

ACL ロギングに最適化された Nexus 7000 と 7700 シリーズ スイッチの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシュート](#)

[設定の注意点](#)

[詳細な ACL ロギング](#)

[グローバル OAL コマンドの説明](#)

[ロギング コマンドの説明](#)

[注意事項と制約事項](#)

概要

このドキュメントでは、Cisco Nexus 7000 および 7700 シリーズ スイッチの最適化されたアクセスコントロールリスト (ACL) のロギング (OAL) を設定する方法について説明します。

前提条件

要件

このドキュメントで説明する設定を開始する前に、基本的な ACL を使用した Nexus の設定を理解しておくことをお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco Nexus 7000 シリーズ スイッチ

- Cisco Nexus 7700 シリーズ スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

ロギング対応 ACL により、ネットワークを通過する、またはネットワーク デバイスによって廃棄されたときのトラフィックを詳細に理解できます。残念ながら、ACL ロギングは CPU 負荷が大きく、ネットワーク デバイスのその他の機能に悪影響を与える可能性があります。CPU サイクルを短縮するために、Cisco Nexus 7000 シリーズ スイッチは OAL を使用します。

OAL を使用すると、ACL ロギングはハードウェアでサポートされます。OAL では、ハードウェアの packets を許可またはドロップして、スーパーバイザに情報を送信するために最適化されたルーチンを使用し、ロギング メッセージを生成できるようにします。たとえば、パケットがハードウェアで転送される際にそのパケットがロギングを有効にした ACL にヒットした場合、パケットのコピーがハードウェアで作成され、パケットは設定された時間間隔に従ってロギングのためスーパーバイザにパントされます。

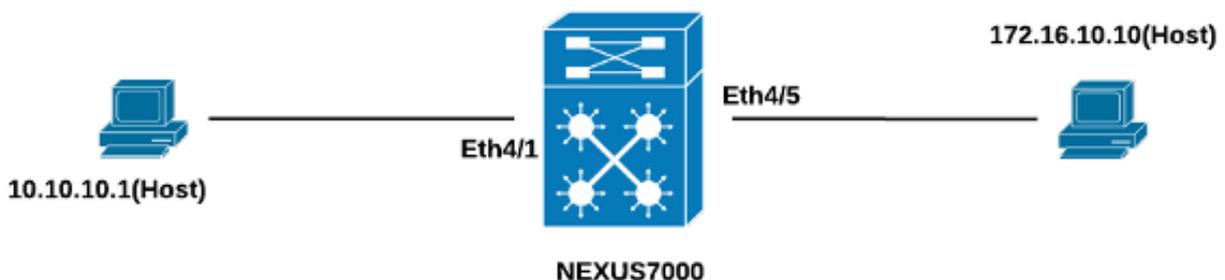
設定

この項では OAL を使用する Nexus スイッチを設定するために使用できる情報を提供します。

この項に記載する例では、IP アドレス 10.10.10.1 のホストが、トラフィックを IP アドレス 172.16.10.10 の別のホストに送信し、その際に ACL のロギングが設定された Nexus 7000 シリーズのインターフェイスを使用します。

ネットワーク図

ホストと Nexus 7000 シリーズのスイッチの間の接続は、次のトポロジに従って発生します。



設定

OAL を使用するようにスイッチを設定するには、次の手順を実行します。

1. OAL を有効にするには、次のグローバル コマンドを設定します。

```
logging ip access-list cache entries 8000
logging ip access-list cache interval 300
logging ip access-list cache threshold 0
```

以下が一例です。

```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

2. ロギングに次の設定を適用します。

```
logging level acllog <number>
acllog match-log-level <number>
logging logfile [name] <number>
```

以下が一例です。

```
Nexus-7000(config)# logging level acllog 5
Nexus-7000(config)# acllog match-log-level 5
Nexus-7000(config)# logging logfile acllog 5
```

3. ロギングを有効にするように ACL を設定します。エントリは、次の例に示すように、log キーワードを有効にして設定する必要があります。

```
Nexus-7000(config)# ip access-list test1
Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
Nexus-7000(config-acl)# 20 deny ip any any log
Nexus-7000(config-acl)#
Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
10 permit ip 10.10.10.1/32 172.16.10.10/32 log
20 deny ip any any log
Nexus-7000(config-acl)#
```

4. 前の手順で設定した ACL を必要なインターフェイスに適用します。

```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)# int ethernet 4/1
Nexus-7000(config-if)# ip access-group test1 in
Nexus-7000(config-if)# ip access-group test1 out
Nexus-7000(config-if)#
Nexus-7000(config-if)# show run int ethernet 4/1
!Command: show running-config interface Ethernet4/1
!Time: Mon Jun 30 16:30:38 2014
version 6.2(6)
interface Ethernet4/1
 ip access-group test1 in
 ip access-group test1 out
 ip address 10.10.10.2/24
 no shutdown
Nexus-7000(config-if)#
```

確認

このセクションに記載されている情報を使用して、設定が適切に機能するか確認します。

このドキュメントで使用する例では、IPアドレス10.10.10.1のホストからIPアドレス

172.16.10.1のホストにpingが開始されます。トラフィックフローを確認するには、CLIでshow logging ip access-list cacheコマンドを入力します。

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
-----
10.10.10.1 172.16.10.10 0 0 Ethernet4/1 (1)ICMP 368
Number of cache entries: 1
-----
```

```
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

300 秒ごとにロギングを確認できますが、これはこれがデフォルトの間隔です。

```
Nexus-7000# show logging logfile
2014 Jun 29 19:19:01 Nexus-7000 %SYSLOG-1-SYSTEM_MSG : Logging logfile (acllog)
cleared by user
2014 Jun 29 19:20:57 Nexus-7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by
admin on console0
2014 Jun 29 19:21:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 2589
2014 Jun 29 19:26:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 4561
```

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

設定の注意事項

この項では、このドキュメントで説明されている設定に関する追加情報を提供します。

詳細な ACL ロギング

Nexus Operating System (NX-OS) リリース 6.2(6)以降では、*詳細な ACL ロギング*を使用できません。この機能は、次の情報を記録します。

- 送信元および宛先 IP アドレス
- 送信元と送信先ポート
- 送信元インターフェイス
- プロトコル
- ACL 名
- ACL のアクション (許可または拒否)
- 適用されたインターフェイス
- パケット数

詳細ロギングを有効にするには、CLI に `logging ip access-list detailed` コマンドを入力します。以下が一例です。

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

詳細ログを有効にした後のログ出力の例を次に示します。

```
2014 Jul 18 02:20:38 Nexus7k-1-oal %ACLLOG-6-ACLLOG_FLOW_INTERVAL: Src IP: 10.10.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/5, Protocol:
"ICMP"(1), ACL Name: test1, ACE Action: Permit, Appl Intf: Ethernet4/5, Hit-count: 69
```

グローバル OAL コマンドの説明

この項では、OAL を使用できるように Nexus 7000 シリーズ スイッチを設定するために使用するグローバル OAL コマンドについて説明します。

コマンド

Switch(config)# logging ip access- list cache {{entries number_of_entries} {interval seconds} このコマンドは OAL グローバル パラメータを設定します。 {rate-limit number_of_packets} {threshold number_of_packets} Switch(config)# no logging ip access- list cache {entries 間隔 rate-limit threshold} entries num_entries interval 秒 threshold num_packets	このコマンドは、OAL グローバル パラメータをデフォルト設定に戻します。 これらのパラメータは、ソフトウェア内にキャッシュされるログ エントリの最大数 これらのパラメータは、エントリが Syslog に送信されるまでの最大時間を指定しま これらのパラメータは、エントリが Syslog に送信されるまでのパケット一致 (ヒッ (レート制限はオフ) です。これは、システムログが一致するパケットの数によっ
--	---

注：次の CLI コマンドの *no form* は、パラメータが変更されている場合にのみデフォルト設定に戻します。Nexus 7000 シリーズ スイッチには、OAL のオプションがあるため、設定は削除されません。

ロギング コマンドの説明

この項では、OAL を使用できるように Nexus 7000 シリーズ スイッチを設定するために使用するロギング コマンドについて説明します。

コマンド

説明

switch(config)#
aclog match-log-
level number このコマンドは、エントリが ACL ログ (aclog) に記録される前に一致している必須
例 : switch(config)# レベルを指定します。範囲は0 ~ 7です。既定値は6です。
aclog match-log-
level 3
Switch(config)# no
aclog match-log-
level number このコマンドはデフォルト設定 (6) にログ レベルを戻します。
例 : switch(config)#
no aclog match-
log- level 6
Switch(config)#
logging level facility このコマンドは、指定された重大度またはそれ以上の重大度である指定のファシリティ
severity-level メッセージを有効にします。このドキュメントで使用する例では、デフォルト設定が
例 : switch(config)# し、aclog レベルは 3 に設定されます。
logging level aclog
3
Switch(config)# no
logging level このコマンドは、指定されたファシリティのロギング重大度をデフォルト レベルに
[facility severity- ファシリティと重大度のレベルを指定しない場合、
level] すべてのファシリティがそれぞれのデフォルト レベルにリセットされます。このド
例 : switch(config)# する例では、aclog はデフォルト (2) に戻ります。
no logging level
aclog 3
Switch(config)#
logging logfile
logfile-name このコマンドは、ロギングが発生する前に、システム メッセージと最小の重大度を
severity-level [size 用されるログ ファイルの名前を設定します。任意で最大ファイル サイズを指定でき
bytes] の重大度は 5 です。デフォルトのファイル サイズは 10,485,760 です。
例 : switch(config)#
logging logfile
aclog 3
Switch(config)# no
logging logfile
[logfile-name
severity-level [size このコマンドは、ログ ファイルへのロギングを無効にします。
bytes]]
例 : switch(config)#
no logging logfile
aclog 3

注 : ログ メッセージがログに入力されるためには、ACL ログ ファシリティ (aclog) のロ
グ レベルとログ ファイルのロギング重大度が、ACL ログの *match-log-level* 設定よりも大
きいが、同じでなければなりません。

注意事項と制約事項

このドキュメントで説明した設定を適用する前に、考慮する必要がある重要なガイドラインと制
限を次に示します。

- Nexus 7000 および 7700 シリーズ スイッチは OAL のみサポートします。
- ACL ログイングは、ACL キャプチャ機能を使用しません。
- 出力 ACL の *log* オプションはマルチキャスト パケットではサポートされません。
- 詳細なログイングのサポートは、IPv6 パケットでは利用できません。
- *aclog* ファシリティのログ レベルとログファイルのログイングの重大度は、*aclog match-log-level* の設定よりも大きいか等しくなるように設定する必要があります。
- OALの使用中は**hardware access-list capture**コマンドを使用しないでください。このコマンドをOALとともに使用してACLキャプチャを有効にすると、すべての仮想デバイスコンテキスト(VDC)でACLログイングが無効になっていることが警告メッセージで通知されます。ACLキャプチャをディセーブルにすると、ACL ログイングはイネーブルになります。このプロセスが正しく動作するには、**no hardware access-list capture** コマンドの使用を無効にします。