DENY-FLOW-REACHED The number of ACL log deny-flows has reached 90 percent
limit
(4630)
-  Aug 28 04:20:17 sfish-231-157.cisco.com 1 2011-08-28T11:17:20 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 100
percent
limit (5000)
```

Syslog サーバの重大度

最大 3 台のリモート Syslog サーバに対して、ACL ロギング Syslog メッセージの重大度を設定できます。 有効な範囲は 0 ～ 7 です。 デフォルトの重大度は 6 です。

重大度コード	重大度	説明
0	Emergency	システムは使用不能
1	Alert	即時対処が必要
2	Critical	クリティカルな状態
3	Error	エラー状態
4	警告	警告状態
5	Notice	正常だが注意を要する状態
6	Informational	情報メッセージ
7	Debug	デバッグレベル メッセージ

Syslog メッセージの重大度の設定

次のいずれかのコマンドを入力して、Syslogメッセージの重大度とメッセージの送信先になるサーバを設定できます。

コマンド	目的
acllog match-log-level *level*	Syslog メッセージを送信する重大度を設定します。level は 0 ～ 7 の重大度コードです。
[**no**] **logging ip access-list cache max-deny-flows**	デフォルトの重大度である 6 に設定を戻します。
logging server *A.B.C.D 0-7*	重大度を設定する Syslog サーバを指定します。*A.B.C.D* は Syslog サーバの IP アドレスです。0-7 は重大度で、選択できます。

IP ACL の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config aclmgr	IP ACL の設定および IP ACL が適用されているインターフェイスを含めて、ACL の設定を表示します。
show ip access-lists [*name*]	すべての IPv4 アクセス コントロール リスト（ACL）または特定の IPv4 ACL を表示します。
show ip access-list [*name*] su**mmary**	設定済みのすべての IPv4 ACL または名前付き IPv4 ACL の要約を表示します。
show running-config interface	ACL が適用されたインターフェイスの設定を表示します。
show logging ip access-list status	VSM の ACL ロギング設定を表示します。
vemcmd show acllog config	VEM ACL ロギング設定を表示します。

IP ACL のモニタリング

IP ACL のモニタリングには、次のいずれかのコマンドを使用します。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。 IPv4 ACL に statistics per-entry コマンドが含まれている場合は、show ip access-lists コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear ip access-list counters	すべての IPv4 ACL または特定の IPv4 ACL の統計情報をクリアします。

IP ACL の設定例

次に、acl-01 という名前の IPv4 ACL を作成し、これをポート ACL として vEthernet インターフェイス 40 に適用する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl# interface vethernet 40
switch(config-acl# ip port access-group acl-01 in
```

次に、ローカルに生成されたトラフィックのアクセスリストマッチングをイネーブルにする例を示します。

```
switch# ip access-list match-local-traffic
```

次に、VSM の ACL ロギングの設定を確認する例を示します。

```
switch# show logging ip access-list status
Max deny flows = 3000
Max permit flows = 3000
Alert interval = 300
Match log level = 6
VSM IP = 192.168.1.1
Syslog IP = 10.1.1.1
Syslog IP = 0.0.0.0
Syslog IP = 0.0.0.0
ACL Logging enabled on module(s):
4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51
52 53 54 55 56 57 58 59 60 61 62 63 64 65 66
ACL Logging disabled on module(s):
3
```

次に、VEM の ACL ロギングの設定を確認する例を示します。

```
switch# vemcmd show acllog config
ACL-Log Config:
Status: enabled
Reporting Interval: 300
Max Permit Flows: 3000
Max Deny Flows: 3000
Syslog Facility : 4
Syslog Severity: 6
Syslog Srvr 1: 10.1.1.1
```

```
Syslog Srvr 2: 0.0.0.0
Syslog Srvr 3: 0.0.0.0
VSM: 192.168.1.1
```

IP ACL の機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能の履歴	リリース	機能情報
ACL ロギング	4.2(1)SV1(5.1)	この機能が導入されました。
mgmt0 インターフェイスの IP ACL	4.2(1) SV1(4)	この機能が導入されました。
IP ACL	4.0(4)SV1(1)	この機能が導入されました。