CHAPTER 10

ACL

この章では、アクセス コントロール リスト（ACL）に関する問題を識別して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

アクセス コントロール リスト（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ドロップします。

ACL は、ネットワークおよび特定のホストを不必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します。たとえば、ACL を使用して、セキュリティの高いネットワークからインターネットへの HTTP は許可しないようにしたりできます。ACL では、サイトの IP アドレスを使用して IP ACL 内でサイトを識別することにより、特定のサイトへの HTTP トラフィックだけを許可するといったこともできます。

トラフィックのフィルタリングに、次のタイプの ACL がサポートされています。

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

ACL ルールを使用してネットワーク トラフィックを設定する方法の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)*』を参照してください。

ACL 設定の制限事項

ACL には、次の設定上の制限事項が適用されます。

- 1 つの ACL に入れられるルールは 128 個までです。
- 1 つの VEM 内に 10,000 個を超える ACL を持つことはできません（すべての ACL にわたって拡散）。

ACL の制限事項

ACL には次の制限事項が適用されます。

- インターフェイス上の各方向に 1 つの IP ACL と 1 つの MAC ACL よりも多くの ACL を適用できません。
- MAC ACL は、レイヤ 2 パケットにしか適用されません。
- VLAN ACL はサポートされていません。
- ACL ルールでは IP フラグメントはサポートされていません。
- 非初期フラグメントは、ACL ルックアップの対象になりません。
- TCP フラグを指定するために制定されたオプションは、サポートされていません。
- 同一ルール内に 2 つの neq（等しくない）演算子を入れることはできません。
- ACL は、ポート チャネルでサポートされていません。

ACL のトラブルシューティング

ここに挙げるコマンドは、インターフェイスに対して設定され適用されているポリシーを見るために VSM 上で使用できるものです。

次のコマンドは、設定済みの ACL を表示するために使用できます。

- **show access-list summary**

次のコマンドは、設定エラーの中での ACLMGR および ACLCOMP のランタイム情報を表示したり、ACLMGR プロセス ランタイム情報設定エラーを収集したりするために VSM 上で使用できます。

- **show system internal aclmgr event-history errors**
- **show system internal aclmgr event-history msgs**
- **show system internal aclmgr ppf**
- **show system internal aclmgr mem-stats**（メモリの使用状況とリークのデバッグ用）
- **show system internal aclmgr status**
- **show system internal aclmgr dictionary**

次のコマンドは、ACLCOMP プロセス ランタイム情報設定エラーの収集に使用できます。

- **show system internal aclcomp event-history errors**
- **show system internal aclcomp event-history msgs**
- **show system internal aclcomp pdl detailed**
- **show system internal aclcomp mem-stats**（メモリの使用状況とリークのデバッグ用）

VEM での ACL ポリシーの表示

ここに挙げるコマンドは、VEM 上の設定済み ACL ポリシーの表示に使用できます。

次のコマンドは、そのサーバにインストールされている ACL のリストを表示します。

```
~ # module vem 3 execute vemcmd show acl
Acl-id Ref-cnt  Type Numrules  Stats
    1      1    IPv4      1    disabled
```

Acl-id は、この VEM のローカル ACLID です。Ref-cnt は、この VEM 内のこの ACL のインスタンスの数です。

次のコマンドは、ACL がインストールされているインターフェイスのリストを表示します。

```
~ # module vem 3 execute vemcmd show acl pinst
LTL   Acl-id    Dir
 16       1    ingress
```

ポリシー検証に関する問題のデバッグ

ポリシー検証のエラーをデバッグするには、次の手順を実行します。

ステップ 1　VSM で、**debug logfile** *filename* コマンドを入力して、出力をブートフラッシュ内のファイルにリダイレクトします。

ステップ 2　**debug aclmgr all** コマンドを入力します。

ステップ 3　**debug aclcomp all** コマンドを入力します。

ポリシーが置かれているか、または対象となっている VEM に対して、VSM から次の手順を実行します。出力は、コンソールに表示されます。

ステップ 4　**module vem** *module-number* **execute vemdpalog debug sfaclagent all** コマンドを入力します。

ステップ 5　**module vem** *module-number* **execute vemdpalog debug sfpdlagent all** コマンドを入力します。

ステップ 6　**module vem** *module-number* **execute vemlog debug sfacl all** コマンドを入力します。

ステップ 7　**module vem** *module-number* **execute vemlog start** コマンドを入力します。

ステップ 8　**module vem** *module-number* **execute vemlog start** コマンドを入力します。

ステップ 9　検証エラーを発生させたポリシーを設定します。

ステップ 10　**module vem** *module-number* **execute vemdpalog show all** コマンドを入力します。

ステップ 11　**module vem** *module-number* **execute vemlog show all** コマンドを入力します。

Telnet または SSH セッションのバッファをファイルに保存します。ブートフラッシュ内に作成されたログファイルをコピーします。