Ondersteuning van Nexus 7000 ACL voor VACL en beperkingen

Inhoud

Inleiding

Dit document beschrijft de opname-functie (ACL) (toegangscontrolelijst), die wordt gebruikt om verkeer op een interface of VLAN selectief te controleren. Wanneer u de opname optie voor een ACL-regel toestaat, worden de pakketten die deze regel overeenkomen op basis van de gespecificeerde actie verzonden of gedaald en kunnen zij ook naar een alternatieve bestemmingsppoort worden gekopieerd voor verdere analyse.

Q. Wat is het gebruik van ACL-opname?

A. Deze optie is analoog aan de VACL-opnamefunctie (VLAN Access Control List) die wordt ondersteund op Catalyst 6000 Series Switch-platforms. U kunt een ACL-opname configureren om selectief verkeer op een interface of VLAN te controleren. Wanneer u de opnameoptie voor een ACL-regel toestaat, worden pakketten die overeenkomen met deze regel verzonden of gedemonteerd op basis van de gespecificeerde vergunning of ontkennen de actie en kunnen ook naar een alternatieve doelpoort worden gekopieerd voor verdere analyse.

Q. Hoeveel ACL-opnamesessies kunnen op een Nexus 7000 switch worden ingesteld?

A. Slechts één ACL-opnamesessie kan op een bepaald moment in het systeem over Virtual Devices (VDC's) actief zijn. De ACL Ternary Content Adresseerbare Geheugen (TCAM) kan net zoveel Application Control Engines (ACE's) in de VACL hebben als kan passen.

Q. Ondersteunt M1-modules ACL-opname?

A. Ja. De ACL-opname op M1-modules wordt ondersteund in Cisco NX-OS release 5.2(1) en hoger.

Q. Ondersteunt M2-modules ACL-opname?

A. Ja. De ACL-opname op M2-modules wordt ondersteund in Cisco NX-OS release 6.1(1) en hoger.

V. Ondersteunen F1-modules ACL-opname?

A. F1-Series modules ondersteunen geen ACL-opname.

Q. Ondersteunt F2-modules ACL-opname?

A. F2-Series modules ondersteunen geen ACL-opname vanaf nu, maar dit kan in de routekaart voorkomen. Raadpleeg de Business Unit (BU) om dit te bevestigen.

Q. Op welke interfaces en richtingen kan ACL-opname worden toegepast?

A. Er kan een ACL-regel met de opnamoptie worden toegepast:

- Op een VLAN
- In de toegangsrichting op alle interfaces
- In de richting van de uitgang op alle Layer 3 interfaces

Q. Zijn er opvallende beperkingen met de ACL-opnamefunctie?

A. Ja. Sommige beperkingen met de eigenschap ACL-opname zijn:

- Een ACL-opname is een hardware-assistent onderdeel en wordt niet ondersteund voor de

beheerinterface of voor controlepakketten die afkomstig zijn van de supervisor. Het wordt ook niet ondersteund voor software ACL's zoals SNMP-community ACL's en Vty ACL's.
- Poortkanalen en supervisor in-band poorten worden niet ondersteund als bestemming voor ACL-opname.
- ACL-opnamesessie-doelinterfaces ondersteunen geen doorsturen en MAC-leren. Als een doelinterface met deze opties is ingesteld, houdt de monitor de ACL-opnamesessie ingedrukt. Gebruik de **show monitor sessie alle** opdracht om te bepalen of het ingeven en MAC learning zijn ingeschakeld.
- De bronpoort van het pakket en de ACL-opnamepoort kunnen geen deel uitmaken van dezelfde pakketreplicatie ASIC. Als beide poorten behoren tot dezelfde ASIC, wordt het pakket niet opgenomen. De opdracht **showmonitor** maakt een lijst van alle poorten die aan dezelfde ASIC zijn gekoppeld als de ACL-opnamepoort.
- Als u een ACL van de monitor van de opname vormt alvorens u de **van de hardwaretoegang tot de opname** ingaat, moet u de monitor sessie sluiten en het terug naar boven brengen om de zitting te beginnen.
- Wanneer ACL-opname is ingeschakeld, is de mogelijkheid om ACL voor alle VDC's te loggen en de snelheidsbeperking te gebruiken uitgeschakeld.

Q. Kan u een ACL-opname uitvoeren en bepaalde verkeer naar bestemming interface X, bepaalde verkeer naar bestemming interface Y en ander verkeer naar bestemming Z?

A. Nee. De bestemming kan slechts één interface zijn ingesteld met de opdracht **voor** de **hardware access-list**.

Q. Kan u de ACL vangst op meer dan één bron VLAN toepassen?

A. Ja. Meervoudige VLAN's kunnen in een VLAN-lijst worden gespecificeerd. Bijvoorbeeld:

```
vlan access-map acl-vlan-first
  match ip address acl-ipv4-first
  match mac address acl-mac-first
  action forward
  statistics per-entry
  vlan filter acl-vlan-first vlan-list 1,2,3
```

Q. Hoeveel actieve L2 VACL's kunnen op een Nexus 7010 worden geconfigureerd?

A. Het maximum aantal ondersteunde IP ACL-items is 64.000 voor apparaten zonder een XL-lijnkaart en 128.000 voor apparaten met een XL-lijnkaart.

V. Hoe werkt VACL-opname voor routeerd verkeer?

A. VACL-opname vindt plaats na herschrijven, zodat frames die VLAN X verbinden en VLAN Y registreren in VLAN Y wordt opgenomen.

Q. Bestaat een mengsel van M1- en M2-kaarten in het chassis in het gebruik van VACL's?

A. Een mix van M1- en M2-kaarten in het chassis mag geen invloed hebben op het gebruik van VACL's.

Q. Wat zijn een paar voorbeeldconfiguraties voor de ACL-opnamefunctie op Nexus 7000?

A. De ACL-opnamerichtlijnen kunnen worden bekeken in Cisco Nexus 7000 Series Security Configuration Guide, release 6.x.

Dit voorbeeld toont hoe om een ACL toe te laten om in de standaard VDC te vangen en een bestemming voor ACL te vormen die pakketten vangen:

```
hardware access-list capture
    monitor session 1 type acl-capture
    destination interface ethernet 2/1
    no shut
    exit
    show ip access-lists capture session 1
```

Dit voorbeeld toont hoe om een opnamesessie voor de ACE's van ACL toe te laten, en dan ACL op een interface toe te passen:

```
ip access-list acl1
      permit tcp any any capture session 1
      exit
      interface ethernet 1/11
      ip access-group acl1 in
      no shut
      show running-config aclmgr
```

Dit voorbeeld toont hoe om ACL met de zitting van ACEs op een VLAN toe te passen:

```
vlan access-map acl-vlan-first
      match ip address acl-ipv4-first
      match mac address acl-mac-first
      action foward
      statistics per-entry
      vlan filter acl-vlan-first vlan-list 1
      show running-config vlan 1
```

Dit voorbeeld toont hoe om een zitting van de vangst voor volledige ACL toe te laten en dan ACL op een interface toe te passen:

```
ip access-list acl2
      capture session 2
      exit
      interface ethernet 7/1
      ip access-group acl1 in
      no shut
      show running-config aclmg
```

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems