Nexus 7000 Series switchingvoorbeeld

Inhoud

Inleiding

Met de ACL-opname (toegangscontrolelijst) kunt u selectief verkeer opnemen op een interface of virtueel lokaal netwerk (VLAN) Wanneer u de opnameoptie voor een ACL-regel toestaat, worden pakketten die overeenkomen met deze regel verzonden of ingetrokken op basis van de gespecificeerde vergunning of ontkennen actie en kunnen ook naar een alternatieve doelpoort worden gekopieerd voor verdere analyse. Een ACL-regel met de opnamoptie kan worden toegepast:

1. In een VLAN
2. In de ingangsrichting op alle interfaces,
3. In de richting van de uitgang op alle Layer 3 interfaces.

Deze optie wordt ondersteund door Nexus 7000 NX-OS release 5.2 en hoger. Dit document biedt een voorbeeld als snelle referentie-handleiding voor het configureren van deze functie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Nexus 7000 met release 5.2.x en hoger.
- M1 serie lijnkaart.

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.

Conventies

Raadpleeg Cisco Technical Tips Convention voor informatie over documentconventies.

ACL-configuratievoorbeeld

Hier is een voorbeeldconfiguratie van ACL-opname die op een VLAN is toegepast, ook bekend als virtuele LAN Access Control List (VACL)-opname. Tien gigabit-sluipschutters zijn misschien niet voor alle scènes haalbaar. De selectieve verkeersopname kan in zulke scenario's zeer nuttig zijn, vooral tijdens het oplossen van problemen wanneer de verkeersvolumes hoog zijn.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

U kunt ook de programmering van de toegangslijst van de externe inhoud adresseerbare geheugen (TCAM) controleren. Deze uitvoer is voor VLAN 500 voor module 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot 1
=======

INSTANCE 0x0
---------------

Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
```

```
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

Caveats

1. Slechts één ACL-opnamesessie kan op een bepaald moment in het systeem over virtuele apparatuur (VDC's) actief zijn.
2. Nexus 7000 F1 Series-modules ondersteunen geen ACL-opname.
3. Nexus 7000 F2 Series-modules ondersteunen momenteel geen ACL-opname, maar dit kan in de routekaart voorkomen.
4. De ACL-opname op Nexus 7000 M2-Series modules wordt ondersteund door Cisco NX-OS release 6.1(1) en hoger.
5. De ACL-opname op Nexus 7000 M1-Series modules wordt ondersteund door Cisco NX-OS release 5.2(1) en hoger.
6. ACL-opname is niet compatibel met ACL-vastlegging. Daarom, als u ACLs met een **logsleutelwoord** hebt, werken deze niet nadat u wereldwijd **hardware access-list opname** hebt ingevoerd.
7. Vanwege bug CSCug20139 is het voorbeeld in dit document gedocumenteerd met een **opnamesessie** per ACE in plaats van per ACL, totdat de fout is opgelost.

Gerelateerde informatie

- Cisco Nexus 7000 Series security configuratiegids van NX-OS, release 6.x, Configuratievoorbeelden voor IP-ACL's
- Technische ondersteuning en documentatie – Cisco Systems