

VACL キャプチャに対するフローベースのスパン代替

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[手順](#)

[制約事項](#)

[関連情報](#)

概要

このドキュメントでは、フローベースのスイッチドポートアナライザ (FSPAN) を使用して、VLAN Access Control List (VACL) のキャプチャをサポートしていない Cisco Catalyst スイッチでフィルタリングされたトラフィックをキャプチャする方法について説明します。

前提条件

要件

このドキュメントに関しては個別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くものです。

- Cisco Catalyst 3750-X シリーズ スイッチ
- Cisco Catalyst 3560-X シリーズ スイッチ
- Cisco Catalyst 3750-E シリーズ スイッチ
- Cisco Catalyst 3560-E シリーズ スイッチ
- Cisco Catalyst 2960-X シリーズ スイッチ iplite ライセンスを実行する
- Cisco IOS[®] リリース 12.2(44)SE 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用され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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ

さい。

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。

手順

Cisco Catalyst 3750-X、3560-X、3750-E、3560-E および 2960-X (iplite ライセンス) スイッチは VACL キャプチャをサポートしません; ただし、これらのスイッチは、フローベースの SPAN およびフローベースのリモート SPAN (RSPAN) をサポートしています。この RSPAN では、VACL キャプチャと同様の結果を実現できます。

フローベースの SPAN は、指定したフィルタを使用して、エンドホスト間で必要なデータをキャプチャするメカニズムを提供します。

SPAN セッションには、次の 3 種類の FSPAN アクセスコントロールリスト (ACL) を接続できます。

- IPv4 FSPAN ACL : IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL : IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL : 非 IP パケットだけをフィルタリングします。

セキュリティ ACL は、スイッチの FSPAN ACL よりも優先されます。FSPAN ACL を適用し、ハードウェアメモリに保存できないセキュリティ ACL をさらに追加した場合は、セキュリティ ACL のスペースを確保するために、FSPAN ACL がメモリから除外されます。この処理 (アンロードと呼ばれる) は、システムメッセージによりユーザに通知されます。

スペースが再び使用可能になると、FSPAN ACL は、スイッチのハードウェアメモリに再び追加されます。この処理 (リロードと呼ばれる) は、システムメッセージによりユーザに通知されます。

3750-X スイッチがサポートする SPAN セッションは 2 つまでで、FSPAN では、この制限を回避できません。FSPAN は、通常の SPAN と同じ複製 ASIC を使用します。

次に示すのは、3750-X スイッチでの FSPAN の使用例です。

```
3750X(config)#ip access-list extended FILTER
3750X(config-ext-nacl)#permit ip host 192.168.1.1 host 172.16.1.1
3750X(config-ext-nacl)#exit
3750X(config)#monitor session 1 source interface gil/0/1 both3750X
(config)#monitor session 1 destination interface gil/0/2 3750X
(config)#monitor session 1 filter ip access-group FILTER
```

```
3750X(config)##exit3750X#show monitor session
sh mon session 1
Session 1
-----
Type                : Local Session
Source Ports        :
Both                : Gil/0/1Destination Ports      : Gil/0/2
Encapsulation       : Native
```

Ingress : Disabled
IP Access-group : FILTER

制約事項

- FSPAN は 3750 で、3750G、2950、2960 および 2960-S スイッチ サポートされません。
- iplite ライセンスを実行する 2960-X は FSPAN だけをサポートします。
- ACL は、一度に 1 つの SPAN または RSPAN にしか接続できません。
- FSPAN ACL が接続されていない場合、FSPAN はディセーブルで、すべてのトラフィックが SPAN 宛先ポートにコピーされます。
- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空の FSPAN ACL を接続すると、パケットはフィルタリングされず、すべてのトラフィックが監視されます。
- Catalyst 3750 ポートは、FSPAN セッション内の宛先ポートとして追加できます。
- VLAN ベースの FSPAN セッションは、Catalyst 3750 スイッチを含むスタックでは設定できません。
- EtherChannel は FSPAN セッションではサポートされていません。
- TCP フラグまたは log キーワードが付いている FSPAN ACL はサポートされていません。
- ポートベースの FSPAN セッションは、Catalyst 3750-E ポートだけが送信元ポートとしてセッションに含まれている場合に限り、Catalyst 3750 スイッチを含むスタックで設定できます。Catalyst 3750 ポートが送信元ポートとしてセッションに含まれている場合、FSPAN ACL コマンドは拒否されます。

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)