Configurar a filtragem multicast no Nexus 7K/N9K

Contents

Introduction

Este documento descreve as diferentes maneiras de configurar as possíveis maneiras de bloquear ou filtrar certos tráfegos multicast nos switches Nexus 7000/9000. Também pode ser usado para conservar recursos multicast. Um dos exemplos comuns é a implementação da operação Universal Plug and Play pela Microsoft, que usa o SSDP para se comunicar entre os servidores.

Prerequisites

Requirements

A Cisco recomenda que você saiba como o Any-Source Multicast (ASM) com o uso do modo PIM Sparse funciona na plataforma Nexus.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Nexus 7K com LC F3/M3 executando NXOS 7.3(4)D1(1)
- Nexus N9K-C93180YC-EX/FX com 7.0(3)I7(9) ou 9.3(5)

Nota: Os resultados podem variar se o software/hardware for diferente.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começam com uma configuração limpa (padrão). Se a rede estiver em produção, certifique-se de que você entendeu o impacto potencial de qualquer comando.

Informações de Apoio

Aqui está a lista dos acrônimos usados:

RP - Ponto de encontro

FHR - roteador First Hop

LHR - Último roteador de esperança

SRC - Fonte multicast

REC - Receptor multicast

PACL - port access-list

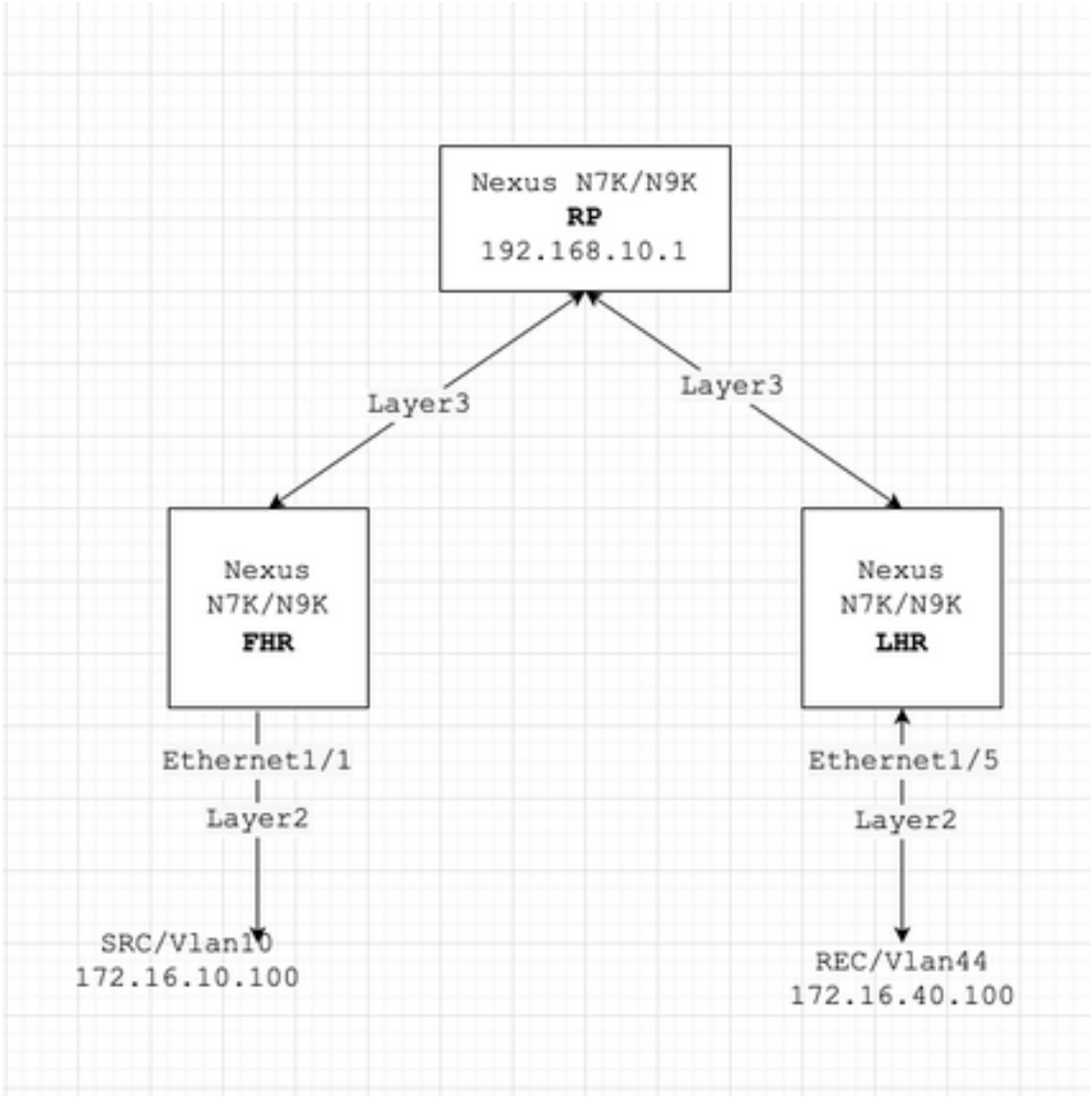
RACL - Routed access-list

SVI - Interface virtual comutada

ACL - Lista de controle de acesso

Configurar

Topologia Genérica



Exemplos de configuração

Vamos supor que:

O endereço IP do RP é 192.168.10.1

O endereço ip do SRC é 172.16.10.100/32

Grupo SSDP: 239.255.255.250/239.255.255.253

Agora, vamos discutir a configuração com base na função do dispositivo. Por exemplo, FHR, LHR, RP, etc.

FHR - Normalmente, o SRC multicast é conectado diretamente aqui

1. Filtrar registro para o RP existente.

```
ip pim rp-address 192.168.10.1 route-map filter-registration

!
```

```
Route-map filter-registration deny 5

 match ip multicast source 172.16.10.100/32 group 239.255.255.250/32

// Above line is specific to SRC/GROUP pair

Route-map filter-registration deny 7

 match ip multicast group 239.255.255.250/32

// Above line is for any SRC and specific group

!

Route-map filter-registration permit 100

 Match ip multicast group 224.0.0.0/4
```

2. Filtrar o registro para o RP definindo um RP falso (que não existe (por exemplo, 1.1.1.1) para grupos SSDP; A FHR, neste caso, assume a função de RP.

```
ip route 1.1.1.1/32 Null0

!

ip pim rp-address 1.1.1.1 route-map SSDP_groups

!

Route-map SSDP_groups permit 5

 match ip multicast group 239.255.255.250/32

Route-map SSDP_groups permit 10

 match ip multicast group 239.255.255.253/32

Route-map SSDP_groups deny 20

 match ip multicast group 224.0.0.0/4

!

ip pim rp-address 192.168.10.1 route-map all_other_groups

!

Route-map all_other_groups deny 5

 match ip multicast group 239.255.255.250/32

Route-map all_other_groups deny 10

 match ip multicast group 239.255.255.253/32

Route-map all_other_groups permit 20

 match ip multicast group 224.0.0.0/4
```

Verifique:

```
Nexus9K_OR_N7K# show ip pim rp

PIM RP Status Information for VRF "default"

BSR disabled

Auto-RP disabled

BSR RP Candidate policy: None

BSR RP policy: None

Auto-RP Announce policy: None

Auto-RP Discovery policy: None


RP: 192.168.10.1, (0),

 uptime: 00:00:27   priority: 0,

 RP-source: (local), group-map: Filter-registration,

 group ranges:

 224.0.0.0/4

 239.255.255.253/32 (deny)

 239.255.255.250/32 (deny)


Nexus9K_OR_N7K# show ip mroute

IP Multicast Routing Table for VRF "default"


(172.16.10.100/32, 239.255.255.250/32), uptime: 00:04:12, ip pim

 Incoming interface: Vlan10, RPF nbr: 172.16.10.100

 Outgoing interface list: (count: 0)


Nexus9K_OR_N7K# show system internal mfwd event-history pkt

 pkt events for MCASTFWD process

2021 Jan  1 11:11:41.792316 mcastfwd [21914]: [21933]: Create state for (172.16.10.100,
239.255.255.250)

F241.01.13-C93180YC-EX-1#

Nexus9K_OR_N7K # show ip pim internal event-history null-register

2021 Jan 01 11:15:19.095711: E_DEBUG    pim [21935]:  Null Register not sent for
(172.16.10.100/32, 239.255.255.250/32) yes
```

Esta saída confirma que o FHR não está registrando o fluxo para RP.

LHR - Normalmente, o REC Multicast é conectado diretamente aqui

3. Aplicando a política IGMP na SVI de entrada (onde a REC reside). A ideia aqui é filtrar os relatórios de associação IGMP para grupos SSDP do REC.

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4

!

route-map filter-SSDP-joins deny 5

 match ip multicast group 239.255.255.250/32

route-map filter-SSDP-joins deny 6

 match ip multicast group 239.255.255.253/32

route-map filter-SSDP-joins permit 100

 match ip multicast group 224.0.0.0/4

!

Interface VlanXX

ip igmp report-policy filter-igmp-joins
```

Verifique:

```
Nexus9K_OR_N7K (config)# show ip mroute 239.255.255.250

IP Multicast Routing Table for VRF "default"


Group not found

!

Nexus9K_OR_N7K (config)# show ip igmp snooping groups vlan 44

Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port


Vlan  Group Address      Ver  Type  Port list

44    */*                -    R     Vlan44

44    239.255.255.250    v2   D     Eth1/5

!

Nexus9K_OR_N7K (config)# show ip pim internal event-history join-prune

!

Nexus9K_OR_N7K (config)# show ip igmp internal event-history debugs

debugs events for IGMP process

2021 Jan  1 11:52:21.277915 igmp [1125]: : Filtered group 239.255.255.250

2021 Jan  1 11:52:21.277903 igmp [1125]: : Received v2 Report for 239.255.255.250 from
172.16.44.100 (Vlan44)
```

Esta saída confirma que o relatório de associação de IGMP é filtrado e (*,G) não é enviada para RP.

PIM - Roteador Habilitado Atuando como FHR/LHR

Você pode usar uma combinação das opções 1 ou 2 e 3, dependendo de seu requisito.

Por exemplo:

4. Filtrar registro para o RP existente (função FHR):

```
ip pim rp-address 192.168.10.1 route-map filter-registration

!

Route-map filter-registration deny 5

 match ip multicast source 172.16.10.100/32 group 239.255.255.250/32

Route-map filter-registration deny 7

 match ip multicast group 239.255.255.250/32

!

Route-map filter-registration permit 100

 Match ip multicast group 224.0.0.0/4
```

5. Política IGMP para filtrar relatórios de associação IGMP do REC (função LHR).

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4

!

route-map filter-SSDP-joins deny 5

 match ip multicast group 239.255.255.250/32

route-map filter-SSDP-joins deny 6

 match ip multicast group 239.255.255.253/32

route-map filter-SSDP-joins permit 100

 match ip multicast group 224.0.0.0/4

!

Interface VlanXX

ip igmp report-policy filter-igmp-joins
```

Verifique:

Quase igual à verificação feita nos pontos C e D.

```
Show ip mroute

Show ip pim rp

Show ip pim internal event-history join-prune

Show ip igmp internal event-history debugs
```

RP - Este é o ponto de encontro

6. Política de registro para bloquear o registro do grupo SSDP da FHR.

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4

ip pim register-policy all_groups

!

Route-map all_groups deny 5

 match ip multicast group 239.255.255.250/32

Route-map all_groups deny 10

 match ip multicast group 239.255.255.253/32

Route-map all_groups permit 20

 match ip multicast group 224.0.0.0/4
```

Verifique:

```
Nexus9K_OR_N7K (config)# show ip mroute 239.255.255.250

IP Multicast Routing Table for VRF "default"


Group not found

!

Nexus9K_OR_N7K (config)# show ip pim internal event-history data-register-receive

2021 Jan 08 03:33:06.353951: E_DEBUG    pim [1359]:  Register disallowed by policy

2021 Jan 08 03:33:06.353935: E_DEBUG    pim [1359]:  Received DATA Register from 172.16.10.1 for
(172.16.10.100/32, 239.255.255.250/32) (pktlen 1028)

2021 Jan 08 03:29:42.602744: E_DEBUG    pim [1359]:  Add new route (172.16.10.100/32,
239.1.1.1/32) to MRIB, multi-route TRUE


F241.01.13-C93180YC-EX-1(config)# show ip pim internal event-history null-register

2021 Jan 08 03:35:40.966617: E_DEBUG    pim [1359]:  Send Register-Stop to 172.16.10.1 for
(172.16.10.100/32, 239.255.255.250/32)
```

```
2021 Jan 08 03:35:40.966613: E_DEBUG    pim [1359]:  Register disallowed by policy

2021 Jan 08 03:35:40.966597: E_DEBUG    pim [1359]:  Received NULL Register from 172.16.10.1 for
(172.16.10.100/32, 239.255.255.250/32) (pktlen 20)
```

Esta saída confirma que o RP está bloqueando o registro para o grupo 239.255.255.250.

7. Aplicando a política Join-prune no RP - união pim (*,G) e (S,G) para grupos SSDP apenas.

```
ip pim rp-address 192.168.10.1 group-list 224.0.0.0/4

ip pim register-policy all_groups

!

Route-map all_groups deny 5

 match ip multicast group 239.255.255.250/32

Route-map all_groups deny 10

 match ip multicast group 239.255.255.253/32

Route-map all_groups permit 20

 match ip multicast group 224.0.0.0/4

!

Interface Ethernet/Y

 ip pim sparse-mode

 ip pim jp-policy all_groups
```

Verifique:

```
Nexus9K_OR_N7K # show ip mroute 239.255.255.253

IP Multicast Routing Table for VRF "default"

Group not found

!

F241.01.13-C93180YC-EX-1# show ip pim internal event-history join-prune

2021 Jan 08 03:53:41.643419: E_DEBUG    pim [1359]:  Join disallowed by inbound JP policy
```

A saída acima confirma (*,G) que a união PIM está bloqueada pelo RP.

Configurar entradas de HW para multicast

Embora todas as opções discutidas nas seções A, B ou C; Impedir que a FHR, a LHR ou a

FHR/LHR registrem o fluxo no RP ou impedir o envio da PIM Join (*,G) para o RP, respectivamente; uma entrada mroute ou snooping ainda pode ser criada e consumirá entradas HW multicast.

> **Nota:** Você pode usar RACL ou PACL em interfaces de entrada SVI ou Camada 2/canais de porta/canais de porta VPC caso o VPC esteja configurado. Se o SRC/REC for pulverizado em uma interface VLAN ou L2 diferente, isso também significa que o RACL ou o PACL precisarão ser aplicados em todos eles. Mas, dependendo do hardware/software (principalmente devido à limitação de hardware), os resultados podem variar.

PACL

Configure o PACL na porta de entrada da Camada 2 ou canal de porta ou canal de porta VPC para bloquear o tráfego SSDP ou a criação de entrada (S, G) no FHR.

> **Nota:** Dependendo do HW usado (exemplo Nexus N9000), o TCAM pode precisar ser gravado antes (o que requer recarregamento) da aplicação do PACL.

Por exemplo:

```
 ip access-list BlockAllSSDP

 Statistics per-entry

 10 deny ip any 239.255.255.250/32

 20 deny ip any 239.255.255.253/32

 30 permit ip any any

!

Interface Ethernet X/Y

Or

Interface port-channel XX

ip port-access group BlockAllSSDP in
```

Verifique:

```
F241.01.13-C93180YC-EX-1#  sh ip mroute  239.255.255.250

IP Multicast Routing Table for VRF "default"

Group not found

!

show ip access-lists block_SSDP
```

```
IP access list block_SSDP

       statistics per-entry

       10 deny ip any 239.255.255.250/32 [match=3] -> Drop counters

       20 deny ip any 239.255.255.253/32 [match=0]

       30 permit ip any any [match=0]
```

Como o tráfego multicast/portas de associação de IGMP estão bloqueadas via PACL, você não verá nenhuma entrada mroute e snooping. Essencialmente, o PACL está descartando ambos.

RACL

Você pode configurar o RACL no SVI de entrada onde o SRC existe, mas dependendo do SW/HW usado; (S, G) a entrada ainda pode ser criada ou o tráfego pode ser encaminhado para outras VLANs locais.

```
ip access-list BlockAllSSDP

 Statistics per-entry

 10 deny ip any 239.255.255.250/32

 20 deny ip any 239.255.255.253/32

 30 permit ip any any

!

Interface VlanXX

ip port-access group BlockAllSSDP in
```

Verifique:

Épraticamente igual ao PACL, mas a opção RACL pode não fornecer os mesmos resultados que o PACL; principalmente, a limitação de HW é mencionada anteriormente também.

Informações Relacionadas

- Este é um bug de solicitação de melhoria CSCvm44596
- Suporte Técnico e Documentação - Cisco Systems