Configurer le filtrage multidiffusion sur Nexus 7K/N9K

Contenu

Introduction

Ce document décrit les différentes manières de configurer les méthodes possibles pour bloquer ou filtrer certains trafics de multidiffusion sur les commutateurs Nexus 7000/9000. Il peut également être utilisé pour conserver les ressources de multidiffusion. L'un des exemples courants est l'implémentation par Microsoft d'une opération Plug and Play universelle qui utilise SSDP pour communiquer entre les serveurs.

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez comment la multidiffusion Any-Source (ASM) avec l'utilisation du mode PIM Sparse fonctionne sur la plate-forme Nexus.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Note: Les résultats peuvent varier si le logiciel/le matériel est différent.

Les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. Tous les périphériques utilisés dans ce document commencent par une configuration effacée (par défaut). Si votre réseau est en production, assurez-vous de bien comprendre l'impact potentiel de toute commande.

Informations générales

Voici la liste des acronymes utilisés :

RP - Point de rendez-vous

FHR - Routeur du premier saut

LHR - routeur du dernier saut

SRC - Source de multidiffusion

REC - Récepteur multidiffusion

PACL - port access-list

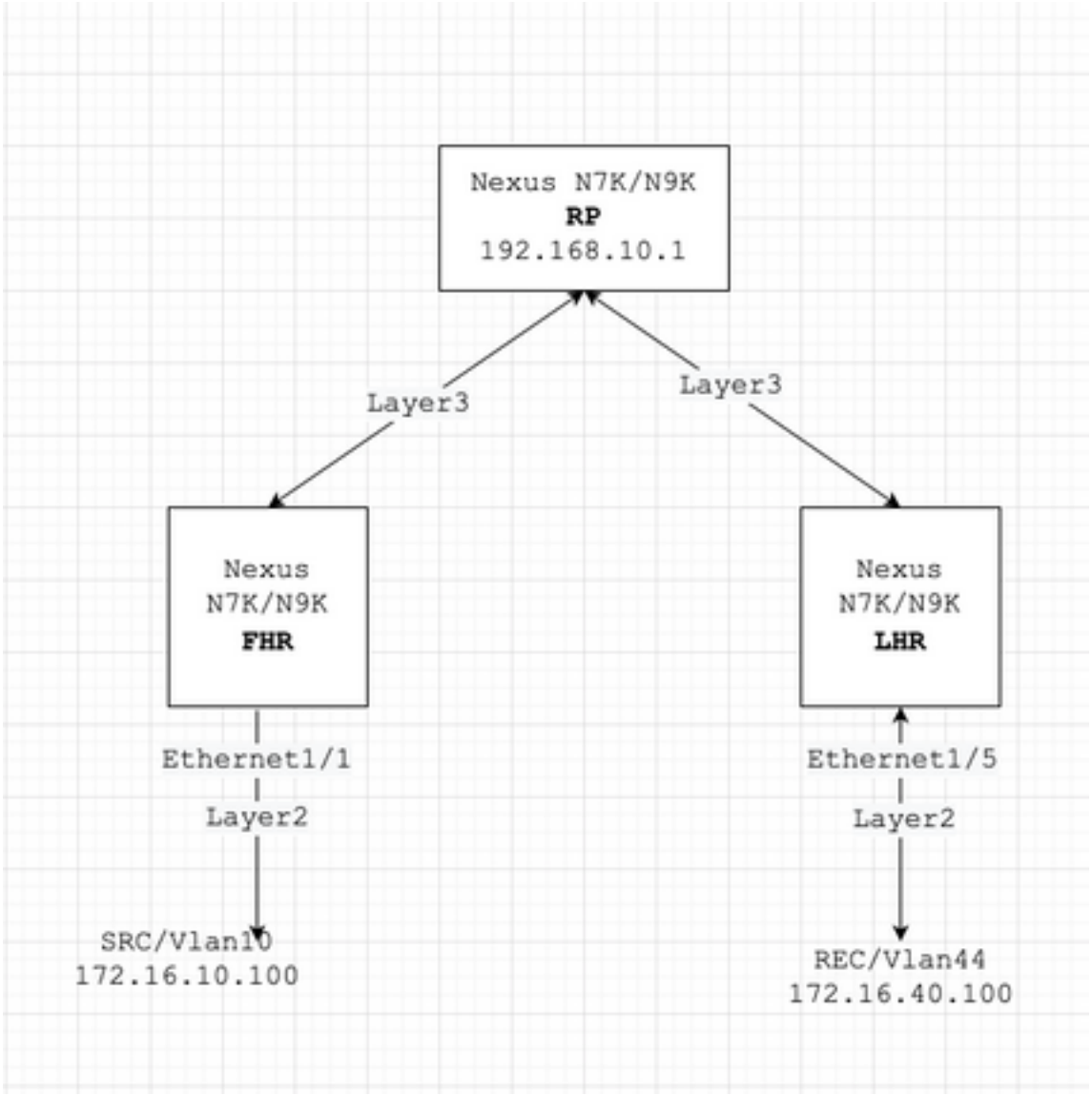
RACL - liste d'accès routée

SVI - Interface virtuelle commutée

ACL - Liste de contrôle d'accès

Configuration

Topologie générique



Exemples de configuration

Supposons ceci :

L'adresse IP du RP est 192.168.10.1

L'adresse IP de SRC est 172.16.10.100/32

Groupe SSDP : 239.255.255.250/239.255.255.253

Maintenant, discutons de la configuration en fonction du rôle du périphérique. Par exemple, FHR, LHR, RP, etc.

FHR : généralement, le SRC multidiffusion est directement connecté ici

1. Filtrer l'enregistrement vers le RP existant.

```
ip pim rp-address 192.168.10.1 route-map filter-registration ! Route-map filter-registration deny 5 mat
multicast source 172.16.10.100/32 group 239.255.255.250/32 // Above line is specific to SRC/GROUP pair
map filter-registration deny 7 match ip multicast group 239.255.255.250/32 // Above line is for any SRC
specific group ! Route-map filter-registration permit 100 Match ip multicast group 224.0.0.0/4
```

2. Filtrer l'enregistrement vers le RP en définissant un RP bidon (qui n'existe pas (par exemple, 1.1.1.1) pour les groupes SSDP ; FHR, dans ce cas, assume le rôle 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 per
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-addre
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
all_other_groups permit 20 match ip multicast group 224.0.0.0/4
```

Vérifier :

```
Nexus9K_OR_N7K# show ip pim rp PIM RP Status Information for VRF "default" BSR disabled Auto-RP disable
RP Candidate policy: None BSR RP policy: None Auto-RP Announce policy: None Auto-RP Discovery policy: N
RP: 192.168.10.1, (0), uptime: 00:00:27 priority: 0, RP-source: (local), group-map: Filter-registration
group rangs: 224.0.0.0/4 239.255.255.253/32 (deny) 239.255.255.250/32 (deny) Nexus9K_OR_N7K# show ip mr
IP Multicast Routing Table for VRF "default" (172.16.10.100/32, 239.255.255.250/32), uptime: 00:04:12,
Incoming interface: Vlan10, RPF nbr: 172.16.10.100 Outgoing interface list: (count: 0) Nexus9K_OR_N7K#
system internal mfwd event-history pkt pkt events for MCASTFWD process 2021 Jan 1 11:11:41.792316 mcast
[21914]: [21933]: Create state for (172.16.10.100, 239.255.255.250) Nexus9K_OR_N7K # show ip pim intern
event-history null-register 2021 Jan 01 11:15:19.095711: E_DEBUG pim [21935]: Null Register not sent fo
(172.16.10.100/32, 239.255.255.250/32) yes
```

Le résultat ci-dessus confirme que FHR n'enregistre pas le flux dans RP.

LHR : généralement, le routeur REC multidiffusion est directement connecté ici

3. Application de la stratégie IGMP sur l'interface SVI d'entrée (où réside REC). L'idée ici est de filtrer les rapports d'adhésion IGMP pour les groupes SSDP de 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 mul
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-SSDP-joins
```

Vérifier :

```
Nexus9K_OR_N7K (config)# show ip mroute 239.255.255.250 IP Multicast Routing Table for VRF "default" Gr
not found ! Nexus9K_OR_N7K (config)# show ip igmp snooping groups vlan 44 Type: S - Static, D - Dynamic
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 igmp internal event-history debugs debug
events for IGMP process 2021 Jan 1 11:52:21.277915 igmp [1125]: : Filtered group 239.255.255.250 2021 J
11:52:21.277903 igmp [1125]: : Received v2 Report for 239.255.255.250 from 172.16.44.100 (Vlan44)
```

Le résultat ci-dessus confirme que le rapport d'appartenance IGMP est filtré et que la jointure (*, G) n'est pas envoyée au RP.

PIM - Routeur activé agissant en tant que FHR/LHR

Vous pouvez utiliser une combinaison des options 1 ou 2 et 3, selon vos besoins.

Exemple :

4. Filtrer l'enregistrement vers le RP existant (rôle FHR) :

```
ip pim rp-address 192.168.10.1 route-map filter-registration ! Route-map filter-registration deny 5 mat
multicast source 172.16.10.100/32 group 239.255.255.250/32 Route-map filter-registration deny 7 match i
multicast group 239.255.255.250/32 ! Route-map filter-registration permit 100 Match ip multicast group
224.0.0.0/4
```

5. Stratégie IGMP pour filtrer les rapports d'appartenance IGMP à partir de REC (rôle 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 mul
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
```

Vérifier :

Àpeu près la même chose que la vérification effectuée aux points C et D ci-dessus.

```
Show ip mroute Show ip pim rp Show ip pim internal event-history join-prune Show ip igmp internal event
history debugs
```

RP : point de rendez-vous

6. Stratégie d'enregistrement pour bloquer l'enregistrement du groupe SSDP à partir de 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 mul
group 239.255.255.253/32 Route-map all_groups permit 20 match ip multicast group 224.0.0.0/4
```

Vérifier :

```
Nexus9K_OR_N7K (config)# show ip mroute 239.255.255.250 IP Multicast Routing Table for VRF "default" Gr
not found ! Nexus9K_OR_N7K (config)# show ip pim internal event-history data-register-receive 2021 Jan
03:33:06.353951: E_DEBUG pim [1359]: Register disallowed by policy 2021 Jan 08 03:33:06.353935: E_DEBUG
[1359]: Received DATA Register from 172.16.10.1 for (172.16.10.100/32, 239.255.255.250/32) (pktlen 1028
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, mul
route TRUE F241.01.13-C93180YC-EX-1(config)# show ip pim internal event-history null-register 2021 Jan
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
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)
```

Le résultat ci-dessus confirme que le RP bloque l'enregistrement du groupe 239.255.255.250.

7. Application de la stratégie Join-Prune sur le RP - jointure pim (*, G) et jointure (S, G) pour le groupe SSDP uniquement.

```
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 mul
group 239.255.255.253/32 Route-map all_groups permit 20 match ip multicast group 224.0.0.0/4 ! Interfac
Ethernet/Y ip pim sparse-mode ip pim jp-policy all_groups
```

Vérifier :

```
Nexus9K_OR_N7K # show ip mroute 239.255.255.253 IP Multicast Routing Table for VRF "default" Group not
! 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
```

La sortie ci-dessus confirme (*, G) que la jointure PIM est bloquée par le RP.

Configurer la conservation des entrées matérielles pour la multidiffusion

Bien que toutes les options examinées à la section A, B ou C ; empêchera FHR, LHR ou FHR/LHR d'enregistrer le flux au niveau RP ou empêchera l'envoi de PIM Join (*, G) vers le RP respectivement ; une entrée mroute ou snooping peut encore être créée et consommera des entrées matérielles multidiffusion.

> **Note**: Vous pouvez utiliser RACL ou PACL sur les interfaces SVI ou Layer2 d'entrée/Port-Channels/Port-Channels VPC si VPC est configuré. Si SRC/REC est pulvérisé dans une interface VLAN ou L2 différente, cela signifie également que RACL ou PACL devra être appliqué à toutes ces interfaces. Cependant, selon le matériel et le logiciel (principalement en raison de la limitation du matériel), les résultats peuvent varier.

PACL

Configurez PACL sur le port d'entrée de couche 2 ou port-channel ou VPC port-channel pour bloquer le trafic SSDP ou la création d'une entrée (S, G) sur FHR.

> **Note**: Selon le matériel utilisé (exemple Nexus N9000), la TCAM peut devoir être découpée avant (qui nécessite de recharger) l'application de la PACL.

Exemple :

```
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-a
group BlockAllSSDP in
```

Vérifier :

```
F241.01.13-C93180YC-EX-1# sh ip mroute 239.255.255.250 IP Multicast Routing Table for VRF "default" Gro
found ! show ip access-lists BlockAllSSDP IP access list BlockAllSSDP statistics per-entry 10 deny ip a
239.255.255.250/32 [match=3] -> Drop counters 20 deny ip any 239.255.255.253/32 [match=0] 30 permit ip
any [match=0]
```

Étant donné que les deux ports d'appartenance de trafic multidiffusion/IGMP sont bloqués via PACL, vous ne verrez aucune entrée de routage de surveillance. Essentiellement, PACL les supprime toutes les deux.

RACINE

Vous pouvez configurer RACL sur l'interface SVI d'entrée où SRC existe mais selon le logiciel/le matériel utilisé ; (S, G) l'entrée peut encore être créée ou le trafic peut être transféré à d'autres VLAN locaux.

```
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
```

Vérifier :

C'est à peu près la même chose que PACL **mais l'option RACL peut ne pas fournir les mêmes résultats que PACL ;** la plupart du temps, c'est la limitation matérielle qui est mentionnée plus haut également.

Informations connexes

- Ceci est un bogue de demande d'amélioration CSCvm44596
- **Support et documentation techniques - Cisco Systems**