VACL-opname voor granulaire verkeersanalyse met Cisco Catalyst 6000/6500 actieve Cisco IOS-software

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het gebruik van de eigenschappen van de VACL-poort (VLAN ACL) voor de analyse van het netwerkverkeer op een meer granulaire manier. In dit document wordt ook het voordeel aangegeven van het VACL-opnamepoortgebruik in tegenstelling tot het VLAN-gebaseerde SPAN-gebruik (VSPAN).

Om de VACL-opnamepoortfunctie op Cisco Catalyst 6000/6500 te configureren die Catalyst OS-software draait, raadpleegt u VACL-opname voor granulaire verkeersanalyse met Cisco Catalyst 6000/6500 actieve CatOS-software.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- IP-toegangslijsten: Raadpleeg IP-toegangslijsten configureren voor meer informatie.
- Virtueel LAN: Raadpleeg het Virtual LANs/VLAN Trunking Protocol (VLAN's/VTP) - Inleiding voor meer informatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies: Cisco Catalyst 6506 Series Switch met Cisco IOS® softwarerelease 12.2(18)SXF8.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco Catalyst 6000/6500 Series Switches die Cisco IOS-softwarerelease 12.1(13)E en hoger uitvoeren.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

VLAN-gebaseerde SPAN

SPAN (Switched Port Analyzer) kopieert verkeer van een of meer bronpoorten in een VLAN of van een of meer VLAN's naar een doelpoort voor analyse. Local SPAN ondersteunt bronpoorten, bron VLAN's en doelpoorten op dezelfde Catalyst 6500 Series Switch.

Een bron VLAN is een VLAN dat voor de analyse van het netwerkverkeer wordt gecontroleerd. VLAN-gebaseerde SPAN (VSPAN) gebruikt een VLAN als SPAN-bron. Alle poorten in de bron-VLAN's worden bronpoorten. Een bronpoort is een poort die wordt gecontroleerd voor netwerkverkeersanalyse. Trunk-poorten kunnen als bronpoorten worden geconfigureerd en gemengd met niet-kofferpoorten, maar SPAN kopieert de insluiting niet vanuit een bronboomstam-poort.

Voor VSPAN sessies met inloop en inslag ingesteld, worden twee pakketten vanuit de doelpoort verzonden als de pakketten op hetzelfde VLAN worden geschakeld (één als inbraakverkeer vanaf de ingangspoort en één als toegangsverkeer vanaf de generatiepoort).

VSPAN controleert alleen verkeer dat Layer 2-poorten in het VLAN verlaat of ingaat.

- Als u een VLAN als ingangsbron configureren en het verkeer wordt naar het gecontroleerde VLAN verzonden, wordt het routed Traffic niet gecontroleerd omdat het nooit verschijnt als ingangsverkeer dat Layer 2-poort in het VLAN ingaat.
- Als u een VLAN als energiebron vormt en het verkeer uit het gecontroleerde VLAN wordt

routed uit, wordt het routed verkeer niet gecontroleerd omdat het nooit verschijnt als persverkeer dat Layer 2 poort in het VLAN verlaat.

Raadpleeg voor meer informatie over Bron VLAN's de eigenschappen van Bron VLAN.

VLAN ACL

VACL's kunnen toegangscontrole bieden voor alle pakketten die binnen een VLAN zijn aangesloten of die in of vanuit een VLAN of een WAN-interface voor VACL-opname worden verzonden. Anders dan standaard Cisco IOS standaard- of uitgebreide ACL's die alleen op routerinterfaces zijn geconfigureerd en alleen op routepakketten worden toegepast, zijn VACL's op alle pakketten van toepassing en kunnen deze op elk VLAN of WAN-interface worden toegepast. VACL's worden verwerkt in hardware. VACL's gebruiken Cisco IOS ACL's. VACL's negeren alle Cisco IOS ACL-velden die niet in hardware worden ondersteund.

U kunt VACL's configureren voor IP-, IPX- en MAC-Layer-verkeer. VACL's die op WAN-interfaces worden toegepast, ondersteunen alleen IP-verkeer voor VACL-opname.

Wanneer u een VACL vormt en deze op een VLAN toepast, worden alle pakketten die het VLAN binnendringen gecontroleerd tegen deze VACL. Als u een VACL op het VLAN en ACL op een Routed Interface in VLAN toepast, wordt een pakket dat in VLAN komt eerst gecontroleerd tegen VACL en, indien toegestaan, dan tegen de input ACL gecontroleerd voordat het door de routed interface wordt verwerkt. Wanneer het pakket aan een ander VLAN wordt routeerd, wordt het eerst gecontroleerd tegen de uitvoer ACL die op de routeinterface wordt toegepast, en, indien toegestaan, wordt VACL die voor het doelVLAN is geconfigureerd toegepast. Als een VACL voor een pakkettype is ingesteld en een pakket van dat type niet overeenkomt met de VACL, wordt de standaardactie ontkend. Dit zijn de richtlijnen voor de opnameoptie in VACL.

- De opnamepoort kan geen ATM-poort zijn.
- De opnamepoort moet in de overspannend-boom staat voor VLAN zijn.
- De switch heeft geen beperkingen ten aanzien van het aantal havens die worden aangedaan.
- De opnamepoort neemt alleen pakketten op die door de geconfigureerde ACL zijn toegestaan.
- Opname poorten geven alleen verkeer door dat van de opnamepoort VLAN afkomstig is. Configureer de opnamepoort als een stam die de vereiste VLAN's draagt om verkeer op te nemen dat naar veel VLAN's gaat.

Waarschuwing: Onjuiste combinatie van ACL's kan de verkeersstroom verstoren. Voer extra voorzichtigheid uit terwijl u de ACLs in uw apparaat vormt.

Opmerking: VACL wordt niet ondersteund door IPv6 op een Catalyst 6000 Series switch. Met andere woorden, VLAN ACL-omleiding en IPv6 zijn niet compatibel, zodat ACL niet kan worden gebruikt om IPv6-verkeer aan te passen.

VACL-gebruik via VSPAN-gebruik

Er zijn verschillende beperkingen voor het gebruik van VSPAN voor verkeersanalyse:

- Alle laag 2 verkeer dat in een VLAN stroomt wordt gevangen. Dit verhoogt de te analyseren hoeveelheid gegevens.
- Het aantal SPAN-sessies dat op Catalyst 6500 Series Switches kan worden ingesteld, is beperkt. Raadpleeg de limieten voor lokale SPAN- en RSPAN-sessies voor meer informatie.

- Een doelhaven ontvangt exemplaren van verzonden en ontvangen verkeer voor alle gecontroleerde bronhavens. Als een doelpoort wordt oversubscript, kan deze verstopt raken. Deze congestie kan het doorsturen van verkeer op een of meer bronpoorten beïnvloeden.

De functie VACL-poort kan helpen bij het overwinnen van een aantal van deze beperkingen. VACL's zijn primair niet ontworpen om verkeer te bewaken, maar met een brede reeks mogelijkheden om het verkeer te classificeren, is de optie Capture Port geïntroduceerd zodat de analyse van het netwerkverkeer veel eenvoudiger kan worden. Dit zijn de voordelen van het VACL-opnamepoortgebruik in vergelijking met VSPAN:

- Gedetailleerde verkeersanalyseVACL's kunnen op basis van IP-adres, IP-adres van de bron, Layer 4-protocoltype, bron- en doellaag 4-poorten en andere informatie overeenkomen. Deze mogelijkheid maakt VACL's zeer nuttig voor identificatie en filtering van granulair verkeer.
- Aantal sessiesVACL's worden in hardware gehandhaafd; het aantal Access Control Entries (ACE) die kunnen worden gemaakt, is afhankelijk van de TCAM die in de switches beschikbaar zijn.
- Overabonnement doelpoortDe identificatie van het granulair verkeer vermindert het aantal frames dat naar de haven van bestemming moet worden doorgestuurd en minimaliseert aldus de kans op overinschrijving.
- PrestatiesVACL's worden in hardware gehandhaafd; er bestaat geen prestatiestraf voor de toepassing van VACL's op een VLAN op de Cisco Catalyst 6500 Series Switches

Configureren

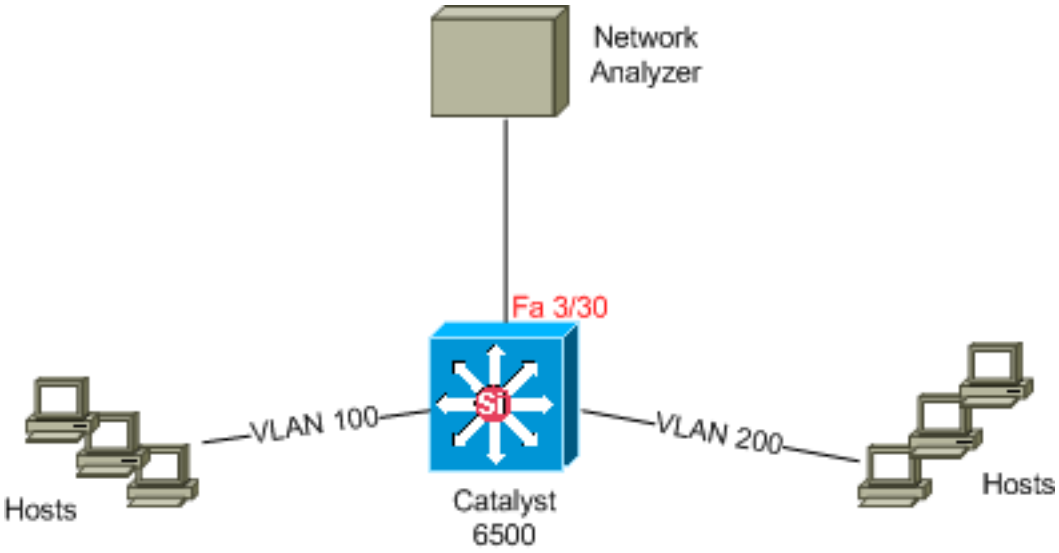
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

- Op VLAN gebaseerde SPAN configureren
- Configuratie met VACL

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie met VLAN-gebaseerde SPAN

Dit configuratievoorbeeld maakt een lijst van de stappen die vereist zijn om al Layer 2-verkeer dat in VLAN 100 en VLAN 200 stroomt op te nemen en naar het apparaat voor netwerkanalyse te verzenden.

1. Specificeer het interessante verkeer. In ons voorbeeld, is het verkeer dat in VLAN 100 en VLAN 200 stroomt.

```
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. Specificeer de doelpoort voor het opgenomen verkeer.

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

Met dit, wordt al laag 2 verkeer dat tot VLAN 100 en VLAN 200 behoort gekopieerd en naar poort Fa3/30 verzonden. Als de bestemmingspoorts deel uitmaakt van hetzelfde VLAN waarvan het verkeer wordt gecontroleerd, wordt het verkeer dat uit de doelpoort gaat niet opgenomen.

Controleer de SPAN-configuratie met de opdracht **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
```

Configuratie met VACL

In dit configuratievoorbeeld zijn er meerdere vereisten van de netwerkbeheerder:

- HTTP-verkeer van een reeks hosts (10.20.20.128/25) in VLAN 2000 naar een specifieke server (10.10.10.101) in VLAN 100 moet worden opgenomen.
- Multicast User Datagram Protocol (UDP)-verkeer in de verzendrichting voor groepsadres 239.0.100 moet vanaf VLAN 100 worden opgenomen.

1. Defineer het interessante verkeer dat moet worden opgenomen en naar analyse wordt verzonden.

```
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. Defineer een umberlla ACL om al ander verkeer in kaart te brengen.

```
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. Defineert de VLAN-toegangskaart.

```
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. Pas de VLAN-toegangskaart op de juiste VLAN's toe.

```
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. Configuratie van de 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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon VLAN access-map** — Hiermee geeft u de inhoud van de VLAN access kaarten weer.

```
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
```

- **VLAN-filter tonen** — Informatie over de VLAN-filters.

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

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- VACL-opname voor granulaire verkeersanalyse met Cisco Catalyst 6000/6500 actieve CatOS-software
- Ondersteuning van Cisco Catalyst 6500 Series Switches
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems