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

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Verwendung der Funktion "Capture Port" (VACL) für die VLAN Access Control List (ACL)-Erfassung für eine detailliertere Analyse des Netzwerkverkehrs. In diesem Dokument werden auch die Vorteile der Verwendung von VACL-Erfassungsports im Vergleich zur VLAN-basierten Nutzung von Switched Port Analyzer (SPAN) (VSPAN) beschrieben.

Um die Funktion für den VACL-Erfassungsport auf dem Cisco Catalyst 6000/6500 zu konfigurieren, auf dem die Cisco IOS®-Software ausgeführt wird, lesen Sie VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running Cisco IOS Software.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese

Konfiguration durchzuführen:

- Virtual LAN - Weitere Informationen finden Sie unter Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) - Einführung.
- Zugriffslisten - Weitere Informationen finden Sie unter Konfigurieren der Zugriffskontrolle.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Catalyst Switch der Serie 6506, auf dem Catalyst OS 8.1(2) ausgeführt wird.

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, die Catalyst OS 6.3 oder höher ausführen.

Konventionen

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

Hintergrundinformationen

VLAN-basiertes SPAN

SPAN kopiert den Datenverkehr von einem oder mehreren Quell-Ports in einem VLAN oder von einem oder mehreren VLANs zu einem Ziel-Port zur Analyse. Das lokale SPAN unterstützt Quellports, Quell-VLANs und Zielports auf demselben Catalyst Switch der Serie 6500.

Ein Quellport ist ein Port, der für die Analyse des Netzwerkverkehrs überwacht wird. Ein Quell-VLAN ist ein VLAN, das für die Analyse des Netzwerkverkehrs überwacht wird. VLAN-basiertes SPAN (VSPAN) ist eine Analyse des Netzwerkverkehrs in einem oder mehreren VLANs. Sie können VSPAN als Eingangs-SPAN, Ausgangs-SPAN oder beides konfigurieren. Alle Ports in den Quell-VLANs werden zu den betrieblichen Quell-Ports für die VSPAN-Sitzung. Die Zielports, die zu einem der VLANs der administrativen Quelle gehören, sind von der operativen Quelle ausgeschlossen. Wenn Sie Ports zu den VLANs der administrativen Quelle hinzufügen oder daraus entfernen, werden die operativen Quellen entsprechend geändert.

Richtlinien für VSPAN-Sitzungen:

- Die Trunk-Ports sind als Quell-Ports für die VSPAN-Sitzungen enthalten, aber nur die VLANs, die sich in der Admin-Quellliste befinden, werden überwacht, wenn diese VLANs für den Trunk aktiv sind.
- Für die VSPAN-Sitzungen mit konfiguriertem Eingangs- und Ausgangs-SPAN wird das

System basierend auf dem Typ der Supervisor Engine betrieben, über den Sie verfügen:WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-SUP720, WS-SUP32-GE-3B - Zwei Pakete werden von der weitergeleitet SPAN-Zielport, wenn die Pakete im selben VLAN geschaltet werden.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE - Nur ein Paket wird vom SPAN-Zielport weitergeleitet.

- Ein In-Band-Port ist nicht als Operative Quelle für die VSPAN-Sitzungen enthalten.
- Wenn ein VLAN gelöscht wird, wird es aus der Quellliste für die VSPAN-Sitzungen entfernt.
- Eine VSPAN-Sitzung wird deaktiviert, wenn die Liste der Admin-Quell-VLANs leer ist.
- Die inaktiven VLANs sind für die VSPAN-Konfiguration nicht zulässig.
- Eine VSPAN-Sitzung ist inaktiv, wenn eines der Quell-VLANs zu den RSPAN-VLANs wird.

Weitere Informationen zu Quell-VLANs finden Sie in den Eigenschaften des Quell-VLANs.

VLAN-ACL

Die VACLs können auf die Steuerung des gesamten Datenverkehrs zugreifen. Sie können die VACLs auf dem Switch so konfigurieren, dass sie auf alle Pakete angewendet werden, die in ein oder aus einem VLAN geroutet oder innerhalb eines VLAN überbrückt werden. Die VACLs dienen ausschließlich der Filterung von Sicherheitspaketen und leiten den Datenverkehr an bestimmte physische Switch-Ports weiter. Im Gegensatz zu den Cisco IOS ACLs sind die VACLs nicht durch Richtung (Eingang oder Ausgang) definiert.

Sie können die VACLs auf den Layer-3-Adressen für IP und IPX konfigurieren. Alle anderen Protokolle werden über die MAC-Adressen und den EtherType mithilfe der MAC-VACLs gesteuert. Der IP- und IPX-Datenverkehr werden nicht von den MAC-VACLs gesteuert. Alle anderen Datenverkehrstypen (AppleTalk, DECnet usw.) werden als MAC-Datenverkehr klassifiziert. Die MAC-VACLs werden für den Zugriff auf diesen Datenverkehr verwendet.

In VACLs unterstützte ACEs

VACL enthält eine geordnete Liste von Zugriffskontrolleinträgen (ACEs). Jede VACL kann ACEs nur eines Typs enthalten. Jeder ACE enthält eine Reihe von Feldern, die dem Inhalt eines Pakets zugeordnet sind. Jedes Feld kann eine zugeordnete Bitmaske haben, um anzugeben, welche Bits relevant sind. Jedem ACE ist eine Aktion zugeordnet, die beschreibt, was das System mit dem Paket tun sollte, wenn eine Übereinstimmung auftritt. Die Aktion hängt von den Funktionen ab. Die Catalyst Switches der Serie 6500 unterstützen drei Typen von ACEs in der Hardware:

- IP-ACEs
- IPX-ACEs
- Ethernet-ACEs

In dieser Tabelle sind die Parameter aufgeführt, die jedem ACE-Typ zugeordnet sind:

ACE-Typ	TCP oder UDP	ICMP	Andere IP	IPX	Ethernet
Layer-4-Parameter	Quell-Port	-	-	-	-
	Quell-Port-Operator	-	-	-	-
	Zielport	-	-	-	-

	Ziel-Port-Operator	ICMP-Code	-	-	-
	K/A	ICMP-Typ	K/A	-	-
Layer-3-Parameter	IP-ToS-Byte	IP-ToS-Byte	IP-ToS-Byte	-	-
	IP-Quelladresse	IP-Quelladresse	IP-Quelladresse	IPX-Quellnetzwerk	-
	IP-Zieladresse	IP-Zieladresse	IP-Zieladresse	IP-Zielnetzwerk	-
	-	-	-	IP-Zielknoten	-
	TCP oder UDP	ICMP	Anderes Protokoll	IPX-Pakettyp	-
Layer-2-Parameter	-	-	-	-	EtherType
	-	-	-	-	Ethernet-Quelladresse
	-	-	-	-	Ethernet-Zieladresse

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 Funktionsübersicht und Einschränkungen.
- 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. Da der Datenverkehr jedoch über eine Vielzahl von Funktionen klassifiziert werden kann, wurde die Funktion "Capture Port" 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 ACEs, 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.

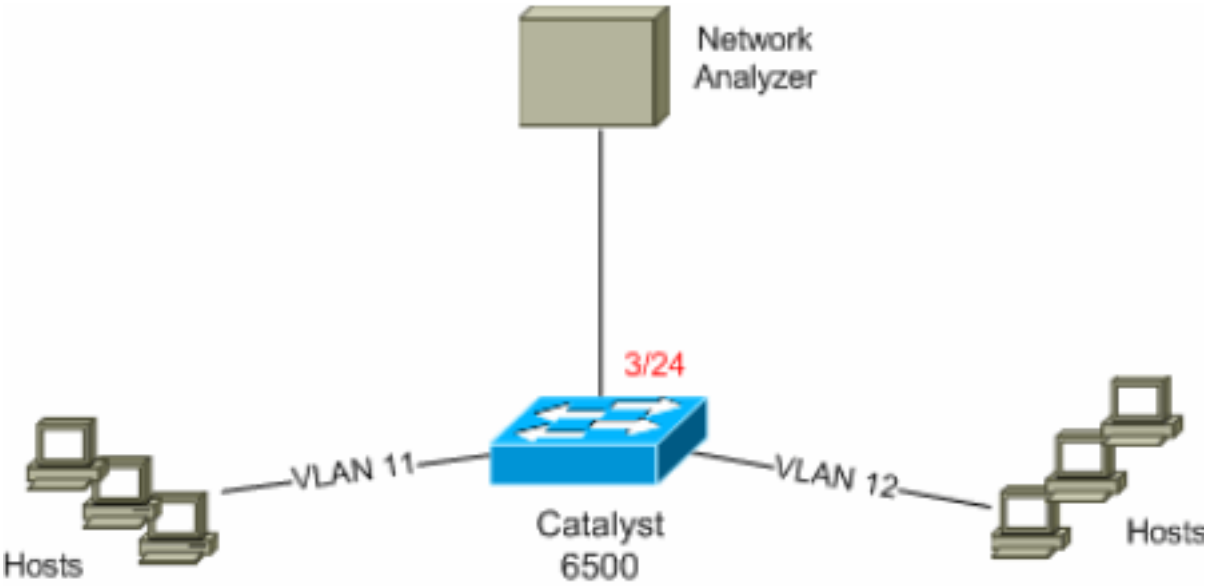
In diesem Dokument werden folgende Konfigurationen verwendet:

- Konfiguration mit VLAN-basiertem SPAN
- Konfiguration mit VACL

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt 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 11 und VLAN 12 fließt, und diese an das Network Analyzer-Gerät zu senden.

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

```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```

   Dadurch wird der gesamte Layer-2-Datenverkehr, der zu VLAN 11 und VLAN 12 gehört, kopiert und an Port 3/24 gesendet.
2. Überprüfen Sie Ihre SPAN-Konfiguration mit dem Befehl **show span all**.

```
6K-CatOS> (enable) show span all

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

Konfiguration mit VACL

In diesem Konfigurationsbeispiel gibt es mehrere Anforderungen des Netzwerkadministrators:

- HTTP-Datenverkehr von einem Hosts (10.12.12.128/25) in VLAN 12 zu einem bestimmten Server (10.11.11.100) in VLAN 11 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 11 erfasst werden.

1. Definieren Sie den interessanten Datenverkehr mithilfe der Sicherheits-ACLs. Denken Sie daran, das Schlüsselwort **capture** für alle definierten ACEs zu erwähnen.

```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
host 239.0.0.100 capture
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. Überprüfen Sie, ob die ACE-Konfiguration korrekt und in der richtigen Reihenfolge ist.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. Übernehmen Sie die ACL der Hardware.

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. Überprüfen Sie den Status der ACL.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. Wenden Sie die VLAN-Zugriffskarte auf die entsprechenden VLANs an.

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                   Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. Überprüfen der Zuordnung von ACL zu VLAN

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. Konfigurieren Sie den Erfassungsport.

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

Hinweis: Wenn eine ACL mehreren VLANs zugeordnet ist, muss der Erfassungsport für alle VLANs konfiguriert werden. Damit der Erfassungsport mehrere VLANs zulässt, konfigurieren Sie den Port als Trunk, und lassen Sie nur die der ACL zugeordneten VLANs zu. Wenn die ACL beispielsweise den VLANs 11 und 12 zugeordnet ist, schließen Sie die Konfiguration ab.

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. Überprüfen Sie die Konfiguration des Erfassungsports.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

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 security acl info**: Zeigt den Inhalt der VACL an, die aktuell konfiguriert sind oder zuletzt für den NVRAM und die Hardware übernommen wurden.
```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```
- **show security acl map**: Zeigt die Zuordnung von ACL zu VLAN oder von ACL zu Port für eine bestimmte ACL, einen bestimmten Port oder ein bestimmtes VLAN an.
```
6K-CatOS> (enable) show security acl map all
ACL Name                        Type Vlans
------------------------------- ---- -----
HttpUdp_Acl                        IP   11
6K-CatOS> (enable)
```
- **show security acl capture-ports**: Zeigt die Liste der Capture-Ports an.
```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

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 Cisco IOS-Software
- Konfigurieren der Zugriffskontrolle - Catalyst Software Configuration Guide 6500, 8.6
- Support-Seiten für LAN-Produkte
- Support-Seite für LAN-Switching
- Technischer Support und Dokumentation - Cisco Systems