Perguntas frequentes sobre captura de ACL/suporte de VACL e limitações do Nexus 7000

Contents

Introduction
P. Qual é o caso de uso da captura ACL?
P. Quantas sessões de captura ACL podem ser configuradas em um switch Nexus 7000?
P. Os módulos M1 suportam captura de ACL?
P. Os módulos M2 suportam captura de ACL?
P. Os módulos F1 suportam captura de ACL?
P. Os módulos F2 suportam captura de ACL?
P. Em quais interfaces e direções uma captura ACL pode ser aplicada?
P. Há alguma limitação notável com o recurso de captura de ACL?
P. Você pode executar uma captura de ACL e fazer com que o tráfego saia da interface de destino X, certo tráfego saia da interface de destino Y e outro tráfego saia da interface de destino Z?
P. Você pode aplicar a captura ACL a mais de uma única VLAN de origem?
P. Quantas VACLs L2 ativas podem ser configuradas em um Nexus 7010?
P. Como a captura de VACL funciona para o tráfego roteado?
P. Uma mistura de placas M1 e M2 no chassi afeta o uso de VACLs?
P. Quais são algumas configurações de exemplo para o recurso de captura de ACL no Nexus 7000?
Informações Relacionadas

Introduction

Este documento descreve o recurso de captura da Lista de Controle de Acesso (ACL - Access Control List), que é usado para monitorar seletivamente o tráfego em uma interface ou VLAN. Quando você habilita a opção de captura para uma regra de ACL, os pacotes que correspondem a essa regra são encaminhados ou descartados com base na ação especificada e também podem ser copiados para uma porta de destino alternativa para análise posterior.

P. Qual é o caso de uso da captura ACL?

A. Esse recurso é análogo ao recurso de captura da Lista de Controle de Acesso de VLAN (VACL - VLAN Access Control List) suportado nas plataformas do Catalyst 6000 Series Switch. Você pode configurar uma captura de ACL para monitorar seletivamente o tráfego em uma interface ou VLAN. Quando você habilita a opção de captura para uma regra de ACL, os pacotes que

correspondem a essa regra são encaminhados ou descartados com base na ação de permissão ou negação especificada e também podem ser copiados para uma porta de destino alternativa para análise posterior.

P. Quantas sessões de captura ACL podem ser configuradas em um switch Nexus 7000?

A. Apenas uma sessão de captura ACL pode estar ativa a qualquer momento no sistema através de Virtual Device Context (VDCs). A TCAM (Ternary Content Addressable Memory) da ACL pode ter o máximo de ACEs (Application Control Engines, mecanismos de controle de aplicativos) na VACL que puder.

P. Os módulos M1 suportam captura de ACL?

A. Yes. A captura de ACL em módulos M1 é suportada no Cisco NX-OS versão 5.2(1) e posterior.

P. Os módulos M2 suportam captura de ACL?

A. Yes. A captura de ACL em módulos M2 é suportada no Cisco NX-OS versão 6.1(1) e posterior.

P. Os módulos F1 suportam captura de ACL?

A. Os módulos F1-Series não suportam captura de ACL.

P. Os módulos F2 suportam captura de ACL?

A. Os módulos F2-Series não suportam captura de ACL a partir de agora, mas isso pode estar no roteiro. Consulte a Unidade de negócios (BU) para confirmar.

P. Em quais interfaces e direções uma captura ACL pode ser aplicada?

A. Uma regra de ACL com a opção de captura pode ser aplicada:

- Em uma VLAN
- Na direção de entrada em todas as interfaces
- Na direção de saída em todas as interfaces de Camada 3

P. Há alguma limitação notável com o recurso de captura de

ACL?

A. Yes. Algumas limitações com o recurso de captura ACL são:

- Uma captura de ACL é um recurso assistido por hardware e não é suportada para a interface de gerenciamento ou para pacotes de controle que se originam no supervisor. Ele também não é suportado para ACLs de software, como ACLs de comunidade SNMP e ACLs vty.
- Os canais de porta e as portas de supervisor na banda não são suportados como um destino para a captura de ACL.
- As interfaces de destino da sessão de captura ACL não suportam encaminhamento de entrada e aprendizado MAC de entrada. Se uma interface de destino for configurada com essas opções, o monitor manterá a sessão de captura da ACL inativa. Use o comando **show monitor session all** para determinar se o encaminhamento de entrada e o aprendizado MAC estão ativados.
- A porta de origem do pacote e a porta de destino de captura da ACL não podem fazer parte do mesmo ASIC de replicação de pacote. Se ambas as portas pertencem ao mesmo ASIC, o pacote não é capturado. O comando **show monitor session** lista todas as portas conectadas ao mesmo ASIC que a porta de destino da captura ACL.
- Se você configurar uma sessão de monitoração de captura de ACL antes de inserir o comando **hardware access-list capture**, você deve desligar a sessão de monitoramento e ativá-la novamente para iniciar a sessão.
- Quando a captura de ACL está ativada, a capacidade de registrar ACL para todos os VDCs e usar o limitador de taxa está desativada.

P. Você pode executar uma captura de ACL e fazer com que o tráfego saia da interface de destino X, certo tráfego saia da interface de destino Y e outro tráfego saia da interface de destino Z?

A. Não. O destino só pode ser uma interface configurada com o comando **hardware access-list capture**.

P. Você pode aplicar a captura ACL a mais de uma única VLAN de origem?

A. Yes. Várias VLANs podem ser especificadas em uma lista de VLANs. Por exemplo:

```
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
```

P. Quantas VACLs L2 ativas podem ser configuradas em um Nexus 7010?

A. O número máximo de entradas IP ACL suportadas é 64.000 para dispositivos sem uma placa de linha XL e 128.000 para dispositivos com uma placa de linha XL.

P. Como a captura de VACL funciona para o tráfego roteado?

A. A captura de VACL ocorre após uma regravação, de modo que os quadros que entram na VLAN X e na VLAN Y de egresso são capturados na VLAN Y.

P. Uma mistura de placas M1 e M2 no chassi afeta o uso de VACLs?

A. Uma combinação de placas M1 e M2 no chassi não deve ter nenhum impacto no uso de VACLs.

P. Quais são algumas configurações de exemplo para o recurso de captura de ACL no Nexus 7000?

A. As diretrizes de captura de ACL podem ser visualizadas no Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x.

Este exemplo mostra como ativar uma captura ACL no VDC padrão e configurar um destino para pacotes de captura ACL:

```
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
```

Este exemplo mostra como habilitar uma sessão de captura para ACEs de uma ACL e depois aplicar a ACL a uma interface:

```
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
```

Este exemplo mostra como aplicar uma ACL com ACEs de sessão de captura a uma VLAN:

```
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
```

Este exemplo mostra como ativar uma sessão de captura para toda a ACL e depois aplicar a ACL a uma interface:

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

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems