CHAPTER 31

Cisco IOS ACL サポートの概要

この章では、Catalyst 6500 シリーズ スイッチの Cisco IOS Access Control List（ACL; アクセス制御リスト）サポートについて説明します。

Cisco IOS ACL 設定の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfacls.html

Cisco IOS ACL 設定時の注意事項および制約事項

Cisco IOS ACL 設定には、次の注意事項および制約事項が適用されます。

- Cisco IOS ACL をレイヤ 3 ポートおよび VLAN インターフェイスに直接、適用できます。
- VLAN ACL（VACL）を VLAN に適用できます（第 32 章「VLAN アクセス制御リスト（VACL）の設定」を参照）。
- 各タイプの ACL（IP、Internetwork Packet Exchange（IPX）、および Media Access Control（MAC; メディア アクセス制御））は対応するトラフィック タイプだけをフィルタリングします。Cisco IOS MAC ACL が IP または IPX トラフィックと一致することはありません。
- PFC3B では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、PISA のソフトウェアでサポートされます。
- パケットがアクセス グループによって拒否された場合、デフォルトで PISA が Internet Control Message Protocol（ICMP）到達不能メッセージを送信します。

  ip unreachables コマンドがイネーブルの場合（デフォルト）、スーパーバイザ エンジンは拒否されたパケットの大部分をハードウェアで廃棄し、一部のパケット（最大で 10 パケット/秒）だけが PISA に送信されて廃棄されます（これにより ICMP 到達不能メッセージが生成されます）。

  拒否されたパケットを廃棄し、ICMP 到達不能メッセージを生成することによって PISA の CPU にかかる負荷を軽減するには、**no ip unreachables** インターフェイス コンフィギュレーション コマンドを入力して、ICMP 到達不能メッセージをディセーブルにします。これにより、アクセス グループによって拒否されたすべてのパケットがハードウェアで廃棄されます。
- パケットが VACL によって拒否された場合、ICMP 到達不能メッセージは送信されません。

- 名前付き ACL（番号付き ACL ではなく）の使用を強く推奨します。ACL の設定時、変更時、またはシステムの再起動時に、CPU の使用を節約できるからです。ACL エントリを作成する、または既存の ACL エントリを変更するときに、ソフトウェアは ACL マージと呼ばれる CPU 中心の処理を実行して、ACL 設定を PFC ハードウェアにロードします。ACL マージは、システムの再起動時にスタートアップ コンフィギュレーションを適用するときにも実行されます。

  名前付き ACL を使用すると、ACL マージが発生するのは、ユーザが **named-acl** コンフィギュレーション モードを終了するときだけになります。しかし、番号付き ACL を使用した場合は、ACE 定義のたびに ACL マージが実行されるので、ACL 設定時に多数の即時マージが発生します。

ハードウェアおよびソフトウェア ACL のサポート

ACL は、PFC3B によってハードウェアで処理することも、または PISA によってソフトウェアで処理することもできます。次の動作における、ACL のソフトウェアとハードウェア処理を説明します。

- PFC3B によるハードウェア サポートは、番号付き ACL の場合より、名前付き ACL の場合の方が効率的です。
- 標準 ACL および拡張 ACL（入力および出力）の [deny] ステートメントに一致する ACL フローは、[ip unreachables] がディセーブルに設定されている場合、ハードウェアによって廃棄されます。
- 標準 ACL および拡張 ACL（入力および出力）の [permit] ステートメントに一致する ACL フローは、ハードウェアで処理されます。
- VACL フローはハードウェアで処理されます。VACL で指定されたフィールドのハードウェア処理がサポートされていない場合、このフィールドは無視されるか（ACL の **log** キーワードなど）、または設定全体が拒否されます（IPX ACL パラメータを含む VACL など）。
- VACL ログ機能はソフトウェアで処理されます。
- ダイナミック ACL フローはハードウェアで処理されます。
- アイドル タイムアウトはソフトウェアで処理されます。

  （注） アイドル タイムアウトの設定はできません。Catalyst 6500 シリーズ スイッチ では、**access-enable host timeout** コマンドはサポートされていません。

- MPLS インターフェイスを除き、セッション内の最初のパケットが RP のソフトウェアで処理された後、再帰 ACL フローがハードウェアで処理されます。
- 特定のポート上の ACL アクセス違反の IP アカウントは､そのポート上で拒否された全パケットを PISA に転送し、ソフトウェアで処理させることによってサポートされます。この動作は他のフローには影響しません。
- PFC3B では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、PISA のソフトウェアでサポートされます。
- 名前ベースの拡張 MAC アドレス ACL は、ハードウェアでサポートされています。

- 次の ACL タイプは、ソフトウェアによって処理されます。
  - Internetwork Packet Exchange（IPX）アクセス リスト
  - 標準 XNS アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - 拡張 MAC アドレス アクセス リスト
  - プロトコル タイプコード アクセス リスト

（注）　ヘッダー長が 5 バイト未満の IP パケットは、アクセス制御されません。

- Optimized ACL Logging（OAL; 最適化された ACL ロギング）を設定しない場合、ロギングを必要とするフローはソフトウェアで処理され、ハードウェアでの非ロギング フローの処理には影響しません（「PFC3B での OAL」（P.31-3）を参照）。
- ソフトウェアで処理されるフローの転送レートは、ハードウェアで処理されるフローに比べると、大幅に小さくなります。
- **show ip access-list** コマンドの出力に表示されるマッチ カウントには、ハードウェアで処理されたパケットは含まれません。

PFC3B での OAL

ここでは OAL（Optimized ACL Logging）について説明します。

OAL の概要

OAL は ACL ロギングをハードウェアでサポートします。OAL を設定しないかぎり、ロギングを必要とするパケットは、PISA のソフトウェアで完全に処理されます。OAL では、PFC3B のハードウェアでパケットの許可または廃棄を行い、最適化ルーチンを使用して情報を PISA に送信し、ロギング メッセージを生成します。

OAL に関する注意事項および制約事項

OAL には、次の注意事項および制約事項が適用されます。

- Optimized ACL Logging（OAL; 最適化された ACL ロギング）キャプチャと VACL キャプチャには互換性がありません。スイッチに両方の機能を混在させないでください。OAL が設定された状態で、SPAN を使用してトラフィックをキャプチャします。
- OAL がサポートされるのは、PFC3B 上だけです。
- OAL は IPv4 ユニキャスト パケットだけをサポートしています。
- OAL は、許可された入力トラフィックの VACL ロギングをサポートしています。

- OAL は、ポート ACL（PACL）はサポートしていません。
- OAL は、次のものに対してはハードウェアでのサポートをしていません。
  - 再帰 ACL
  - 他の機能（QoS など）のトラフィックのフィルタ処理に使用される ACL
  - 例外パケット（TTL 障害や MTU 障害など）
  - IP オプションが指定されたパケット
  - レイヤ 3 でルータへのアドレスが指定されたパケット
  - ICMP 到達不能メッセージを生成するために PISA へ送信されるパケット
  - ハードウェアでは加速されず、機能によって処理されるパケット
- 拒否されたパケットに OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL の設定

ここでは、OAL の設定手順について説明します。

（注）
- この項で使用しているコマンドの構文および使用方法の詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Command Reference*, Release 12.2ZY』を参照してください。
- 拒否されたパケットに OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL グローバル パラメータの設定

OAL グローバル パラメータを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# logging ip access-list cache {{entries number_of_entries} | {interval seconds} | {rate-limit number_of_packets} | {threshold number_of_packets}}`	OAL グローバル パラメータを設定します。
`Router(config)# no logging ip access-list cache {entries | interval | rate-limit | threshold}`	OAL グローバル パラメータをデフォルトに戻します。

OAL グローバル パラメータを設定する場合、次の情報に注意してください。

- **entries** *number_of_entries*
  - キャッシュされるエントリの最大数を設定します。
  - 範囲 : 0 ～ 1,048,576（カンマを付けずに入力）
  - デフォルト : 8192
- **interval** *seconds*
  - ログのためにエントリが送信されるまでの最大時間を設定します。この時間中エントリが非アクティブの場合、キャッシュから削除されます。
  - 範囲 : 5 ～ 86,400（1440 分つまり 24 時間、カンマを付けずに入力）
  - デフォルト : 300 秒（5 分）
- **rate-limit** *number_of_packets*
  - ソフトウェアで 1 秒間にログに記録されるパケット数を設定します。
  - 範囲 : 10 ～ 1,000,000（カンマを付けずに入力）
  - デフォルト : 0（レート制限がオフになり、すべてのパケットがログに記録されます）
- **threshold** *number_of_packets*
  - エントリがログに記録されるまでに一致するパケット数を設定します。
  - 範囲 : 1 ～ 1,000,000（カンマを付けずに入力）
  - デフォルト : 0（一致パケット数に達してもログの記録は開始されません）

インターフェイスでの OAL の設定

インターフェイスで OAL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port}`	設定するインターフェイスを指定します。
ステップ 2	`Router(config-if)# logging ip access-list cache in`	インターフェイスの入力トラフィックに対して OAL をイネーブルにします。
	`Router(config-if)# no logging ip access-list cache`	インターフェイスでの OAL をディセーブルにします。
ステップ 3	`Router(config-if)# logging ip access-list cache out`	インターフェイスの出力トラフィックに対して OAL をイネーブルにします。
	`Router(config-if)# no logging ip access-list cache`	インターフェイスでの OAL をディセーブルにします。

1. *type* = レイヤ 3 スイッチド トラフィックをサポートする任意のタイプ

OAL 情報の表示

OAL 情報を表示するには、次の作業を行います。

コマンド	目的
`Router # show logging ip access-list cache`	OAL 情報を表示します。

キャッシュされた OAL エントリのクリア

キャッシュされた OAL エントリをクリアするには、次の作業を行います。

コマンド	目的
`Router # clear logging ip access-list cache`	キャッシュされた OAL エントリをクリアします。

ACL におけるレイヤ 4 演算の使用上の注意事項および制約事項

ここでは、レイヤ 4 ポート演算を含む ACL を設定する場合の注意事項および制約事項について説明します。

- 「レイヤ 4 演算の使用」（P.31-6）
- 「LOU の使用」（P.31-7）

レイヤ 4 演算の使用

次のタイプの演算子を指定できます。

- gt（geater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）
- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に指定する演算は、*9* つまでにしてください。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

レイヤ 4 演算を使用するときは、次の 2 つの注意事項に従ってください。

- レイヤ 4 演算は、演算子またはオペランドが異なっていると、違う演算であると見なされます。たとえば、次の ACL には 3 つの異なるレイヤ 4 演算が定義されています（[gt 10] と [gt 11] は 2 つの異なるレイヤ 4 演算です）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

（注）　[eq] 演算子の使用に制限はありません。[eq] 演算子は LOU またはレイヤ 4 演算ビットを使用しないためです。LOU については、「LOU の使用」（P.31-7）を参照してください。

- レイヤ 4 演算は、同じ演算子 / オペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。たとえば次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

LOU の使用

LOU は、演算子 / オペランドの組み合わせを保存するレジスタです。ACL はすべて、LOU を使用します。最大 32 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存できますが、range 演算子だけは例外です。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子 / オペランドの組み合わせが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

レイヤ 4 演算数と LOU 数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU: 4

LOU は、次のように使用されています。

- LOU 1 に、[gt 10] と [lt 9] が保存されます。
- LOU 2 に、[gt 11] と [lt 6] が保存されます。
- LOU 3 に、[gt 20] が保存されます（半分は空き）。
- LOU 4 に、[range 11 13] が保存されます（range は 1 LOU を使用）。