ACL ロギングの設定

この章の内容は、次のとおりです。

ACL ロギングに関する情報

ACL ロギング機能では、ACL フローをモニタし、インターフェイスでドロップされたパケットをログに記録することができます。

IPv6 ACL ロギングの概要

ACL ロギング機能を設定すると、システムは ACL のフローをモニタし、ACL エントリの拒否条件に一致する各フローのドロップ パケットと統計情報をログに記録します。

統計情報とドロップパケットのログは、フローごとに生成されます。 フローは、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、宛先ポート値によって定義されます。 一致するフローについて維持される統計情報は、指定された時間間隔での ACL エントリによるフローの拒否件数です。

新しいフローが拒否されると（システム上ではすでにアクティブではないフロー）、システムはヒット カウント値 1 の 最初の Syslog メッセージを生成します。 次に、フローが拒否されるたびにシステムはフロー エントリを作成し、ヒット カウント値を増やします。

既存のフローが拒否されると、システムは各間隔の終了時に Syslog メッセージを生成し、現在の間隔でのフローに対するヒット カウント値を報告します。 Syslog メッセージの生成後、フローの

ヒットカウント値は次の間隔の間にゼロにリセットされます。この間隔の間に一度もヒットした記録がない場合は、フローが削除され、Syslog メッセージは生成されません。

ACL ロギングの注意事項と制約事項

ACL ロギングには次の設定上の注意事項と制約事項があります。

- 拒否 ACE 条件のみに一致するシステム ログ パケット。 許可 ACE 条件のロギングはサポートしていません。
- ロギング オプションは ACL 拒否エントリに適用される可能性があります。 ロギング オプションを暗黙的に拒否されたトラフィックに適用するには、特定のすべて拒否 ACL エントリのロギング オプションを設定する必要があります。
- ACL ロギングは、**ipv6 port traffic-filter** コマンドによって設定されたポート ACL （PACL）と、**ipv6 traffic-filter** コマンドのみによって設定されたルーテッド ACL （RACL）に適用されます。
- フローと拒否フローの総数は、DOS 攻撃を避けるためにユーザ定義の最大値に 限定されます。 この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- CPU 使用率に影響を与えずに多数のフローをサポートできるようにするため、システムはハッシュ テーブルを使用してフローの場所を特定します。 システムはタイマー キューを使用して、多数のフローのエージング管理を効率よく行います。
- ACL ロギング プロセスによって生成される Syslog エントリ数は、ACL ロギング プロセスで設定されたロギング レベルによって制限されています。 Syslogエントリの数がこの制限を超えると、ロギング機能が一部のロギング メッセージをドロップする場合があります。 したがって、ACL ロギングは課金ツールやアクセス リストとの一致数を正確に把握するための情報源として使用しないでください。
- ハードウェアの速度リミッタはパケット単位でトラフィックの速度を制限しますが、コントロール プレーン ポリシング（COPP）は、バイト単位でトラフィックの速度を制限します。パケット サイズとハードウェア速度リミッタの両方の値が大きい場合、COPP のデフォルト値を上回り、システムがパケットをドロップ する可能性があります。 この制限を回避するには、デフォルトの CIR 値（64000 バイト）を 2560000 バイトなどの大きな値に増やします。デフォルト CIR を増やすと、通常はパケットのロギングが発生します。
- IPv6 ロギングは管理または VTY （端末）ポートではサポートされていません
- IPv6 ロギングは出力 RACL ではサポートされません（ASIC の制約事項のため）。
- IPv6 ロギングは出力 VACL ではサポートされません（ASIC の制約事項のため）。

ACL ロギングの設定

ACL ロギング プロセスを設定するには、まずアクセス リストを作成し、指定された ACL を使用してインターフェイスで IPv6 トラフィックのフィルタリングをイネーブルにし、最後に ACL ロギング プロセス パラメータを設定します。

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	**ipv6 access-list** *name* 例： `switch(config)# ipv6 access-list logging-test`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト 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	**deny ipv6 any** *destination-address* **log** 例： `switch(config-ipv6-acl)# deny ipv6 any 2001:DB8:1::1/64 log`	IPv6 アクセス リストに拒否条件を設定します。このエントリに対する一致をシステムがログに記録するようにするには、拒否条件を設定するときに **log** キーワードを使用する必要があります。
ステップ 4	**exit** 例： `switch(config-ipv6-acl)# exit`	設定を更新し、IPv6 アクセス リスト コンフィギュレーション モードを終了します。
ステップ 5	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet 1/1`	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 6	**ipv6 traffic-filter logging-test** {**in** | **out**} 例： `switch(config-if)# ipv6 traffic-filter logging-test in`	指定された ACL を使用して、インターフェイス上で IPv6 トラフィックのフィルタリングをイネーブルにします。 発信または着信トラフィックに ACL を適用できます。
ステップ 7	**exit** 例： `switch(config-if)# exit`	設定を更新し、インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**logging ip access-list cache interval** *interval* 例： `switch(config)# logging ip access-list cache interval 490`	ACL ロギング プロセスのログ更新間隔を秒数で設定します。 デフォルト値は 300 秒です。 指定できる範囲は 5 ～ 86400 秒です。
ステップ 9	**logging ip access-list cache entries** *number-of-flows* 例： `switch(config)# logging ip access-list cache entries 8001`	ACL ロギング プロセスによってモニタリングするフローの最大数を指定します。 デフォルト値は 8000 です。 指定できる値の範囲は、0 ～ 1048576 です。
ステップ 10	**logging ip access-list cache threshold** *threshold* 例： `switch(config)# logging ip access-list cache threshold 490`	アラート間隔の期限が満了する前に規定のパケット数がログ記録されると、システムは Syslog メッセージを生成します。
ステップ 11	**hardware rate-limiter access-list-log** *packets* 例： `switch(config)# hardware rate-limiter access-list-log 200`	アクセス リスト ロギングのためにスーパーバイザモジュールにコピーされるパケットのレート制限を pps で設定します。 範囲は 0 ～ 30000 です。
ステップ 12	**acllog match-log-level** *severity-level* 例： `switch(config)# acllog match-log-level 5`	ACL 一致をログ記録する最小の重大度を指定します。 デフォルト値は 6（情報）です。 0（緊急）～7（デバッグ）までの範囲があります。

ACL ロギング設定の確認

ACL ロギング設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show logging ip access-list status	拒否フローの最大数、現在の有効なログ間隔と現在の有効なしきい値を表示します。
show logging ip access-list cache	送信元 IP アドレスと宛先 IP アドレス、S ポートおよび D ポート情報などのアクティブ ログ フロー情報を表示します。

ACL ロギングの設定例

次に、ACL ロギング プロセスの設定方法の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 access-list logging-test
switch(config-ipv6-acl)# deny ipv6 any 2001:DB8:1::1/64 log
switch(config-ipv6-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ipv6 traffic-filter logging-test in
switch(config-if)# exit
switch(config)# logging ip access-list cache interval 400
switch(config)# logging ip access-list cache entries 100
switch(config)# logging ip access-list cache threshold 900
switch(config)# hardware rate-limiter access-list-log 200
switch(config)# acllog match-log-level 5
switch(config)# exit
switch#
```

次の例は、一般的な PACL ロギングの設定を示しています。

```
switch(config)# interface ethernet 8/11
switch(config-if)# ipv6 port traffic-filter v6log-pacl in
switch(config-if)# switchport access vlan 4064
switch(config-if)# speed 1000

switch(config)# interface Vlan 4064
switch(config-if)# no shutdown
switch(config-if)# no ip redirects
switch(config-if)# ipv6 address 4064::1/64


Switch# show vlan filter
vlan map v6-vaclmap:
Configured on VLANs: 4064

Switch# show vlan access-map v6-vaclmap
Vlan access-map v6-vaclmap
match ipv6: v6-vacl
action: drop
statistics per-entry
```