Flow-Based SPAN Alternative zur VACL-Erfassung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ein FSPAN (Flow-Based Switched Port Analyzer) verwendet wird, um gefilterten Datenverkehr auf Cisco Catalyst Switches zu erfassen, die keine VACL-Erfassung (VLAN Access Control List) unterstützen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst Switches der Serie 3750-X
- Cisco Catalyst Switches der Serie 3560-X
- Cisco Catalyst Switches der Serie 3750-E
- Cisco Catalyst Switches der Serie 3560-E
- Cisco Catalyst Switches der Serie 2960-X mit IP-Lizenz
- Cisco IOS® Version 12.2(44)SE und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Vorgehensweise

Cisco Catalyst Switches der Serien 3750-X, 3560-X, 3750-E, 3560-E und 2960-X (optionale Lizenz) unterstützen keine VACL-Erfassung. Diese Switches unterstützen jedoch ein Flow-Based SPAN und ein Flow-Based Remote SPAN (RSPAN), was ähnliche Ergebnisse wie die VACL-Erfassung erzielen kann.

Flow-Based SPAN stellt einen Mechanismus bereit, mit dem bestimmte Filter verwendet werden, um erforderliche Daten zwischen Endhosts zu erfassen.

Sie können der SPAN-Sitzung drei Typen von FSPAN-Zugriffskontrolllisten (ACLs) hinzufügen:

- IPv4 FSPAN ACL - Filtert nur IPv4-Pakete.
- IPv6 FSPAN ACL: Nur IPv6-Pakete werden gefiltert.
- MAC FSPAN ACL - Filtert nur Nicht-IP-Pakete.

Sicherheitszugriffskontrolllisten haben eine höhere Priorität als FSPAN-Zugriffskontrolllisten auf einem Switch. Wenn Sie FSPAN-ACLs anwenden und dann weitere Sicherheits-ACLs hinzufügen, die nicht in den Hardwarespeicher passen, werden die FSPAN-ACLs aus dem Speicher entfernt, um Platz für die Sicherheits-ACLs zu schaffen. Eine Systemmeldung benachrichtigt den Benutzer über diese Aktion, die als Entladen bezeichnet wird.

Wenn wieder Speicherplatz verfügbar ist, werden die FSPAN-ACLs wieder dem Hardwarespeicher des Switches hinzugefügt. Eine Systemmeldung benachrichtigt den Benutzer über diese Aktion, die als Neloading bezeichnet wird.

Die Switches der Serie 3750-X unterstützen bis zu zwei SPAN-Sitzungen, was FSPAN nicht vermeiden kann. FSPAN verwendet denselben Replizierungs-ASIC wie ein reguläres SPAN.

Dies ist ein Beispiel für die Verwendung von FSPAN auf einem 3750-X-Switch:

```
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 gi1/0/1 both3750X
(config)#monitor session 1 destination interface gi1/0/2 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               : Gi1/0/1Destination Ports      : Gi1/0/2
   Encapsulation      : Native
         Ingress      : Disabled
IP Access-group        : FILTER
```

Einschränkungen

- FSPAN wird von Switches der Serien 3750, 3750G, 2950, 2960 und 2960-S nicht unterstützt.
- 2960-X, der die IP-Lizenz ausführt, unterstützt nur FSPAN.
- Sie können ACLs jeweils nur an eine SPAN- oder RSPAN-Sitzung anschließen.
- Wenn keine FSPAN-ACLs angeschlossen sind, ist FSPAN deaktiviert, und der gesamte Datenverkehr wird in die SPAN-Zielports kopiert.
- Wenn mindestens eine FSPAN-ACL angeschlossen ist, ist FSPAN aktiviert.
- Wenn Sie eine leere FSPAN-ACL an eine SPAN-Sitzung anschließen, werden keine Pakete gefiltert, und der gesamte Datenverkehr wird überwacht.
- In einer FSPAN-Sitzung können Catalyst 3750-Ports als Zielports hinzugefügt werden.
- VLAN-basierte FSPAN-Sitzungen können nicht auf einem Stack konfiguriert werden, der Catalyst 3750-Switches umfasst.
- EtherChannels werden in einer FSPAN-Sitzung nicht unterstützt.
- FSPAN-ACLs mit TCP-Flags oder dem **log-**Schlüsselwort werden nicht unterstützt.
- Port-basierte FSPAN-Sitzungen können auf einem Stack konfiguriert werden, der Catalyst 3750-Switches umfasst, sofern die Sitzung nur Catalyst 3750-E-Ports als Quell-Ports umfasst. Wenn die Sitzung über Catalyst 3750-Ports als Quell-Ports verfügt, wird der Befehl FSPAN ACL abgelehnt.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems