Nexus 7000 シリーズ スイッチの ACL キャプチャの例

内容

概要

アクセスコントロールリスト(ACL)キャプチャは、インターフェイスまたは仮想ローカルエリアネットワーク(VLAN)上のトラフィックを選択的にキャプチャする機能を提供します。ACLルールのキャプチャオプションを有効にすると、指定した許可または拒否アクションに基づいてパケットが転送または廃棄されます。

1. VLAN 内、
2. すべてのインターフェイス上の入力方向、
3. すべてのレイヤ 3 インターフェイス上の出力方向。

この機能は、Nexus 7000 NX-OSリリース5.2以降でサポートされています。このドキュメントでは、この機能の設定方法に関するクイックリファレンスガイドとして例を示します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

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

- リリース 5.2 以降の Nexus 7000
- M1 シリーズ ライン カード

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ACL の設定例

VLAN に適用される ACL キャプチャ（仮想 LAN アクセス コントロール リスト（VACL）キャプチャとも呼ばれる）の設定例を示します。指定された 10 ギガビット スニファは、すべてのシナリオには実行できない場合があります。選択的なトラフィックのキャプチャは、特にトラフィック量が多い場合のトラブルシューティングでのシナリオなどに非常に役立ちます。

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

アクセス リストの Ternary Content Addressable Memory（TCAM）プログラムもチェックできます。この出力はモジュール 1 の VLAN 500 用です。

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot 1
=======

INSTANCE 0x0
---------------

Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
```

```
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

警告

1. 仮想デバイス コンテキスト（VDC）全体でシステムで同時にアクティブにできる ACL キャプチャ セッションは 1 つのみです。
2. Nexus 7000 F1 シリーズ モジュールは、ACL キャプチャをサポートしていません。
3. Nexus 7000 F2 シリーズ モジュールは、現在 ACL キャプチャをサポートしていませんが、これがロードマップになる場合もあります。
4. Nexus 7000 M2 シリーズ モジュールの ACL キャプチャは、Cisco NX-OS リリース 6.1(1) 以降でサポートされています。
5. Nexus 7000 M1 シリーズ モジュールの ACL キャプチャは、Cisco NX-OS リリース 5.2(1) 以降でサポートされています。
6. ACL キャプチャは、ACL ロギングと互換性がありません。 そのため、**log キーワードが含まれる ACL がある場合、hardware access-list capture** をグローバルに入力するとこれらは機能しません。
7. バグ CSCug20139のため、このドキュメントの例は、バグが解決されるまで ACL ではなく ACE あたりの **capture session で記載されます。**

関連情報

- Cisco Nexus 7000 シリーズ NX-OS セキュリティ設定ガイド、リリース 6.x、IP ACL の設定例
- テクニカル サポートとドキュメント – Cisco Systems