Configuration et vérification de la fonction NAT sur les commutateurs Catalyst 9000

Table des matières

Introduction

Ce document décrit comment configurer et valider la traduction d'adresses de réseau (NAT) sur la plate-forme Catalyst 9000.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Adressage IP
- Listes de contrôle d'accès

Informations générales

Le cas le plus courant pour la fonction NAT est celui de la traduction dâ€™un espace réseau IP privé en adresses routables Internet uniques au monde.

Le périphérique qui exécute la fonction NAT doit disposer dâ€™une interface sur le réseau interne (local) et dâ€™une interface sur le réseau externe (global).

Un périphérique NAT est responsable de l'inspection du trafic source afin de déterminer s'il nécessite une traduction basée sur la configuration des règles NAT.

Si une traduction est requise, le périphérique traduit l'adresse IP source locale en une adresse IP unique au monde et en assure le suivi dans sa table de traduction NAT.

Lorsque des paquets reviennent avec une adresse routable, le périphérique vérifie sa table NAT pour voir si une autre traduction est en ordre.

Si câ€™est le cas, le routeur traduit lâ€™adresse globale interne en lâ€™adresse locale interne appropriée et achemine le paquet.

Composants utilisés

Avec Cisco IOS® XE 16.12.1, la NAT est désormais disponible sur la licence Network Advantage. Sur toutes les versions antérieures, il est disponible sur la licence DNA Advantage.

Plateforme	Introduction de la fonction NAT
C9300	Cisco IOS® XE version 16.10.1
C9400	Cisco IOS® XE version 17.1.1
C9500	Cisco IOS® XE version 16.5.1a
C9600	Cisco IOS® XE version 16.11.1

Ce document est basé sur la plate-forme Catalyst 9300 avec Cisco IOS® XE Version 16.12.4

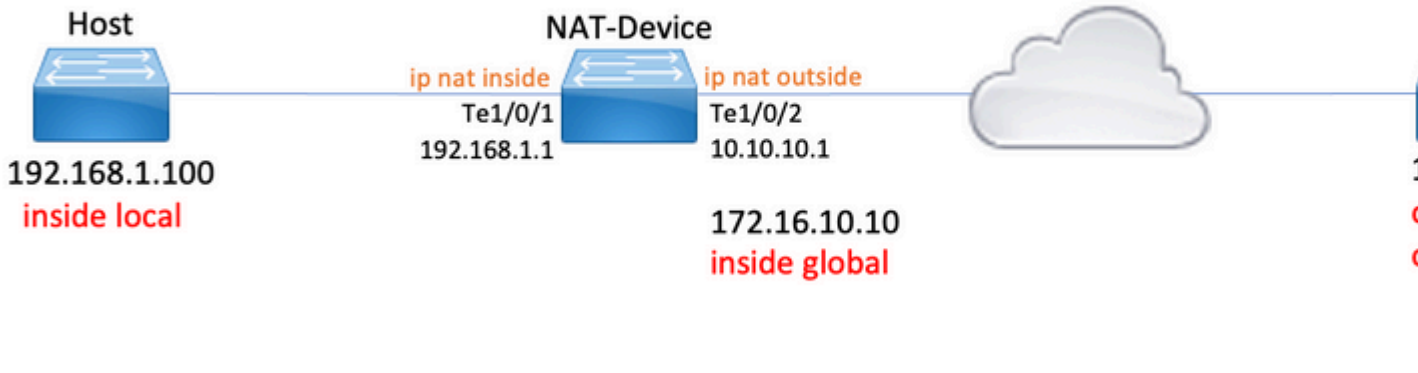
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Terminologie

NAT statique	Permet un mappage 1 à 1 d'une adresse locale vers une adresse globale.
NAT dynamique	Mappe les adresses locales à un pool d'adresses globales.
Surcharge NAT	Mappe les adresses locales à une adresse globale unique qui utilise des ports L4 uniques.
Local interne	Adresse IP attribuée à un hôte sur le réseau interne.
Globale interne	Il sâ€™agit de lâ€™adresse IP de lâ€™hôte interne telle quâ€™elle apparaît au réseau externe. Vous pouvez considérer cela comme l'adresse vers laquelle le local interne est traduit.
Local externe	Adresse IP dâ€™un hôte externe telle quâ€™elle apparaît au réseau interne.
Externe global	Adresse IP attribuée à un hôte sur le réseau externe. Dans la plupart des cas, les adresses locales et globales externes sont identiques.
FMAN-RP	Gestionnaire de fonctionnalités RP. Il s'agit du plan de contrôle de Cisco IOS® XE qui transmet les informations de programmation à FMAN-FP.

FMAN-FP	Gestionnaire de fonctionnalités FP. FMAN-FP reçoit des informations de FMAN-RP et les transmet à FED.
NOURRIR	Pilote du moteur de transfert. FMAN-FP utilise le FED pour programmer les informations du plan de contrôle dans le circuit ASIC (Application Specific Integrated Circuit) du plan de données d'accès unifié (UADP).

Diagramme du réseau



Configurer

Exemples de configuration

Configuration **NAT statique** pour traduire 192.168.1.100 (local interne) en 172.16.10.10 (global interne) :

<#root>

```
NAT-Device#
show run interface te1/0/1

Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/1
no switchport
ip address 192.168.1.1 255.255.255.0
ip nat inside                          <-- NAT inside interface

end

NAT-Device#
show run interface te1/0/2

Building configuration...
```

```
Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/2
no switchport
ip address 10.10.10.1 255.255.255.0
ip nat outside                          <-- NAT outside interface

end

ip nat inside source static 192.168.1.100 172.16.10.10              <-- static NAT rule


NAT-Device#
show ip nat translations

Pro Inside global      Inside local      Outside local      Outside global
icmp 172.16.10.10:4    192.168.1.100:4   10.20.30.40:4      10.20.30.40:4
<-- active NAT translation

---  172.16.10.10      192.168.1.100     ---                ---
<-- static NAT translation added as a result of the configuration
```

Configuration **NAT dynamique** pour traduire 192.168.1.0/24 en 172.16.10.1 - 172.16.10.30 :

<#root>

```
NAT-Device#
show run interface te1/0/1

Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/1
no switchport
ip address 192.168.1.1 255.255.255.0
ip nat inside                               <-- NAT inside interface

end

NAT-Device#
show run interface te1/0/2

Building configuration...
```

```
Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/2
no switchport
ip address 10.10.10.1 255.255.255.0
ip nat outside


<-- NAT outside interface


end
!
ip nat pool TAC-POOL 172.16.10.1 172.16.10.30 netmask 255.255.255.224      <-- NAT pool configuration


ip nat inside source list hosts pool TAC-POOL


<-- NAT rule configuration


!
ip access-list standard hosts                                              <-- ACL to match hosts to be


10 permit 192.168.1.0 0.0.0.255

NAT-Device#
show ip nat translations


Pro Inside global     Inside local     Outside local      Outside global
icmp 172.16.10.10:6   192.168.1.100:6  10.20.30.40:6      10.20.30.40:6
---  172.16.10.10     192.168.1.100    ---                ---
```

Configuration de la **surcharge NAT dynamique (PAT)** pour traduire 192.168.1.0/24 en 10.10.10.1 (interface externe ip nat) :

```
<#root>

NAT-Device#
show run interface te1/0/1


Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/1
no switchport
ip address 192.168.1.1 255.255.255.0
ip nat inside                              <-- NAT inside interface
```

```
end

NAT-Device#
show run interface te1/0/2


Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/2
no switchport
ip address 10.10.10.1 255.255.255.0
ip nat outside                              <-- NAT outside interface


end
!
ip nat inside source list hosts interface TenGigabitEthernet1/0/2 overload          <-- NAT configuratio


!
ip access-list standard hosts                                                       <-- ACL to match hos


 10 permit 192.168.1.0 0.0.0.255
```

Notez que le port incrémente l'adresse globale interne de 1 pour chaque traduction :

<#root>

```
NAT-Device#
show ip nat translations


Pro Inside global      Inside local      Outside local      Outside global
icmp 10.10.10.1:1024   192.168.1.100:1   10.20.30.40:1        10.20.30.40:1024


<-- Notice layer 4 port increments


icmp 10.10.10.1:1025   192.168.1.100:2   10.20.30.40:2        10.20.30.40:1025


<-- Notice layer 4 port increments


icmp 10.10.10.1:1026   192.168.1.100:3   10.20.30.40:3        10.20.30.40:1026
icmp 10.10.10.1:1027   192.168.1.100:4   10.20.30.40:4        10.20.30.40:1027
icmp 10.10.10.1:1028   192.168.1.100:5   10.20.30.40:5        10.20.30.40:1028
icmp 10.10.10.1:1029   192.168.1.100:6   10.20.30.40:6        10.20.30.40:1029
icmp 10.10.10.1:1030   192.168.1.100:7   10.20.30.40:7        10.20.30.40:1030
icmp 10.10.10.1:1031   192.168.1.100:8   10.20.30.40:8        10.20.30.40:1031
```

10.10.10.1:1024 = inside global

192.168.1.100:1 = inside local

Vérification de la NAT statique

Vérification du logiciel

La moitié d'une traduction avec NAT statique est attendue lorsqu'il n'y a pas de flux actif traduit. Lorsque le flux devient actif, une traduction dynamique est créée

<#root>

NAT-Device#

show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 172.16.10.10:10 192.168.1.100:10 10.20.30.40:10 10.20.30.40:10

<-- dynamic translation

--- 172.16.10.10 192.168.1.100 --- ---

<-- static configuration from NAT rule configuration

Avec la commande **show ip nat translations verbose**, vous pouvez déterminer l'heure de création du flux et le temps restant sur la traduction.

<#root>

NAT-Device#

show ip nat translations verbose

Pro Inside global Inside local Outside local Outside global
icmp 172.16.10.10:10 192.168.1.100:10 10.20.30.40:10 10.20.30.40:10

create 00:00:13, use 00:00:13, left 00:00:46,

<-- NAT timers

```
flags:
extended, use_count: 0, entry-id: 10, lc_entries: 0
--- 172.16.10.10 192.168.1.100 --- ---
create 00:09:47, use 00:00:13,
flags:
static, use_count: 1, entry-id: 9, lc_entries: 0
```

Vérifiez les statistiques NAT. Le compteur d'accès NAT s'incrémente lorsqu'un flux correspond à une règle NAT et est créé.

Le compteur d'échecs NAT s'incrémente lorsque le trafic correspond à une règle mais que nous ne pouvons pas créer la traduction.

<#root>

NAT-DEVICE#

show ip nat statistics

Total active translations: 1 (

1 static,

0 dynamic; 0 extended)

<-- 1 static translation

Outside interfaces:

TenGigabitEthernet1/0/1 <-- NAT outside interface

Inside interfaces:

TenGigabitEthernet1/0/2 <-- NAT inside interface

Hits: 0 Misses: 0 <-- NAT hit and miss counters.

```
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list hosts interface TenGigabitEthernet1/0/1 refcount 0
```

Pour que la traduction se produise, il doit y avoir une contiguïté avec la source et la destination du flux NAT. Notez l'ID de contiguïté.

<#root>

NAT-Device#

show ip route 10.20.30.40

```
Routing entry for 10.20.30.40/32
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
* 10.10.10.2
Route metric is 0, traffic share count is 1

NAT-Device#
```

show platform software adjacency switch active f0

```
Adjacency id:
```

0x29(41)

<-- adjacency ID

```
Interface: TenGigabitEthernet1/0/1, IF index: 52, Link Type: MCP_LINK_IP
Encap: 0:ca:e5:27:3f:e4:70:1f:53:0:b8:e4:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

192.168.1.100

<-- source adjacency

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 464, HW handle: (nil) (created)

Adjacency id:
```

0x24 (36)

<-- adjacency ID

```
Interface: TenGigabitEthernet1/0/2, IF index: 53, Link Type: MCP_LINK_IP
Encap: 34:db:fd:ee:ce:e4:70:1f:53:0:b8:d6:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

10.10.10.2

<-- next hop to 10.20.30.40

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 452, HW handle: (nil) (created)
```

Les débogages NAT peuvent être activés pour vérifier que le commutateur reçoit le trafic et si cela crée un flux NAT

> **Remarque** : notez que le trafic ICMP soumis à la NAT est toujours géré dans le logiciel, de sorte que les débogages de plateforme n'affichent pas les journaux pour le trafic ICMP.

<#root>

```
NAT-Device#
```

debug ip nat detailed

```
IP NAT detailed debugging is on
NAT-Device#
*Mar 8 23:48:25.672: NAT: Entry assigned id 11
```

<-- receive traffic and flow created

```
*Mar 8 23:48:25.672: NAT: i: icmp (192.168.1.100, 11) -> (10.20.30.40, 11) [55]
*Mar 8 23:48:25.672: NAT:
```

s=192.168.1.100->172.16.10.10

```
, d=10.20.30.40 [55]NAT: dyn flow info download suppressed for flow 11
```

<-- source is translated

```
*Mar 8 23:48:25.673: NAT: o: icmp (10.20.30.40, 11) -> (172.16.10.10, 11) [55]
*Mar 8 23:48:25.674: NAT: s=10.20.30.40,
```

d=172.16.10.10->192.168.1.100

```
 [55]NAT: dyn flow info download suppressed for flow 11
```

<-- return source is translated

```
*Mar 8 23:48:25.675: NAT: i: icmp (192.168.1.100, 11) -> (10.20.30.40, 11) [56]
```

Lorsque le flux expire ou est supprimé, vous voyez l'action DELETE dans les débogages :

<#root>

```
*Mar 31 17:58:31.344: FMANRP-NAT: Received flow data, action:
```

DELETE

<-- action is delete

```
*Mar 31 17:58:31.344: id 2, flags 0x1, domain 0
src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40,
dst_global_addr 10.20.30.40, src_local_port 31783, src_global_port 31783,
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 0,
outside_mapping_id 0, inside_mapping_type 0,
outside_mapping_type 0
```

Vérification du matériel

Lorsque la règle NAT est configurée, le périphérique programme cette règle dans TCAM sous la région NAT 5. Vérifiez que la règle est programmée dans TCAM.

Les sorties sont au format hexadécimal, donc la conversion en adresse IP est nécessaire.

<#root>

NAT-Device#

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region NAT_1 (370) type 6 asic 3
=======================================================
Printing entries for region NAT_2 (371) type 6 asic 3
=======================================================
Printing entries for region NAT_3 (372) type 6 asic 3
=======================================================
Printing entries for region NAT_4 (373) type 6 asic 3
=======================================================
```

Printing entries for region NAT_5 (374) type 6 asic 3 <-- NAT Region 5

```
=======================================================
TAQ-2 Index-128 (A:1,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:ffffffff
Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
```

c0a80164

<--

inside local IP address 192.168.1.100 in hex (c0a80164)

```
AD 10087000:00000073

TAQ-2 Index-129 (A:1,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:ffffffff:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:
```

ac100a0a

```
:00000000
```

<-- inside global IP address 172.16.10.10 in hex (ac100a0a)

```
AD 10087000:00000073
```

Enfin, lorsque le flux devient actif, la programmation matérielle peut être confirmée par la vérification de TCAM sous la région NAT 1.

<#root>

```
NAT-Device#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region
```

NAT_1

```
 (370) type 6 asic 1
```

<-- NAT Region 1

```
==========================================================
TAQ-2 Index-32 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:06005ac9:00000000:00000017:00000000:00000000:
```

0a141e28:c0a80164

```
AD 10087000:000000b0

TAQ-2 Index-33 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:06000017:00000000:00005ac9:00000000:00000000:
```

ac100a0a:0a141e28

```
AD 10087000:000000b1

Starting at Index-32 Key1 from right to left:
```

c0a80164

```
 = 192.168.1.100 (Inside Local)
```

0a141e28

```
 = 10.20.30.40 (Outside Global)
```

00000017

```
 = 23 (TCP destination port)
```

06005ac9

```
 = 06 for TCP and 5ac9 is 23241 which is source port from "show ip nat translations" of the inside host

Repeat the same for Index-33 which is the reverse translation:
```

0a141e28

= 10.20.30.40 (Outside Global)

ac100a0a

= 172.16.10.10 (Inside Global)

00005ac9

= 23241 TCP Destination port

06000017

= 06 for TCP and 17 for TCP source port 23

Vérification de la NAT dynamique

Vérification du logiciel

Vérifiez que le pool d'adresses vers lequel traduire les adresses IP internes est configuré.

Cette configuration permet de traduire le réseau 192.168.1.0/24 en adresses 172.16.10.1 à 172.16.10.254

<#root>

NAT-Device#

show run | i ip nat

ip nat inside

<-- ip nat inside on inside interface

ip nat outside

<-- ip nat outside on outside interface

ip nat pool MYPOOL 172.16.10.1 172.16.10.254 netmask 255.255.255.0 <-- Pool of addresses to translate

ip nat inside source list hosts pool MYPOOL <-- Enables hosts that match ACL "h

NAT-Device#

show ip access-list 10 <-- ACL to match hosts to be translated

Standard IP access list 10
10 permit 192.168.1.0, wildcard bits 0.0.0.255

```
NAT-Device#
```

Notez qu'avec la NAT dynamique, il ne crée pas d'entrées avec seulement la configuration. Un flux actif doit être créé avant que la table de traduction ne soit remplie.

<#root>

```
NAT-Device#
```

```
show ip nat translations
```

```
<...empty...>
```

Vérifiez les statistiques NAT. Le compteur d'accès NAT s'incrémente lorsqu'un flux correspond à une règle NAT et est créé.

Le compteur d'échecs NAT s'incrémente lorsque le trafic correspond à une règle mais que nous ne pouvons pas créer la traduction.

<#root>

```
NAT-DEVICE#
```

```
show ip nat statistics
```

```
Total active translations: 3794 (1 static,
```

```
3793 dynamic
```

```
; 3793 extended)
```

```
<-- dynamic translations
```

```
Outside interfaces:
```

```
TenGigabitEthernet1/0/1           <-- NAT outside interface
```

```
Inside interfaces:
```

```
TenGigabitEthernet1/0/2           <-- NAT inside interface
```

```
Hits: 3793
```

```
 Misses: 0
```

```
<-- 3793 hits
```

```
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
```

```
Dynamic mappings:                 <-- rule for dynamic mappings
```

-- Inside Source
[Id: 1]

access-list hosts interface TenGigabitEthernet1/0/1

refcount 3793

<-- NAT rule displayed

Confirmer la présence de la contiguïté avec la source et la destination

<#root>

NAT-Device#

show platform software adjacency switch active f0

Number of adjacency objects: 4

Adjacency id:

0x24(36)

<-- adjacency ID

Interface: TenGigabitEthernet1/0/2, IF index: 53, Link Type: MCP_LINK_IP
Encap: 34:db:fd:ee:ce:e4:70:1f:53:0:b8:d6:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:

10.10.10.2

<-- adjacency to destination

IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 449, HW handle: (nil) (created)

Adjacency id:

0x25 (37)

<-- adjacency ID

Interface: TenGigabitEthernet1/0/1, IF index: 52, Link Type: MCP_LINK_IP
Encap: 0:ca:e5:27:3f:e4:70:1f:53:0:b8:e4:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None

```
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

192.168.1.100

<-- source adjacency

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 451, HW handle: (nil) (created)
```

Une fois les contiguïtés confirmées si un problème avec NAT est présent, vous pouvez commencer avec des débogages NAT indépendants de la plate-forme

<#root>

```
NAT-Device#
```

debug ip nat

```
IP NAT debugging is on
NAT-Device#
```

debug ip nat detailed

```
IP NAT detailed debugging is on

NAT-Device#
```

show logging

```
*May 13 01:00:41.136: NAT: Entry assigned id 6
*May 13 01:00:41.136: NAT: Entry assigned id 7
*May 13 01:00:41.136: NAT: i:
```

tcp (192.168.1.100, 48308)

```
 -> (10.20.30.40, 23) [30067]
```

<-- first packet ingress without NAT

```
*May 13 01:00:41.136: NAT: TCP Check for Limited ALG Support
*May 13 01:00:41.136: NAT:
```

s=192.168.1.100->172.16.10.10

```
, d=10.20.30.40 [30067]NAT: dyn flow info download suppressed for flow 7
```

<-- confirms source address translation

```
*May 13 01:00:41.136: NAT: attempting to setup alias for 172.16.10.10 (redundancy_name , idb NULL, flags
*May 13 01:00:41.139: NAT: o:
```

tcp (10.20.30.40, 23)

```
 -> (172.16.10.10, 48308) [40691]
```

<-- return packet from destination to be translated

```
*May 13 01:00:41.139: NAT: TCP Check for Limited ALG Support
*May 13 01:00:41.139: NAT: s=10.20.30.40,
```

d=172.16.10.10->192.168.1.100

```
 [40691]NAT: dyn flow info download suppressed for flow 7
```

<-- return packet is translated

```
*May 13 01:00:41.140: NAT: i: tcp (192.168.1.100, 48308) -> (10.20.30.40, 23) [30068]
```

Vous pouvez également déboguer le fonctionnement de la NAT FMAN-RP :

<#root>

```
NAT-Device#
```

debug platform software nat all

```
NAT platform all events debugging is on

Log Buffer (100000 bytes):

*May 13 01:04:16.098: FMANRP-NAT: Received flow data, action:
```

ADD

<-- first packet in flow so we ADD an entry

```
*May 13 01:04:16.098: id 9, flags 0x1, domain 0
```

src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40

,

<-- verify inside local/global and outside local/global

```
dst_global_addr 10.20.30.40, src_local_port 32529, src_global_port 32529,
```

dst_local_port 23, dst_global_port 23

,

<-- confirm ports, in this case they are for Telnet

```
proto 6, table_id 0 inside_mapping_id 1,
outside_mapping_id 0, inside_mapping_type 2,
outside_mapping_type 0
*May 13 01:04:16.098: FMANRP-NAT: Created TDL message for flow info:
ADD id 9
*May 13 01:04:16.098: FMANRP-NAT: Sent TDL message for flow data config:
ADD id 9
```

```
*May 13 01:04:16.098: FMANRP-NAT: Received flow data, action:
 MODIFY            <-- subsequent packets are MODIFY

*May 13 01:04:16.098: id 9, flags 0x1, domain 0
src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40,
dst_global_addr 10.20.30.40, src_local_port 32529, src_global_port 32529,
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 1,
outside_mapping_id 0, inside_mapping_type 2,
outside_mapping_type 0
*May 13 01:04:16.098: FMANRP-NAT: Created TDL message for flow info:
MODIFY id 9
*May 13 01:04:16.098: FMANRP-NAT: Sent TDL message for flow data config:
MODIFY id 9
```

Si la règle est supprimée pour une raison quelconque telle que l'expiration ou la suppression manuelle, une action DELETE est observée :

```
<#root>

*May 13 01:05:20.276: FMANRP-NAT: Received flow data, action:

DELETE           <-- DELETE action

*May 13 01:05:20.276: id 9, flags 0x1, domain 0
src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40,
dst_global_addr 10.20.30.40, src_local_port 32529, src_global_port 32529,
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 0,
outside_mapping_id 0, inside_mapping_type 0,
outside_mapping_type 0
```

Vérification du matériel

Vérifiez si la règle NAT qui correspond au trafic à traduire est correctement ajoutée dans le matériel sous la région NAT 5 :

```
<#root>

NAT-Device#

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

Printing entries for region

NAT_1

 (370) type 6 asic 1

<<<< empty due to no active flow
```

```
=========================================================
Printing entries for region NAT_2 (371) type 6 asic 1
=========================================================
Printing entries for region NAT_3 (372) type 6 asic 1
=========================================================
Printing entries for region NAT_4 (373) type 6 asic 1
=========================================================
Printing entries for region NAT_5 (374) type 6 asic 1
=========================================================
TAQ-2 Index-128 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:fffffff8:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:ac100a00:00000000
AD 10087000:00000073

TAQ-2 Index-129 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:
```

ffffff00

```
Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
```

c0a80100

```
AD 10087000:00000073
```

ffffff00 = 255.255.255.0 in hex

c0a80100 = 192.168.1.0 in hex which matches our network in the NAT ACL

Enfin, vous devez confirmer que la traduction active est programmée correctement dans la région 1 NAT TCAM

<#root>

```
NAT-Device#
```

show ip nat translations

```
Pro Inside global       Inside local        Outside local      Outside global
tcp 172.16.10.10:54854  192.168.1.100:54854 10.20.30.40:23     10.20.30.40:23
--- 172.16.10.10        192.168.1.100       ---                ---

NAT-Device#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region
```

NAT_1

```
 (370) type 6 asic 1
=========================================================
TAQ-2 Index-32 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
```

Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:0600d646:00000000:00000017:00000000:00000000:

0a141e28

:

c0a80164

AD 10087000:000000b0

TAQ-2 Index-33 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:06000017:00000000:0000d646:00000000:00000000:

ac100a0a

:

0a141e28

AD 10087000:000000b1

Printing entries for region NAT_2 (371) type 6 asic 1
===
Printing entries for region NAT_3 (372) type 6 asic 1
===
Printing entries for region NAT_4 (373) type 6 asic 1
===
Printing entries for region NAT_5 (374) type 6 asic 1
===

Starting at Index-32 Key 1 from right to left:

c0a80164

 - 192.168.1.100 (inside local)

0a141e28

 - 10.20.30.40 (outside local/global)

00000017

 - TCP port 23

0600d646

 - 6 for TCP protocol and 54854 for TCP source port

Starting at Index-33 Key 1 from right to left

0a141e28

 - 10.20.30.40 destination address

ac100a0a

 - 172.16.10.10 (inside global source IP address)

0000d646

 - TCP source port

06000017

- TCP protocol 6 and 23 for the TCP destination port

Vérification de la surcharge NAT dynamique (PAT)

Vérification du logiciel

Les processus de journalisation permettant de vérifier la PAT sont identiques à la NAT dynamique. Il vous suffit de confirmer la traduction correcte des ports et que les ports sont programmés correctement dans le matériel.

La PAT est obtenue par le mot clé « overload » ajouté à la règle NAT.

<#root>

NAT-Device#

show run | i ip nat

ip nat inside

<-- ip nat inside on NAT inside interface

ip nat outside

<-- ip nat outside on NAT outside interface

ip nat pool MYPOOL 172.16.10.1 172.16.10.254 netmask 255.255.255.0 <-- Address pool to translate to

ip nat inside source list hosts pool MYPOOL overload <-- Links ACL hosts to address pool

Confirmer la présence de la contiguïté avec la source et la destination

<#root>

NAT-Device#

show ip route 10.20.30.40

Routing entry for 10.20.30.40/32
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
*

10.10.10.2

Route metric is 0, traffic share count is 1

NAT-Device#

show platform software adjacency switch active f0

Number of adjacency objects: 4

Adjacency id:

0x24

(36)

<-- adjacency ID

Interface: TenGigabitEthernet1/0/2, IF index: 53, Link Type: MCP_LINK_IP
Encap: 34:db:fd:ee:ce:e4:70:1f:53:0:b8:d6:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:

10.10.10.2 <-- adjacency to destination

IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 449, HW handle: (nil) (created)

Adjacency id:

0x25

(37)

<-- adjacency ID

Interface: TenGigabitEthernet1/0/1, IF index: 52, Link Type: MCP_LINK_IP
Encap: 0:ca:e5:27:3f:e4:70:1f:53:0:b8:e4:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:

192.168.1.100 <-- source adjacency

IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 451, HW handle: (nil) (created)

Confirmez que la traduction est ajoutée à la table de traduction lorsque le flux est actif. Notez qu'avec la PAT, aucune demi-entrée n'est créée, contrairement à la NAT dynamique.

Suivez les numéros de port sur les adresses locales internes et globales internes.

<#root>

NAT-Device#

show ip nat translations

```
Pro Inside global      Inside local        Outside local      Outside global
tcp 172.16.10.10:1024  192.168.1.100:52448 10.20.30.40:23     10.20.30.40:23
```

Vérifiez les statistiques NAT. Le compteur d'accès NAT s'incrémente lorsqu'un flux correspond à une règle NAT et est créé.

Le compteur d'échecs NAT s'incrémente lorsque le trafic correspond à une règle mais que nous ne pouvons pas créer la traduction.

<#root>

NAT-DEVICE#

show ip nat statistics

Total active translations: 3794 (1 static,

3793 dynamic

; 3793 extended)

<-- dynamic translations

Outside interfaces:

TenGigabitEthernet1/0/1 <-- NAT outside interface

Inside interfaces:

TenGigabitEthernet1/0/2 <-- NAT inside interface

Hits: 3793

Misses: 0

<-- 3793 hits

CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0

Dynamic mappings:

<-- rule for dynamic mappings

-- Inside Source
[Id: 1]

access-list hosts interface TenGigabitEthernet1/0/1

refcount 3793

<-- NAT rule displayed

Les débogages NAT indépendants de la plate-forme montrent que la traduction de port se produit :

<#root>

NAT-Device#

debug ip nat detailed

IP NAT detailed debugging is on
NAT-Device#

debug ip nat

IP NAT debugging is on

NAT-device#

show logging

Log Buffer (100000 bytes):

*May 18 23:52:20.296: NAT: address not stolen for 192.168.1.100, proto 6 port 52448
*May 18 23:52:20.296: NAT: Created portlist for proto tcp globaladdr 172.16.10.10
*May 18 23:52:20.296: NAT: Allocated Port for 192.168.1.100 -> 172.16.10.10:

wanted 52448 got 1024<-- confirms PAT is used

*May 18 23:52:20.296: NAT: Entry assigned id 5
*May 18 23:52:20.296: NAT: i: tcp (192.168.1.100, 52448) -> (10.20.30.40, 23) [63338]
*May 18 23:52:20.296: NAT: TCP Check for Limited ALG Support
*May 18 23:52:20.296: NAT: TCP

s=52448->1024

, d=23

<-- confirms NAT overload with PAT

*May 18 23:52:20.296: NAT:

s=192.168.1.100->172.16.10.10, d=10.20.30.40

[63338]NAT: dyn flow info download suppressed for flow 5

<-- shows inside translation

*May 18 23:52:20.297: NAT: attempting to setup alias for 172.16.10.10 (redundancy_name , idb NULL, flags
*May 18 23:52:20.299: NAT: o: tcp (10.20.30.40, 23) -> (172.16.10.10, 1024) [55748]
*May 18 23:52:20.299: NAT: TCP Check for Limited ALG Support
*May 18 23:52:20.299: NAT: TCP s=23,

d=1024->52448

<-- shows PAT on return traffic

*May 18 23:52:20.299: NAT: s=10.20.30.40, d=172.16.10.10->192.168.1.100 [55748]NAT: dyn flow info downlo

<#root>

NAT-Device#

debug platform software nat all

NAT platform all events debugging is on
NAT-Device#

*May 18 23:52:20.301: FMANRP-NAT: Received flow data, action:

ADD <-- first packet in flow ADD operation

*May 18 23:52:20.301: id 5, flags 0x5, domain 0

src_local_addr 192.168.1.100, src_global_addr 172.16.10.10

, dst_local_addr 10.20.30.40,

<-- source translation

dst_global_addr 10.20.30.40,

src_local_port 52448, src_global_port 1024

,

<-- port translation

dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 1,
outside_mapping_id 0, inside_mapping_type 2,
outside_mapping_type 0
<snip>

Vérification du matériel

Vérifiez que la règle NAT est correctement installée avec dans le matériel sous la région NAT 5

<#root>

```
NAT-Device#
show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_


Printing entries for region
NAT_1
 (370) type 6 asic 1
<-- NAT_1 empty due to no active flow


=========================================================
Printing entries for region NAT_2 (371) type 6 asic 1
=========================================================
Printing entries for region NAT_3 (372) type 6 asic 1
=========================================================
Printing entries for region NAT_4 (373) type 6 asic 1
=========================================================
Printing entries for region NAT_5 (374) type 6 asic 1
=========================================================
TAQ-2 Index-128 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:fffffffc:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:ac100a00:00000000
AD 10087000:00000073

TAQ-2 Index-129 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:
ffffff00


Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
c0a80100


AD 10087000:00000073


ffffff00 = 255.255.255.0 in hex for our subnet mask in NAT ACL


c0a80100 = 192.168.1.0 in hex for our network address in NAT ACL
```

Enfin, vous pouvez vérifier que le flux NAT est programmé dans la TCAM matérielle sous NAT_Region 1 lorsque le flux est actif

```
<#root>
NAT-Device#
show ip nat translations


Pro Inside global      Inside local        Outside local  Outside global
tcp 172.16.10.10:1024  192.168.1.100:20027 10.20.30.40:23 10.20.30.40:23

NAT-Device#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

Printing entries for region

NAT_1

(370) type 6 asic 1

<-- NAT region 1

==========
TAQ-2 Index-32 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:

06004e3b

:00000000:

00000017

:00000000:00000000:

0a141e28

:

c0a80164

AD 10087000:000000b0

TAQ-2 Index-33 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:

06000017

:00000000:

00000400

:00000000:00000000:

0a141e28

:

0a141e28

AD 10087000:000000b1

Starting at Index-32 Key1 from right to left:

c0a80164

- 192.168.1.100 (inside local source address)

0a141e28

- 10.20.30.40 (inside global address/outside local address)

00000017

- 23 (TCP destination port)

06004e3b

- TCP source port 20027 (4e3b) and TCP protocol 6

Starting at Index-33 Key1 from right to left:

0a141e28

 - 10.20.30.40 (outside global address/outside local address)

ac100a0a

 - 172.16.10.10 (inside global)

00000400

 - TCP inside global source port 1024

06000017

 - TCP protocol 6 and TCP source port 23

Débogages au niveau paquet

Le premier paquet d'un flux qui correspond à une règle NAT dans le matériel doit être envoyé au processeur du périphérique pour être traité. Pour afficher les sorties de débogage associées au chemin de punt, vous pouvez activer les traces de chemin de punt FED au niveau de débogage pour garantir que le paquet est punté. Le trafic NAT qui a besoin de ressources CPU passe dans la file d'attente CPU du trafic de transit.

Vérifiez si la file d'attente CPU du trafic de transit voit des paquets qui lui sont envoyés activement.

<#root>

NAT-DEVICE#

show platform software fed switch active punt cpuq clear <-- clear statistics

NAT-DEVICE#

show platform software fed switch active punt cpuq 18   <-- transit traffic queue

Punt CPU Q Statistics
==========

CPU Q Id :

18

CPU Q Name :

CPU_Q_TRANSIT_TRAFFIC

Packets received from ASIC : 0 **<-- no punt traffic for NAT**

Send to IOSd total attempts : 0
Send to IOSd failed count : 0
RX suspend count : 0
RX unsuspend count : 0
RX unsuspend send count : 0
RX unsuspend send failed count : 0
RX consumed count : 0
RX dropped count : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count : 0
RX packets dq'd after intack : 0
Active RxQ event : 0
RX spurious interrupt : 0
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

Replenish Stats for all rxq:

Number of replenish : 0
Number of replenish suspend : 0
Number of replenish un-suspend : 0

NAT-DEVICE#

show platform software fed switch active punt cpuq 18 **<-- after new translation**

Punt CPU Q Statistics
==========

CPU Q Id : 18
CPU Q Name : CPU_Q_TRANSIT_TRAFFIC

Packets received from ASIC : 5 **<-- confirms the UADP ASIC punts to**

Send to IOSd total attempts : 5
Send to IOSd failed count : 0
RX suspend count : 0
RX unsuspend count : 0
RX unsuspend send count : 0
RX unsuspend send failed count : 0
RX consumed count : 0
RX dropped count : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count : 5
RX packets dq'd after intack : 0
Active RxQ event : 5
RX spurious interrupt : 0
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

Replenish Stats for all rxq:

```
Number of replenish : 18
Number of replenish suspend : 0
Number of replenish un-suspend : 0
----------------------------------------
```

Dépannage de l'évolutivité NAT

Prise en charge matérielle actuelle du nombre maximal d'entrées NAT TCAM, comme illustré dans le tableau :

Remarque : chaque traduction NAT active nécessite 2 entrées TCAM.

Plateforme	Nombre maximal d'entrées TCAM
Catalyst 9300	5000
Catalyst 9400	14000
Catalyst 9500	14000
Hautes performances du Catalyst 9500	15500
Catalyst 9600	15500

Si vous suspectez un problème d'évolutivité, vous pouvez confirmer le nombre total de traductions NAT TCP/UDP à vérifier par rapport à une limite de plate-forme.

<#root>

```
NAT-Device#
```

show ip nat translations | count tcp

```
Number of lines which match regexp =
```

621 <-- current number of TCP translations

```
NAT-Device#
```

show ip nat translations | count udp

```
Number of lines which match regexp =
```

4894 <-- current number of UDP translations

Si vous avez épuisé votre espace NAT TCAM, le module NAT du commutateur ne peut pas traiter ces traductions. Dans ce scénario, le trafic soumis à la traduction NAT est envoyé au processeur du périphérique à traiter.

Cela peut provoquer une latence et peut être confirmé par des abandons qui s'incrémentent dans la file d'attente du contrôleur de plan de contrôle, qui est responsable du trafic NAT punt. La file d'attente du CPU où le trafic NAT va est le « trafic de transit ».

<#root>

NAT-Device#

show platform hardware fed switch active qos queue stats internal cpu policer

```
                          CPU Queue Statistics
============================================================================================
                                                (default) (set)     Queue        Queue
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
<snip>
14   13     Sw forwarding               Yes     1000      1000     0            0
15   8      Topology Control            Yes     13000     16000    0            0
16   12     Proto Snooping              Yes     2000      2000     0            0
17   6      DHCP Snooping               Yes     500       500      0            0

18   13     Transit Traffic             Yes     1000      1000     34387271     399507


<-- drops for NAT traffic headed towards the CPU


19   10     RPF Failed                  Yes     250       250      0            0
20   15     MCAST END STATION           Yes     2000      2000     0            0
<snip>
```

Confirmez l'espace TCAM NAT disponible dans le code 17.x. Cette sortie provient d'un 9300 avec le modèle NAT activé afin que l'espace soit optimisé.

<#root>

NAT-DEVICE#

show platform hardware fed switch active fwd-asic resource tcam utilization

```
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable

CAM Utilization for ASIC [0]
Table                  Subtype      Dir      Max      Used    %Used       V4        V6     MPLS    Other
-------------------------------------------------------------------------------------------------------
Mac Address Table      EM           I       32768       22    0.07%        0         0         0        22
Mac Address Table      TCAM         I        1024       21    2.05%        0         0         0        21
L3 Multicast           EM           I        8192        0    0.00%        0         0         0         0
L3 Multicast           TCAM         I         512        9    1.76%        3         6         0         0
L2 Multicast           EM           I        8192        0    0.00%        0         0         0         0
L2 Multicast           TCAM         I         512       11    2.15%        3         8         0         0
IP Route Table         EM           I       24576       16    0.07%       15         0         1         0
IP Route Table         TCAM         I        8192       25    0.31%       12        10         2         1
QOS ACL                TCAM         IO       1024       85    8.30%       28        38         0        19
Security ACL           TCAM         IO       5120      148    2.89%       27        76         0        45
Netflow ACL            TCAM         I         256        6    2.34%        2         2         0         2

PBR ACL                TCAM         I        5120       24    0.47%       18         6         0         0


Netflow ACL            TCAM         O         768        6    0.78%        2         2         0         2
Flow SPAN ACL          TCAM         IO       1024       13    1.27%        3         6         0         4
```

```
Control Plane          TCAM        I         512      281   54.88%     130      106         0        45
Tunnel Termination     TCAM        I         512       18    3.52%       8       10         0         0
Lisp Inst Mapping      TCAM        I         512        1    0.20%       0        0         0         1
Security Association   TCAM        I         256        4    1.56%       2        2         0         0
Security Association   TCAM        O         256        5    1.95%       0        0         0         5
CTS Cell Matrix/VPN
Label                  EM          O        8192        0    0.00%       0        0         0         0
CTS Cell Matrix/VPN
Label                  TCAM        O         512        1    0.20%       0        0         0         1
Client Table           EM          I        4096        0    0.00%       0        0         0         0
Client Table           TCAM        I         256        0    0.00%       0        0         0         0
Input Group LE         TCAM        I        1024        0    0.00%       0        0         0         0
Output Group LE        TCAM        O        1024        0    0.00%       0        0         0         0
Macsec SPD             TCAM        I         256        2    0.78%       0        0         0         2
```

Confirmez l'espace TCAM NAT disponible dans le code 16.x. Cette sortie provient d'un 9300 avec le modèle d'accès SDM, de sorte que l'espace disponible pour les entrées NAT TCAM n'est pas optimisé.

<#root>

```
NAT-DEVICE#
```

`show platform hardware fed switch active fwd-asic resource tcam utilization`

```
CAM Utilization for ASIC [0]
 Table                                              Max Values        Used Values
------------------------------------------------------------------------------
Unicast MAC addresses                               32768/1024         20/21
L3 Multicast entries                                 8192/512           0/9
L2 Multicast entries                                 8192/512           0/11
Directly or indirectly connected routes             24576/8192          5/23
QoS Access Control Entries                           5120               85
Security Access Control Entries                      5120              145
Ingress Netflow ACEs                                  256                8
Policy Based Routing ACEs                            1024               24 <-- NAT usage in PRB TCAM
Egress Netflow ACEs                                   768                8
Flow SPAN ACEs                                       1024               13
Control Plane Entries                                 512              255
Tunnels                                               512               17
Lisp Instance Mapping Entries                        2048                3
Input Security Associations                           256                4
SGT_DGT                                              8192/512           0/1
CLIENT_LE                                            4096/256           0/0
INPUT_GROUP_LE                                       1024               0
OUTPUT_GROUP_LE                                      1024               0
Macsec SPD                                            256                2
```

L'espace matériel disponible pour NAT TCAM peut être augmenté par une modification du modèle SDM pour préférer NAT. Cela permet d'allouer la prise en charge matérielle pour le nombre maximal d'entrées TCAM.

<#root>

```
NAT-Device#conf t
Enter configuration commands, one per line. End with CNTL/Z.
NAT-Device(config)#
```

sdm prefer nat

Si vous comparez SDM avant et après la conversion au modèle NAT, vous pouvez confirmer que l'espace TCAM utilisable est échangé pour les entrées de contrôle d'accès QoS et les entrées de contrôle d'accès PBR (Policy Based Routing).

PBR TCAM est l'emplacement où la NAT est programmée.

<#root>

```
NAT-Device#
```

show sdm prefer

```
Showing SDM Template Info

This is the Access template.
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 1024
L2 Multicast entries: 8192
Overflow L2 Multicast entries: 512
L3 Multicast entries: 8192
Overflow L3 Multicast entries: 512
Directly connected routes: 24576
Indirect routes: 8192
Security Access Control Entries: 5120
QoS Access Control Entries: 5120
```

Policy Based Routing ACEs: 1024 <-- NAT

<...snip...>

```
NAT-Device#
```

show sdm prefer

```
Showing SDM Template Info

This is the NAT template.
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 1024
L2 Multicast entries: 8192
Overflow L2 Multicast entries: 512
L3 Multicast entries: 8192
Overflow L3 Multicast entries: 512
Directly connected routes: 24576
Indirect routes: 8192
Security Access Control Entries: 5120
QoS Access Control Entries: 1024
```

```
Policy Based Routing ACEs: 5120       <-- NAT

<snip>
```

Traduction d'adresses uniquement (AOT)

Lâ€™AOA est un mécanisme qui peut être utilisé lorsque la fonction NAT est requise pour traduire uniquement le champ dâ€™adresse IP et non les ports de couche 4 dâ€™un flux. Si cela répond aux exigences, l'AOA peut augmenter considérablement le nombre de flux à traduire et à transférer dans le matériel.

- L'AOA est plus efficace lorsque la majorité des flux NAT sont destinés à un seul ensemble de destinations ou à un petit ensemble de destinations.
- L'AOA est désactivée par défaut. Une fois activé, il est nécessaire d'effacer les traductions NAT actuelles.

Remarque : l'AOT est uniquement pris en charge avec la NAT statique et la NAT dynamique qui n'incluent pas la PAT.

Cela signifie que les seules configurations NAT possibles qui autorisent l'AOT sont :

```
#ip nat inside source static <source> <destination>
#ip nat inside source list <list> pool <pool name>
```

Vous pouvez activer l'AOA avec cette commande :

<#root>

```
NAT-Device(config)#
```

no ip nat create flow-entries

Vérifiez que la règle NAT AOA est programmée correctement. Cette sortie provient d'une traduction NAT statique.

<#root>

```
NAT-DEVICE#
```

show running-config | include ip nat

```
ip nat outside
ip nat inside
```

no ip nat create flow-entries   <-- AOT enabled

```
ip nat inside source static 10.10.10.100 172.16.10.10      <-- static NAT enabled


NAT-DEVICE#
show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_


Printing entries for region NAT_1 (376) type 6 asic 1
=====================================================
Printing entries for region NAT_2 (377) type 6 asic 1
=====================================================
Printing entries for region NAT_3 (378) type 6 asic 1
=====================================================
Printing entries for region NAT_4 (379) type 6 asic 1
=====================================================
Printing entries for region NAT_5 (380) type 6 asic 1
=====================================================
TAQ-1 Index-864 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:ffffffff
Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:

0a0a0a64


AD 10087000:00000073

TAQ-1 Index-865 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:ffffffff:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:

ac100a0a

:00000000
AD 10087000:00000073


0a0a0a64 = 10.10.10.100 (inside local)
ac100a0a = 172.16.10.10 (inside global)
```

Vérifiez l'entrée AOA dans TCAM en confirmant que seules les adresses IP source et de destination sont programmées lorsque le flux devient actif.

<#root>

```
NAT-DEVICE#
show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_


Printing entries for region NAT_1 (376) type 6 asic 1
=====================================================
Printing entries for region NAT_2 (377) type 6 asic 1
=====================================================
TAQ-1 Index-224 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0000f000:00000000:00000000:00000000:00000000:00000000:ffffffff:ffffffff
Key1 00009000:00000000:00000000:00000000:00000000:00000000:

c0a80164:0a0a0a64 <-- no L4 ports, only source and destination IP is programmed
```

```
AD 10087000:000000b2

TAQ-1 Index-225 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:00000000:00000000:00000000:00000000:00000000:ffffffff:00000000
Key1 00009000:00000000:00000000:00000000:00000000:00000000:
```

ac100a0a

```
:00000000
AD 10087000:000000b3
```

0a0a0a64 = 10.10.10.100 in hex (inside local IP address)

c0a80164 = 192.168.1.100 in hex (outside local/outside global)
ac100a0a = 172.16.10.10 (inside global)

Informations connexes

- Guide de configuration NAT du Catalyst 9300 17.3.x
- Guide de configuration NAT du Catalyst 9400 17.3.x
- Guide de configuration NAT du Catalyst 9500 17.3.x
- Guide de configuration NAT du Catalyst 9600 17.3.x
- Assistance et documentation techniques - Cisco Systems

Interne Cisco Informations

CSCvz46804 Amélioration apportée à l'ajout d'un syslog lorsque les ressources NAT TCAM sont épuisées ou lorsqu'une entrée NAT ne peut pas être programmée correctement.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.