VACL-Erfassung für detaillierte Datenverkehrsanalysen mit Cisco Catalyst 6000/6500 mit Cisco IOS-Software

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Verwendung der Funktion zum Erfassen des VLAN-ACL-Ports (VACL) für eine detailliertere Analyse des Netzwerkverkehrs. In diesem Dokument werden auch die Vorteile der Verwendung von VACL-Erfassungsports im Vergleich zur VLAN-basierten SPAN-Nutzung (VSPAN) erläutert.

Informationen zur Konfiguration der VACL-Capture-Port-Funktion auf Cisco Catalyst 6000/6500, die Catalyst OS-Software ausführt, finden Sie unter VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running CatOS Software.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- IP-Zugriffslisten: Weitere Informationen finden Sie unter Konfigurieren von IP-Zugriffslisten.
- Virtuelles LAN: Weitere Informationen finden Sie unter Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) - Einführung.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen: Cisco Catalyst Switches der Serie 6506 mit Cisco IOS® Softwareversion 12.2(18)SXF8

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit Cisco Catalyst Switches der Serien 6000/6500 verwendet werden, auf denen die Cisco IOS Software Version 12.1(13)E und höher ausgeführt wird.

Konventionen

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

Hintergrundinformationen

VLAN-basiertes SPAN

SPAN (Switched Port ANalyzer) kopiert den Datenverkehr von einem oder mehreren Quell-Ports in einem VLAN oder von einem oder mehreren VLANs zur Analyse an einen Zielport. Das lokale SPAN unterstützt Quellports, Quell-VLANs und Zielports auf demselben Catalyst Switch der Serie 6500.

Ein Quell-VLAN ist ein VLAN, das für die Analyse des Netzwerkverkehrs überwacht wird. VLAN-basiertes SPAN (VSPAN) verwendet ein VLAN als SPAN-Quelle. Alle Ports in den Quell-VLANs werden zu Quell-Ports. Ein Quellport ist ein Port, der für die Analyse des Netzwerkverkehrs überwacht wird. Trunk-Ports können als Quell-Ports konfiguriert und mit Nicht-Trunk-Quell-Ports gemischt werden, SPAN kopiert die Kapselung jedoch nicht von einem Quell-Trunk-Port.

Bei VSPAN-Sitzungen mit sowohl Eingang als auch Ausgang werden zwei Pakete vom Zielport weitergeleitet, wenn die Pakete im gleichen VLAN geschaltet werden (eines als Eingangs- und Ausgangs-Datenverkehr vom Eingangsport und eines als Ausgangs-Datenverkehr vom Ausgangs-Port).

Das VSPAN überwacht nur den Datenverkehr, der Layer-2-Ports im VLAN verlässt oder eingeht.

- Wenn Sie ein VLAN als Eingangs-Quelle konfigurieren und der Datenverkehr in das überwachte VLAN weitergeleitet wird, wird der geroutete Datenverkehr nicht überwacht, da er

nie als Eingangs-Datenverkehr angezeigt wird, der in einen Layer-2-Port im VLAN eingeht.
- Wenn Sie ein VLAN als Ausgangsquelle konfigurieren und der Datenverkehr aus dem überwachten VLAN weitergeleitet wird, wird der geroutete Datenverkehr nicht überwacht, da er nie als Ausgangsverkehr angezeigt wird, der einen Layer-2-Port im VLAN verlässt.

Weitere Informationen zu Quell-VLANs finden Sie unter Merkmale des Quell-VLANs.

VLAN-ACL

VACLs können die Zugriffskontrolle für alle Pakete bereitstellen, die innerhalb eines VLAN überbrückt werden, in ein oder aus einem VLAN oder einer WAN-Schnittstelle geroutet werden, um die VACL-Erfassung zu ermöglichen. Im Gegensatz zu regulären Cisco IOS-Standard- oder erweiterten ACLs, die nur auf Router-Schnittstellen konfiguriert sind und nur auf geroutete Pakete angewendet werden, gelten VACLs für alle Pakete und können auf alle VLAN- oder WAN-Schnittstellen angewendet werden. VACLs werden in der Hardware verarbeitet. VACLs verwenden Cisco IOS ACLs. VACLs ignorieren alle Cisco IOS ACL-Felder, die nicht von der Hardware unterstützt werden.

Sie können VACLs für IP-, IPX- und MAC-Layer-Datenverkehr konfigurieren. Die auf WAN-Schnittstellen angewendeten VACLs unterstützen nur IP-Datenverkehr zur VACL-Erfassung.

Wenn Sie eine VACL konfigurieren und auf ein VLAN anwenden, werden alle im VLAN eingehenden Pakete mit dieser VACL abgeglichen. Wenn Sie eine VACL auf das VLAN und eine ACL auf eine geroutete Schnittstelle im VLAN anwenden, wird ein im VLAN eingehendes Paket zuerst mit der VACL abgeglichen und, falls zulässig, mit der Eingabe-ACL abgeglichen, bevor es von der gerouteten Schnittstelle verarbeitet wird. Wenn das Paket an ein anderes VLAN weitergeleitet wird, wird es zuerst mit der auf die geroutete Schnittstelle angewendeten Ausgabe-ACL überprüft, und, falls zulässig, mit der für das Ziel-VLAN konfigurierten VACL. Wenn eine VACL für einen Pakettyp konfiguriert ist und ein Paket dieses Typs nicht mit der VACL übereinstimmt, wird die Standardaktion abgelehnt. Dies sind die Richtlinien für die Erfassungsoption in VACL.

- Der Erfassungsport darf kein ATM-Port sein.
- Der Erfassungsport muss sich im Spanning-Tree-Weiterleitungsstatus für das VLAN befinden.
- Der Switch hat keine Einschränkung hinsichtlich der Anzahl der Erfassungsports.
- Der Erfassungsport erfasst nur Pakete, die von der konfigurierten ACL zugelassen sind.
- Capture-Ports übertragen nur Datenverkehr, der zum Capture-Port-VLAN gehört. Konfigurieren Sie den Erfassungsport als Trunk, der die erforderlichen VLANs überträgt, um Datenverkehr zu vielen VLANs zu erfassen.

Vorsicht: Eine falsche Kombination von ACLs kann den Datenverkehrsfluss stören. Seien Sie besonders vorsichtig, wenn Sie die ACLs in Ihrem Gerät konfigurieren.

Hinweis: VACL wird auf einem Catalyst Switch der Serie 6000 nicht von IPv6 unterstützt. Mit anderen Worten: Die Umleitung der VLAN-ACLs und IPv6 sind nicht kompatibel, sodass die ACL nicht für den IPv6-Datenverkehr verwendet werden kann.

Vorteile der VACL-Nutzung gegenüber der VSPAN-Nutzung

Die VSPAN-Nutzung für die Datenverkehrsanalyse unterliegt mehreren Einschränkungen:

- Der gesamte Layer-2-Datenverkehr, der in einem VLAN fließt, wird erfasst. Dies erhöht die

Menge der zu analysierenden Daten.
- Die Anzahl der SPAN-Sitzungen, die auf den Catalyst Switches der Serie 6500 konfiguriert werden können, ist begrenzt. Weitere Informationen finden Sie unter Lokale SPAN- und RSPAN-Sitzungsbeschränkungen.
- Ein Zielport empfängt Kopien von gesendetem und empfangenen Datenverkehr für alle überwachten Quell-Ports. Wenn ein Zielport überbelegt ist, kann dieser überlastet werden. Diese Überlastung kann die Weiterleitung des Datenverkehrs an einem oder mehreren Quellports beeinträchtigen.

Die Funktion "VACL Capture Port" kann dabei helfen, einige dieser Einschränkungen zu überwinden. VACLs sind in erster Linie nicht für die Überwachung des Datenverkehrs konzipiert, aber mit einer breiten Palette von Funktionen zur Klassifizierung des Datenverkehrs wurde die Capture Port-Funktion eingeführt, um die Analyse des Netzwerkverkehrs zu vereinfachen. Dies sind die Vorteile der VACL Capture Port-Nutzung gegenüber VSPAN:

- Präzise DatenverkehrsanalyseVACLs können auf Basis der Quell-IP-Adresse, der Ziel-IP-Adresse, des Layer-4-Protokolltyps, der Quell- und Ziel-Layer-4-Ports und anderer Informationen übereinstimmen. Diese Funktion macht VACLs sehr nützlich für die präzise Identifizierung und Filterung von Datenverkehr.
- Anzahl der SitzungenVACLs werden in der Hardware durchgesetzt. Die Anzahl der ACE-Einträge (Access Control Entries), die erstellt werden können, hängt von dem in den Switches verfügbaren TCAM ab.
- Überbelegung des ZielportsDie präzise Identifizierung des Datenverkehrs verringert die Anzahl der Frames, die an den Zielport weitergeleitet werden, und minimiert so die Wahrscheinlichkeit einer Überbelegung.
- LeistungVACLs werden in der Hardware durchgesetzt. Bei der Anwendung von VACLs auf ein VLAN der Cisco Catalyst Switches der Serie 6500 treten keine Leistungseinbußen auf.

Konfigurieren

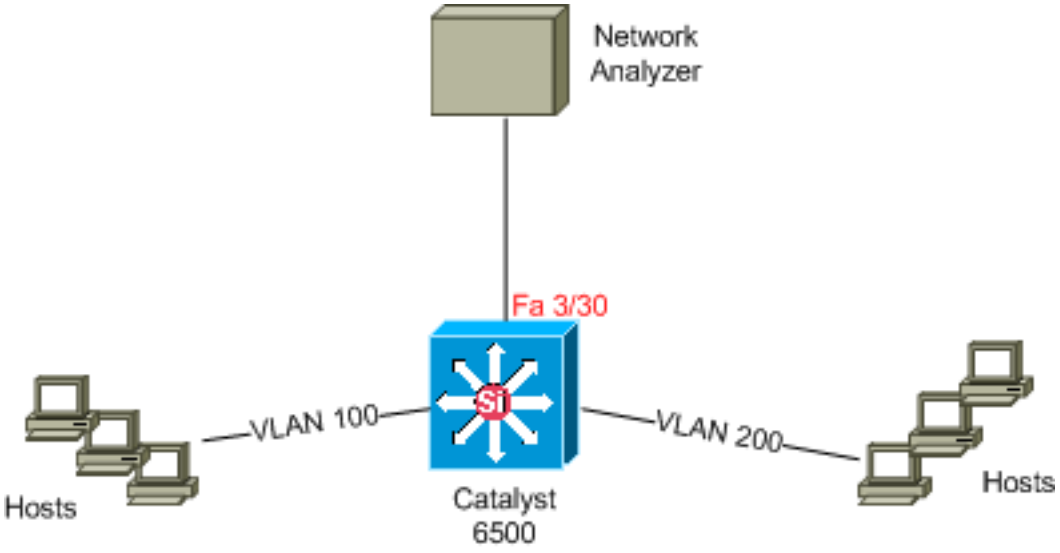
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

- Konfiguration mit VLAN-basiertem SPAN
- Konfigurieren mit VACL

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration mit VLAN-basiertem SPAN

In diesem Konfigurationsbeispiel werden die erforderlichen Schritte aufgelistet, um den gesamten Layer-2-Datenverkehr zu erfassen, der in VLAN 100 und VLAN 200 fließt, und diese an das Network Analyzer-Gerät zu senden.

1. Geben Sie den interessanten Datenverkehr an. In unserem Beispiel fließt der Datenverkehr in VLAN 100 und VLAN 200.

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

 !--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. Geben Sie den Zielport für den erfassten Datenverkehr an.

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

Dadurch wird der gesamte Layer-2-Datenverkehr, der zu VLAN 100 und VLAN 200 gehört, kopiert und an Port Fa3/30 gesendet. Wenn der Zielport Teil desselben VLAN ist, dessen Datenverkehr überwacht wird, wird der Datenverkehr, der vom Zielport ausgeht, nicht erfasst.

Überprüfen Sie Ihre SPAN-Konfiguration mit dem Befehl **show monitor**.

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
    RX Only        : None
```

```
    TX Only        : None
    Both           : 100,200
Source RSPAN VLAN  : None
Destination Ports  : Fa3/30
Filter VLANs       : None
Dest RSPAN VLAN    : None
```

Konfiguration mit VACL

In diesem Konfigurationsbeispiel gibt es mehrere Anforderungen des Netzwerkadministrators:

- HTTP-Datenverkehr von einem Hosts (10.20.20.128/25) in VLAN 200 zu einem bestimmten Server (10.10.10.101) in VLAN 100 muss erfasst werden.
- Der Multicast User Datagram Protocol (UDP)-Datenverkehr in der Übertragungsrichtung, der für die Gruppenadresse 239.0.0.100 bestimmt ist, muss aus VLAN 100 erfasst werden.

1. Definieren Sie den interessanten Datenverkehr, der erfasst und zur Analyse gesendet werden soll.
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```
2. Definieren Sie eine übergeordneten ACL, um den gesamten anderen Datenverkehr zuzuordnen.
```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```
3. Definieren Sie die VLAN-Zugriffskarte.
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```
4. Wenden Sie die VLAN-Zugriffskarte auf die entsprechenden VLANs an.
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```
5. Konfigurieren Sie den Capture-Port.
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle.

Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show vlan access-map** - Zeigt den Inhalt der VLAN Access Maps an.

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter**: Zeigt Informationen zu den VLAN-Filtern an.

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- VACL-Erfassung für detaillierte Datenverkehrsanalysen mit Cisco Catalyst 6000/6500 mit CatOS-Software
- Unterstützung für Cisco Catalyst Switches der Serie 6500
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems