Validation des ACL de sécurité sur les commutateurs Catalyst 9000

Table des matières

Introduction

Ce document décrit comment vérifier et dépanner les listes de contrôle d'accès (ACL) sur les commutateurs de la gamme Catalyst 9000.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- C9200
- C9300
- C9400
- C9500
- C9600

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.

> **Remarque** : consultez le guide de configuration approprié pour connaître les commandes utilisées pour activer ces fonctions sur d'autres plates-formes Cisco.

Informations générales

Les listes de contrôle dâ€™accès filtrent le trafic lorsquâ€™il traverse un routeur ou un commutateur et autorisent ou refusent les paquets qui traversent des interfaces spécifiées. Une liste de contrôle dâ€™accès est un ensemble séquentiel de conditions dâ€™autorisation et de refus qui sâ€™appliquent aux paquets. Lorsqu'un paquet est reçu sur une interface, le commutateur compare les champs du paquet avec les listes de contrôle d'accès appliquées afin de vérifier que le paquet a les autorisations requises pour être transféré, sur la base des critères spécifiés dans les listes d'accès. Un par un, il teste les paquets par rapport aux conditions dâ€™une liste dâ€™accès. La première correspondance détermine si le commutateur accepte ou rejette les paquets. Comme le commutateur arrête le test après la première correspondance, l'ordre des conditions dans la liste est critique. Si aucune condition ne correspond, le commutateur rejette le paquet. S'il n'y a aucune restriction, le commutateur transfère le paquet ; sinon, le commutateur abandonne le paquet. Le commutateur peut utiliser des listes de contrôle dâ€™accès sur tous les paquets quâ€™il transfère.

Vous pouvez configurer des listes d'accès afin de fournir une sécurité de base à votre réseau. Si vous ne configurez pas de listes de contrôle dâ€™accès, tous les paquets qui passent par le commutateur peuvent être autorisés sur toutes les parties du réseau. Vous pouvez utiliser des listes de contrôle dâ€™accès afin de contrôler quels hôtes peuvent accéder aux différentes parties dâ€™un réseau ou pour décider quels types de trafic sont transférés ou bloqués au niveau des interfaces de routeur. Par exemple, vous pouvez transférer le trafic de messagerie mais pas le trafic Telnet.

Terminologie

AS	Entrée de contrôle d'accès (ACE) : une seule règle/ligne dans une liste de contrôle d'accès
ACL	Liste de contrôle d'accès (ACL) : groupe d'ACE appliqué à un port

DACL	DACL (Downloadable ACL) : liste de contrôle d'accès diffusée dynamiquement via la stratégie de sécurité ISE
PACL	ACL de port (PACL) : liste de contrôle d'accès appliquée à une interface de couche 2
RACL	ACL routée (RACL) - Une ACL appliquée à une interface de couche 3
VACL	VLAN ACL (VACL) : liste de contrôle d'accès appliquée à un VLAN
GACL	ACL de groupe (GACL) : liste de contrôle d'accès attribuée dynamiquement à un groupe d'utilisateurs ou à un client en fonction de leur identité
ACL IP	Sert à classer les paquets IPv4/IPv6. Ces règles contiennent divers champs et attributs de paquets de couche 3 et de couche 4, notamment, mais sans s'y limiter, les adresses IPv4 source et de destination, les ports source et de destination TCP/UDP, les indicateurs TCP et DSCP, etc.
MACL	MAC Address ACL (MACL) : permet de classer les paquets non IP. Les règles contiennent divers champs et attributs de couche 2, notamment l'adresse MAC source/de destination, l'un ou l'autre type, etc.
PO4L	Port opérateur de couche 4 (L4OP) : fait correspondre une logique autre que EQ (Equal To). GT (supérieur à), LT (inférieur à), NE (différent de) et RANGE (de-à)
VCU	Value Comparison Unit (VCU) : les opérations L4OP sont traduites en VCU afin d'effectuer la classification sur les en-têtes de couche 4
VMR	Résultat de masque de valeur (VMR) : une entrée ACE est programmée en interne dans TCAM en tant que VMR.
CGD	Base de données de groupes de classes (CGD) : emplacement où FMAN-FP stocke le contenu de la liste de contrôle d'accès
Classes	Identification des ACE dans CGD
centrage	Groupe de classes (CG) : groupe de classes sur la manière dont les listes de contrôle d'accès sont identifiées dans CGD
CGE	CGE (Class Group Entry) : entrée ACE stockée dans un groupe de classes
VENTILATEUR	Forwarding Manager (FMAN) : couche de programmation entre Cisco IOS® XE et le

	matériel
NOURRIR	Pilote de moteur de transfert (FED) : composant qui programme le matériel du périphérique

Exemples d'utilisation des ressources ACL

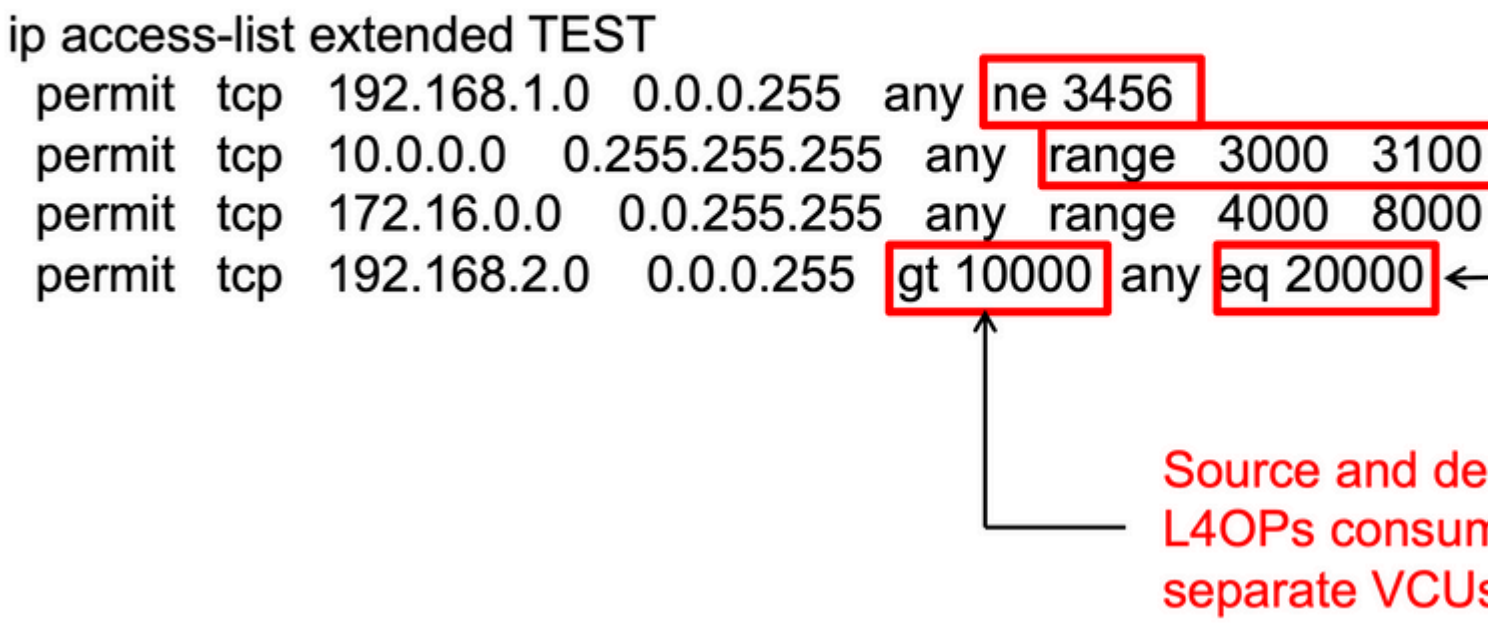
Trois exemples sont donnés ici afin de démontrer comment les ACL consomment TCAM, L4OP et VCU.

Exemple 1. TCAM IPv4

```
access-list 101 permit ip any 10.1.1.0 0.0.0.255
access-list 101 permit ip any 10.1.2.0 0.0.0.255
access-list 101 permit ip any 10.1.3.0 0.0.0.255
access-list 101 permit ip any 10.1.4.0 0.0.0.255
access-list 101 permit ip any 10.1.5.0 0.0.0.255
```

	Entrées TCAM	**OPl4**	**VCU**
Consommation	5	0	0

Exemple 2 . IPv4 TCAM/L4OP/VCU



<#root>

```
ip access-list extended TEST
10 permit tcp 192.168.1.0 0.0.0.255 any
```

neq 3456

<-- 1 L4OP, 1 VCU

```
20 permit tcp 10.0.0.0 0.255.255.255 any
```

range 3000 3100 <-- 1 L4OP, 2 VCU

```
30 permit tcp 172.16.0.0 0.0.255.255 any
```

range 4000 8000 <-- 1 L4OP, 2 VCU

```
40 permit tcp 192.168.2.0 0.0.0.255
```

gt 10000

```
 any
```

eq 20000 <-- 2 L4OP, 2 VCU

	Entrées TCAM	**OPl4**	**VCU**
Consommation	4	5	7

Exemple 3 . IPv6 TCAM/L4OP/VCU

Les ACE IPv6 utilisent deux entrées TCAM contre une pour IPv4. Dans cet exemple, quatre ACE consomment huit TCAM au lieu de quatre.

<#root>

```
ipv6 access-list v6TEST
sequence 10 deny ipv6 any 2001:DB8:C18::/48 fragments
sequence 20 deny ipv6 2001:DB8::/32 any
sequence 30 permit tcp host 2001:DB8:C19:2:1::F host 2001:DB8:C18:2:1::1
```

eq bgp <-- One L4OP & VCU

```
sequence 40 permit tcp host 2001:DB8:C19:2:1::F
```

eq bgp

```
 host 2001:DB8:C18:2:1::1
```

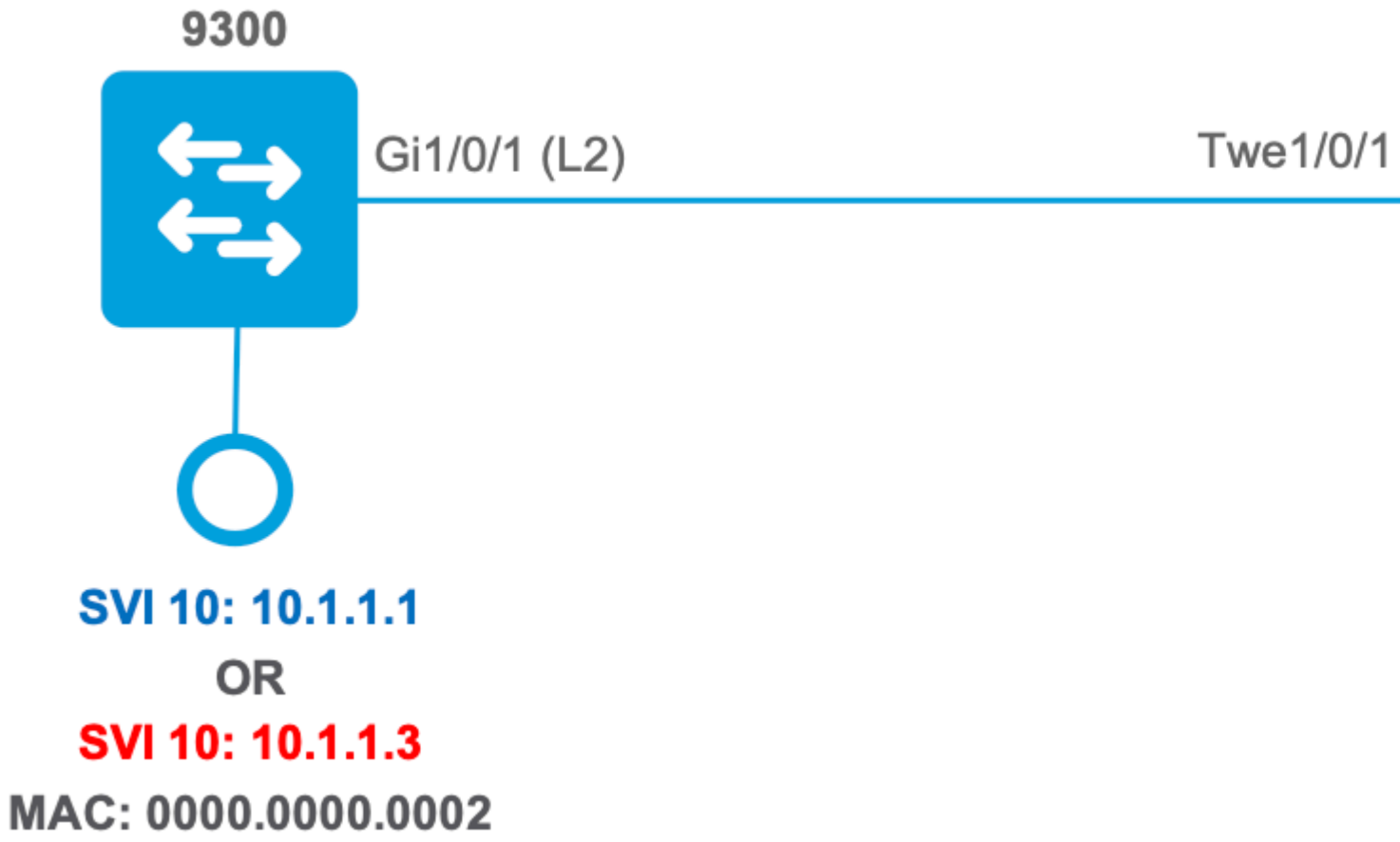
<-- One L4OP & VCU

	Entrées TCAM	**OPl4**	**VCU**

Consommation	8	2	2

Topologie

L'interface SVI 9300 VLAN 10 utilise l'une des deux adresses IP indiquées dans cette image, selon qu'un résultat de transfert ou d'abandon est indiqué dans les exemples.



Configuration et vérification

Cette section explique comment vérifier et dépanner la programmation des listes de contrôle dâ€™accès dans le logiciel et le matériel.

Scénario 1. PACL (IP ACL)

Les PACL sont attribuées à une interface de couche 2.

- Frontière de sécurité : ports ou VLAN
- Pièce jointe : interface de couche 2
- Direction : entrée ou sortie (une à la fois)
- Types de listes de contrôle d'accès pris en charge : ACL MAC et ACL IP (standard ou étendues)

Configuration de PACL avec IP ACL

<#root>

```
9500H(config)#
ip access-list extended TEST          <-- Create a named extended ACL

9500H(config-ext-nacl)#
permit ip host 10.1.1.1 any
9500H(config-ext-nacl)#
permit udp host 10.1.1.1 eq 1000 host 10.1.1.2


9500H#
show access-lists TEST                        <-- Display the ACL configured

Extended IP access list TEST
    10 permit ip host 10.1.1.1 any
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2
9500H(config)#
interface twentyFiveGigE 1/0/1        <-- Apply ACL to Layer 2 interface

9500H(config-if)#
ip access-group TEST in


9500H#
show running-config interface twentyFiveGigE 1/0/1

Building configuration...
Current configuration : 63 bytes
!
interface TwentyFiveGigE1/0/1
 ip access-group TEST in                              <-- Display the ACL applied to the interface

end
```

Vérification de PACL

Récupérez l'IF_ID associé à l'interface.

```
<#root>
9500H#
show platform software fed active ifm interfaces ethernet

Interface
```

```
 IF_ID

               State
--------------------------------------------------------------

TwentyFiveGigE1/0/1


0x00000008

          READY

<-- IF_ID value for Tw1/0/1
```

Vérifiez l'ID de groupe de classes (ID de GC) lié à l'IF_ID.

```
<#root>

9500H#

show platform software fed active acl interface 0x8       <-- IF_ID with leading zeros omitted


############################################################
########                                ##################
#######   Printing Interface Infos     #################
########                                ##################
############################################################

INTERFACE:

TwentyFiveGigE1/0/1                                    <-- Confirms the interface matches the IF_ID


MAC 0000.0000.0000
############################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028

Interface Type: Port                                      <-- Type: Port indicates Layer 2 interface



if-id: 0x0000000000000008                                 <-- IF_ID 0x8 is correct

    Input IPv4: Policy Handle: 0x5b000093

Policy Name: TEST                                       <-- The named ACL bound to this interface



    CG ID: 9                                           <-- Class Group ID for this entry



CGM Feature: [0] acl                                     <-- Feature is ACL
```

```
        Bind Order: 0
```

Informations ACL associées à l'ID CG.

<#root>

```
9500H#
```

show platform software fed active acl info acl-cgid 9 <-- The CG ID associated to the ACL TEST

```
##########################################################
#########                                ##################
########      Printing CG Entries       ##################
#########                                ##################
##########################################################
==================================
```

ACL CG (acl/9): TEST type: IPv4   <-- feature ACL/CG ID 9: ACl name TEST : ACL type IPv4

```
Total Ref count 1
---------------------------------
```

1 Interface

<-- ACL is applied to one interface

```
---------------------------------
  region reg_id: 10
    subregion subr_id: 0
      GCE#:1
```

#flds: 2

l4:N

```
 matchall:N deny:N
```

<-- #flds: 2 = two fields in entry | l4:N (no Layer 4 port match)

```
        Result: 0x01010000
```

ipv4_src: value

```
 =
```

0x0a010101

```
,
```

mask = 0xffffffff

<-- src 0x0a010101 hex = 10.1.1.1 | mask 0xffffffff = exact host match

ipv4_dst: value

=

0x00000000, mask = 0x00000000

<--

dst & mask = 0x00000000 = match any

GCE#:1 #flds: 4

l4:Y

matchall:N deny:N

<-- #flds: 4 = four fields in entry | l4:Y (ACE uses UDP port L4 match)

Result: 0x01010000

ipv4_src: value = 0x0a010101, mask = 0xffffffff <-- Exact match (host) 10.1.1.1

ipv4_dst: value = 0x0a010102, mask = 0xffffffff <-- Exact match (host) 10.1.1.2

ip_prot: start = 17, end = 17 <-- protocol 17 is UDP

l4_src: start = 1000, end = 1000 <-- matches eq 1000 (equal UDP port 1000)

Informations de stratégie sur l'ID de centralisation, ainsi que sur les interfaces qui utilisent l'ID de centralisation.

<#root>

9500H#

show platform software fed active acl policy 9 <-- Use the CG ID value

```
#########################################################
#########                              ##################
########     Printing Policy Infos     ##################
#########                              ##################
#########################################################
```

INTERFACE: TwentyFiveGigE1/0/1 <-- Interface with ACL applied

```
MAC 0000.0000.0000
#########################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028
    Interface Type: Port


if-id: 0x0000000000000008                              <-- The Interface IF_ID 0x8


------------

Direction: Input                                       <-- ACl is applied in the ingress direction


Protocol Type:IPv4                                     <-- Type is IPv4


    Policy Intface Handle: 0x880000c1
    Policy Handle: 0x5b000093

#########################################################
#########                              ##################
########      Policy information       #################
#########                              ##################
#########################################################
Policy handle      : 0x5b000093

Policy name        : TEST                              <-- ACL Name TEST


ID                 : 9                                 <-- CG ID for this ACL entry


Protocol           : [3] IPV4

Feature            : [1] AAL_FEATURE_PACL              <-- ASIC feature is PACL


Number of ACLs     : 1

#########################################################
## Complete policy ACL information
#########################################################
Acl number    : 1
====================================
Acl handle      : 0x320000d2
Acl flags       : 0x00000001

Number of ACEs

  : 3

<-- 3 ACEs: two explicit and the implicit deny entry


  Ace handle [1] : 0xb700010a
  Ace handle [2] : 0x5800010b


Interface(s):
```

```
        TwentyFiveGigE1/0/1                                  <-- The interface ACL is applied

##########################################################
#########                             ##################
########  Policy instance information  #################
#########                             ##################
##########################################################
Policy intf handle    : 0x880000c1
Policy handle         : 0x5b000093
ID                    : 9
Protocol              : [3] IPV4
Feature               : [1] AAL_FEATURE_PACL
Direction             : [1] Ingress
Number of ACLs        : 1
Number of VMRs        : 3------------
```

Vérifiez que la liste PACL fonctionne.

> **Remarque** : Lorsque vous entrez dans le champ show ip access-lists privileged EXEC , le nombre de correspondances affiché ne tient pas compte des paquets dont l'accès est contrôlé dans le matériel. Utilisez la commande d'exécution privilégiée {*switch_num*|active|standby}show platform software fed switch compteurs hardware{switch_num|active|standby}afin d'obtenir des statistiques de base sur les listes de contrôle d'accès matérielles pour les paquets commutés et routés.

<#root>

```
### Ping originated from neighbor device with source 10.1.1.1 ###


C9300#

ping 10.1.1.2 source g 1/0/1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.1                    <--- Ping source is permitted and p


!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms <-- 100% ping success



### Ping originated from neighbor device with source 10.1.1.3 ###

C9300#

ping 10.1.1.2 source g 1/0/1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.3                    <-- Ping source is denied (implicit
```

```
.....
Success rate is 0 percent (0/5)                                    <-- 0% ping success


### Confirm PACL drop ###

9500H#
show access-lists TEST


Extended IP access list TEST

    10 permit ip host 10.1.1.1 any                                 <-- Counters in this command do not
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2


9500H#
show platform software fed active acl counters hardware | i PACL Drop
Ingress IPv4 PACL Drop            (0x77000005):         11 frames    <-- Hardware level command displays

Ingress IPv6 PACL Drop            (0x12000012):          0 frames


<...snip...>
```

Scénario 2. PACL (MAC ACL)

Les PACL sont attribuées à une interface de couche 2.

- Frontière de sécurité : ports ou VLAN
- Pièce jointe : interface de couche 2
- Direction : entrée ou sortie (une à la fois)
- Types de listes de contrôle d'accès pris en charge : ACL MAC et ACL IP (standard ou étendues)

Configuration de PACL avec MAC ACL

```
<#root>

9500H#
show run | sec mac access-list


mac access-list extended
MAC-TEST           <-- MAC ACL named MAC-TEST



permit host 0001.aaaa.aaaa any             <-- permit host MAC to any dest MAC


9500H#
show access-lists MAC-TEST
```

```
Extended MAC access list MAC-TEST
    permit host 0001.aaaa.aaaa any

9500H#
```

show running-config interface twentyFiveGigE 1/0/1

```
Building configuration...

interface TwentyFiveGigE1/0/1
switchport access vlan 10
switchport mode access
```

mac access-group MAC-TEST in <-- Applied MACL to layer 2 interface

Vérification de PACL

Récupérez l'IF_ID associé à l'interface.

<#root>

```
9500H#
```

show platform software fed active ifm interfaces ethernet

```
Interface
```

IF_ID

```
              State
----------------------------------------------------------------
```

TwentyFiveGigE1/0/1

0x00000008

```
          READY
```

<-- IF_ID value for Tw1/0/1

Vérifiez l'ID de groupe de classes (ID de GC) lié à l'IF_ID.

<#root>

```
9500H#
```

show platform software fed active acl interface 0x8 <-- IF_ID with leading zeros omitted

```
#########################################################
########                              ##################
#######   Printing Interface Infos     #################
########                              ##################
#########################################################
```

```
INTERFACE: TwentyFiveGigE1/0/1                                  <-- Confirms the interface matches the IF

MAC 0000.0000.0000
##########################################################
    intfinfo: 0x7f489404e408
    Interface handle: 0x7e000028

Interface Type: Port                                          <-- Type: Port indicates Layer 2 interface



if-id: 0x0000000000000008                                     <-- IF_ID 0x8 is correct

    Input MAC: Policy Handle: 0xde000098

 Policy Name: MAC-TEST                                      <-- The named ACL bound to this interface



CG ID: 20                                                <-- Class Group ID for this entry



CGM Feature: [0] acl                                          <-- Feature is ACL

        Bind Order: 0
```

Informations ACL associées à l'ID CG.

```
<#root>

9500H#

show platform software fed active acl info acl-cgid 20  <-- The CG ID associated to the ACl MAC-TEST


##########################################################
#########                           ##################
########      Printing CG Entries      #################
#########                           ##################
##########################################################
==================================

ACL CG (acl/20): MAC-TEST type: MAC                             <-- feature ACL/CG ID 20: ACL name MAC-TES

Total Ref count 1
---------------------------------

1 Interface                                                     <-- Applied to one interface


---------------------------------
  region reg_id: 3
```

```
    subregion subr_id: 0
       GCE#:1 #flds: 2 l4:N matchall:N deny:N
         Result: 0x01010000

 mac_dest: value = 0x00, mask = 0x00                 <-- Mac dest: hex 0x00 mask 0x00 is "any destinati



mac_src: value = 0x1aaaaaaaa

,

mask = 0xffffffffffff


<-- Mac source: 0x1aaaaaaaa | hex with leading zeros omitted (0001.aaaa.aaaa) & mask 0xffffffffffff is h
```

Informations de stratégie sur l'ID de centralisation, ainsi que sur les interfaces qui utilisent l'ID de centralisation.

```
<#root>

9500H#

show platform software fed active acl policy 20      <-- Use the CG ID value


############################################################
#########                                ##################
########     Printing Policy Infos     ##################
#########                                ##################
############################################################


INTERFACE: TwentyFiveGigE1/0/1                             <-- Interface with ACL applied


MAC 0000.0000.0000
############################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028
    Interface Type: Port


if-id: 0x0000000000000008                                  <-- The Interface IF_ID 0x8


------------

Direction:  Input                                          <-- ACl is applied in the ingress direction


Protocol Type:MAC                                          <-- Type is MAC


    Policy Intface Handle: 0x30000c6
    Policy Handle: 0xde000098

############################################################
```

```
#########                                ##################
########          Policy information     ##################
#########                                ##################
#########################################################
Policy handle          : 0xde000098
Policy name            : MAC-TEST                          <-- ACL name is MAC-TEST


ID                     : 20                                <-- CG ID for this ACL entry


Protocol               : [1] MAC
Feature                : [1] AAL_FEATURE_PACL              <-- ASIC Feature is PACL


Number of ACLs         : 1

#########################################################
## Complete policy ACL information
#########################################################
Acl number : 1
====================================
Acl handle : 0xd60000dc
Acl flags : 0x00000001
Number of ACEs : 2                                         <-- 2 ACEs: one permit, and one implicit deny


  Ace handle [1] : 0x38000120
  Ace handle [2] : 0x31000121


Interface(s):


        TwentyFiveGigE1/0/1                                <-- Interface the ACL is applied


#########################################################
#########                                ##################
########  Policy instance information  ##################
#########                                ##################
#########################################################
Policy intf handle     : 0x030000c6
Policy handle          : 0xde000098
ID                     : 20
Protocol               : [1] MAC
Feature                : [1] AAL_FEATURE_PACL
Direction              : [1] Ingress
Number of ACLs         : 1
Number of VMRs         : 3------------
```

Vérifiez que la liste PACL fonctionne :

- La MACL autorise uniquement l'adresse source 0001.aaaa.aaaa.
- Comme il sâ€™agit dâ€™une liste de contrôle dâ€™accès MAC, un paquet ARP non IP est abandonné, ce qui entraîne lâ€™échec de la requête ping.

<#root>

Ping originated from neighbor device with Source MAC 0000.0000.0002

C9300#

ping 10.1.1.2 source vlan 10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
.....

Success rate is 0 percent (0/5)

C9300#

show ip arp

Protocol Address   Age (min) Hardware Addr   Type   Interface
Internet 10.1.1.2   0

Incomplete

       ARPA

<-- ARP is unable to complete on Source device

Monitor capture configured on Tw 1/0/1 ingress

9500H#

monitor capture 1 interface TwentyFiveGigE 1/0/1 in match any

9500H#

show monitor cap

Status Information for Capture 1
  Target Type:

 Interface: TwentyFiveGigE1/0/1, Direction: IN

9500H#sh monitor capture 1 buffer brief | inc ARP

    5   4.767385 00:00:00:00:00:02 b^F^R

ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1

    8   8.767085 00:00:00:00:00:02 b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1
   11 10.767452 00:00:00:00:00:02 b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1
   13 12.768125 00:00:00:00:00:02 b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1

<-- 9300 (10.1.1.1) sends ARP request, but since there is no reply 4 more ARP requests are sent

9500H#

```
show platform software fed active acl counters hardware | inc MAC PACL Drop
Ingress MAC PACL Drop                        (0x73000021): 937 frames        <-- Confirmed that ARP requ

Egress MAC PACL Drop                         (0x0200004c): 0 frames

<...snip...>
```

Scénario 3. RACL

RACL est attribué à une interface de couche 3, telle qu'une interface SVI ou une interface routée.

- Frontière de sécurité : différents sous-réseaux
- Pièce jointe : interface de couche 3
- Direction : entrée ou sortie
- Types de listes de contrôle d'accès pris en charge : IP ACL (standard ou étendues)

Configuration de RACL

<#root>

```
9500H(config)#

ip access-list extended TEST          <-- Create a named extended ACL


9500H(config-ext-nacl)#

permit ip host 10.1.1.1 any

9500H(config-ext-nacl)#

permit udp host 10.1.1.1 eq 1000 host 10.1.1.2



9500H#

show access-lists TEST                        <-- Display the ACL configured


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2

9500H(config)#

interface Vlan 10                     <-- Apply ACL to Layer 3 SVI interface


9500H(config-if)#

ip access-group TEST in



9500H#

show running-config interface Vlan 10


Building configuration...
```

```
Current configuration : 84 bytes
!
interface Vlan10
 ip access-group TEST in                              <-- Display the ACL applied to the interface

end
```

Vérification de RACL

Récupérez l'IF_ID associé à l'interface.

```
<#root>

9500H#

show platform software fed active ifm mappings l3if-le  <-- Retrieve the IF_ID for a Layer 3 SVI type po

Mappings Table

L3IF_LE                    Interface                              IF_ID             Type
------------------------------------------------------------------------------------------------
0x00007f8d04983958

Vlan10


0x00000026

        SVI_L3_LE

<-- IF_ID value for SVI 10
```

Vérifiez l'ID de groupe de classes (ID de GC) lié à l'IF_ID.

```
<#root>

9500H#

show platform software fed active acl interface 0x26  <-- IF_ID for SVI Vlan 10 with leading zeros omitt

#########################################################
########                              ##################
#######     Printing Interface Infos   #################
########                              ##################
#########################################################


INTERFACE: Vlan10                                        <-- Confirms the interface matches the IF_ID


MAC 0000.0000.0000
#########################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x6e000047
```

Interface Type: L3 **<-- Type: L3 indicates Layer 3 type interface**

if-id: 0x0000000000000026 **<-- IF_ID 0x26 is correct**

Input IPv4: Policy Handle: 0x2e000095

Policy Name: TEST **<-- The named ACL bound to this interface**

CG ID: 9 **<-- Class Group ID for this entry**

CGM Feature: [0] acl **<-- Feature is ACL**

Bind Order: 0

Informations ACL associées à l'ID CG.

<#root>

9500H#

show platform software fed active acl info acl-cgid 9 <-- The CG ID associated to the ACL TEST

```
############################################################
#########                                ##################
########      Printing CG Entries       #################
#########                                ##################
############################################################
==================================
```

ACL CG (acl/9): TEST type: IPv4

<-- feature ACL/CG ID 9: ACl name TEST : ACl type IPv4

```
Total Ref count 2
---------------------------------
```

2 Interface **<-- Interface count is 2. Applied to SVI 10 and as PACL to Tw1/0/**

```
---------------------------------
region reg_id: 10
  subregion subr_id: 0
    GCE#:1
```

#flds: 2

l4:N

matchall:N deny:N

<-- #flds: 2 = two fields in entry | l4:N (no Layer 4 port match)

Result: 0x01010000

ipv4_src: value

=

0x0a010101

,

mask = 0xffffffff

<-- src 0x0a010101 hex = 10.1.1.1 | mask 0xffffffff = exact host match

ipv4_dst: value

=

0x00000000, mask = 0x00000000

<--

dst & mask = 0x00000000 = match any

GCE#:1 #flds: 4

l4:Y

matchall:N deny:N

<-- #flds: 4 = four fields in entry | l4:Y (ACE uses UDP port L4 match)

Result: 0x01010000

ipv4_src: value = 0x0a010101, mask = 0xffffffff <-- Exact match (host) 10.1.1.1

ipv4_dst: value = 0x0a010102, mask = 0xffffffff <-- Exact match (host) 10.1.1.2

ip_prot: start = 17, end = 17 <-- protocol 17 is UDP

l4_src: start = 1000, end = 1000 <-- matches eq 1000 (equal UDP port 1000)

Informations de stratégie sur l'ID de centralisation, ainsi que sur les interfaces qui utilisent l'ID de centralisation.

<#root>

9500H#

show platform software fed active acl policy 9 <-- Use the CG ID Value

```
##########################################################
#########                                 ##################
########     Printing Policy Infos     ##################
#########                                 ##################
##########################################################
```

INTERFACE: Vlan10 <-- Interface with ACL applied

MAC 0000.0000.0000

```
##########################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x6e000047
    Interface Type: L3
```

if-id: 0x0000000000000026 <-- Interface IF_ID 0x26

Direction: Input <-- ACL applied in the ingress direction

Protocol Type:IPv4 <-- Type is IPv4

```
    Policy Intface Handle: 0x1c0000c2
    Policy Handle: 0x2e000095
```

```
##########################################################
#########                                 ##################
########        Policy information     ##################
#########                                 ##################
##########################################################
Policy handle        : 0x2e000095
```

Policy name : TEST <-- ACL name TEST

ID : 9

<-- CG ID for this ACL entry

Protocol : [3] IPV4

Feature : [27] AAL_FEATURE_RACL <-- ASIC feature is RACL

Number of ACLs : 1

```
##########################################################
## Complete policy ACL information
##########################################################
Acl number       : 1
====================================
Acl handle         : 0x7c0000d4
Acl flags          : 0x00000001
```

Number of ACEs   : 5   <-- 5 Aces: 2 explicit, 1 implicit deny, 2 ???

```
  Ace handle [1] : 0x0600010f
  Ace handle [2] : 0x8e000110
  Ace handle [3] : 0x3b000111
  Ace handle [4] : 0xeb000112
  Ace handle [5] : 0x79000113
```

Interface(s):

**   Vlan10   <-- The interface the ACL is applied**

```
##########################################################
#########                                ##################
########  Policy instance information  ##################
#########                                ##################
##########################################################
Policy intf handle     : 0x1c0000c2
Policy handle          : 0x2e000095
ID                     : 9
Protocol               : [3] IPV4
Feature                : [27] AAL_FEATURE_RACL
Direction              : [1] Ingress
Number of ACLs         : 1
Number of VMRs         : 4------------
```

Vérifiez que le RACL fonctionne.

> **Remarque** : Lorsque vous entrez dans le champ show ip access-lists privileged EXEC , le nombre de correspondances affiché ne tient pas compte des paquets dont l'accès est contrôlé dans le matériel. Utilisez le *matériel des compteurs de liste de contrôle dâ€™accès* show platform software fed switch{*switch_num*|active|standby}pour obtenir des statistiques de base sur les listes de contrôle dâ€™accès matérielles pour les paquets commutés et routés.

<#root>

Ping originated from neighbor device with source 10.1.1.1

```
C9300#
```

ping 10.1.1.2 source g 1/0/1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.1.1.1                          <--- Ping source is permitted and p


!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms <-- 100% ping success



### Ping originated from neighbor device with source 10.1.1.3 ###

C9300#

ping 10.1.1.2 source g 1/0/1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.3                          <-- Ping source is denied (implicit


.....

Success rate is 0 percent (0/5)                                        <-- 0% ping success


### Confirm RACL drop ###

9500H#

show access-lists TEST


Extended IP access list TEST


    10 permit ip host 10.1.1.1 any                                     <-- Counters in this command do not
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2


9500H#

show platform software fed active acl counters hardware | i RACL Drop
Ingress IPv4 RACL Drop              (0xed000007):         100 frames  <-- Hardware level command display


<...snip...>
```

Scénario 4 . VACL

Les VACL sont attribuées à un VLAN de couche 2.

- Frontière de sécurité : dans OU sur un VLAN
- Pièce jointe : VLAN/VLAN Map
- Direction : entrée et sortie en même temps
- Types de listes de contrôle d'accès pris en charge : ACL MAC et ACL IP (standard ou étendues)

Configurer la VACL

<#root>

```
ip access-list extended TEST

 10 permit ip host 10.1.1.1 any
 20 permit ip any host 10.1.1.1

ip access-list extended ELSE

 10 permit ip any any

vlan access-map VACL 10

 match ip address TEST
 action forward
vlan access-map VACL 20

 match ip address ELSE
 action drop

vlan filter VACL vlan-list 10



9500H#
sh vlan access-map VACL

Vlan access-map "VACL" 10
  Match clauses:
    ip address: TEST

 Action:

    forward

Vlan access-map "VACL" 20
  Match clauses:
    ip address: ELSE

 Action:

    drop

9500H#
sh vlan filter access-map VACL

VLAN Map VACL is filtering VLANs:

10
```

Vérifier la VACL

Récupérez l'IF_ID associé à l'interface.

```
<#root>

9500H#

show platform software fed active ifm interfaces vlan


Interface

IF_ID

               State
--------------------------------------------------------------------------

Vlan10                           0x00420010

        READY
```

Vérifiez l'ID de groupe de classes (ID de GC) lié à l'IF_ID.

```
<#root>

9500H#

show platform software fed active acl interface 0x420010  <-- IF_ID for the Vlan


##########################################################
########                              ##################
#######   Printing Interface Infos     #################
########                              ##################
##########################################################

INTERFACE: Vlan10                                              <-- Can be L2 only, with no vlan interfa


MAC 0000.0000.0000
##########################################################
    intfinfo: 0x7fc8cc7c7f48
    Interface handle: 0xf1000024
    Interface Type: Vlan
    if-id: 0x0000000000420010


Input IPv4:

 Policy Handle: 0xd10000a3

<-- VACL has both Ingress and Egress actions



Policy Name: VACL                                      <-- Name of the VACL used
```

CG ID: 530 **<-- Class Group ID for entry**

CGM Feature: [35] acl-grp **<-- Feature is ACL group, versus ACl**

Bind Order: 0

Output IPv4:

Policy Handle: 0xc80000a4

<-- VACL has both Ingress and Egress actions

Policy Name: VACL
CG ID: 530
CGM Feature: [35] acl-grp
Bind Order: 0

Informations ACL associées à l'ID du groupe GC.

Deux listes de contrôle dâ€™accès sont utilisées dans la même stratégie VACL nommée, regroupées dans ce groupe de listes de contrôle dâ€™accès

<#root>

9500H#

show platform software fed active acl info acl-grp-cgid 530 <-- use the group-id command versus gc ID

```
##########################################################
#########                                ##################
########    Printing CG Entries          #################
#########                                ##################
##########################################################
==================================
```

ACL CG (acl-grp/530): VACL type: IPv4 **<-- feature acl/group ID 530: name VA**

```
Total Ref count 2
---------------------------------
```

2 VACL **<-- Ingress and egress ACL direction**

```
---------------------------------
  region reg_id: 12
    subregion subr_id: 0
      GCE#:10 #flds: 2 l4:N matchall:N deny:N
        Result: 0x06000000
```

ipv4_src: value = 0x0a010101, mask = 0xffffffff **<-- permit from host 10.1.1.1 (see PACL exampl**

```
ipv4_dst: value = 0x00000000, mask = 0x00000000           <-- to any other host

      GCE#:20 #flds: 2 l4:N matchall:N deny:N
        Result: 0x06000000

ipv4_src: value = 0x00000000, mask = 0x00000000           <-- permit from any host



ipv4_dst: value = 0x0a010101, mask = 0xffffffff           <-- to host 10.1.1.1

      GCE#:10 #flds: 2 l4:N matchall:N deny:N
        Result: 0x05000000

 ipv4_src: value = 0x00000000, mask = 0x00000000           <-- This is the ACL named 'ELSE' which is per


        ipv4_dst: value = 0x00000000, mask = 0x00000000           <-- with VACL, the logic used was "per
```

Informations de stratégie sur l'ID de centralisation, ainsi que sur les interfaces qui utilisent l'ID de centralisation.

```
<#root>

9500H#

show platform software fed active acl policy 530     <-- use the acl-grp ID


############################################################
#########                                  ##################
########     Printing Policy Infos     ##################
#########                                  ##################
############################################################

INTERFACE: Vlan10
MAC 0000.0000.0000
############################################################
    intfinfo: 0x7fa15802a5d8
    Interface handle: 0xf1000024

Interface Type: Vlan                                      <-- Interface type is the Vlan, not a specific in



if-id: 0x0000000000420010                                 <-- the Vlan IF_ID matches Vlan 10

------------

Direction: Input                                              <-- VACL in the input direction
```

```
Protocol Type:IPv4
    Policy Intface Handle: 0x44000001
    Policy Handle: 0x29000090

#########################################################
#########                               ##################
########       Policy information      ##################
#########                               ##################
#########################################################
Policy handle       : 0x29000090
```

Policy name   : VACL   <-- the VACL policy is named 'VACL'

```
ID                  : 530
Protocol            : [3] IPV4
```

Feature   : [23] AAL_FEATURE_VACL   <-- ASIC feature is VACL

Number of ACLs   : 2   <-- 2 ACL used in the VACL: "TEST & ELSE"

```
#########################################################
## Complete policy ACL information
#########################################################
Acl number : 1
====================================
Acl handle : 0xa6000090
Acl flags : 0x00000001
Number of ACEs : 4
  Ace handle [1] : 0x87000107
  Ace handle [2] : 0x30000108
  Ace handle [3] : 0x73000109
  Ace handle [4] : 0xb700010a

Acl number : 2
====================================
Acl handle : 0x0f000091
Acl flags : 0x00000001
Number of ACEs : 1
  Ace handle [1] : 0x5800010b

Interface(s):
        Vlan10
#########################################################
#########                               ##################
########  Policy instance information  ##################
#########                               ##################
#########################################################
Policy intf handle    : 0x44000001
Policy handle         : 0x29000090
```

ID   : 530   <-- 530 is the acl group ID

```
Protocol              : [3] IPV4
Feature               : [23] AAL_FEATURE_VACL
```

Direction   : [1] Ingress   <-- Ingress VACL direction

```
Number of ACLs        : 2
Number of VMRs        : 4------------
Direction:  Output
Protocol Type:IPv4
    Policy Intface Handle: 0xac000002
    Policy Handle: 0x31000091

#########################################################
#########                               ##################
########        Policy information     ##################
#########                              ##################
#########################################################
Policy handle        : 0x31000091
Policy name          : VACL
ID                   : 530
Protocol             : [3] IPV4
Feature              : [23] AAL_FEATURE_VACL
Number of ACLs       : 2

#########################################################
## Complete policy ACL information
#########################################################
Acl number    : 1
====================================
Acl handle      : 0xe0000092
Acl flags       : 0x00000001
Number of ACEs  : 4
  Ace handle [1] : 0xf500010c
  Ace handle [2] : 0xd800010d
  Ace handle [3] : 0x4c00010e
  Ace handle [4] : 0x0600010f

Acl number    : 2
====================================
Acl handle      : 0x14000093
Acl flags       : 0x00000001
Number of ACEs : 1
  Ace handle [1] : 0x8e000110

Interface(s):
        Vlan10
#########################################################
#########                               ##################
########  Policy instance information  ##################
#########                              ##################
#########################################################
Policy intf handle    : 0xac000002
Policy handle         : 0x31000091
ID                    : 530                             <-- 530 is the acl group ID


Protocol              : [3] IPV4
Feature               : [23] AAL_FEATURE_VACL
Direction             : [2] Egress                      <-- Egress VACL direction


Number of ACLs        : 2
Number of VMRs        : 4------------
```

Vérifiez que la VACL fonctionne.

- Le dépannage est le même scénario que pour les sections PACL et RACl. Reportez-vous à ces sections pour plus de détails sur le test ping.
- Requête ping de 10.1.1.3 vers 10.1.1.2 refusée par la stratégie de liste de contrôle dâ€™accès appliquée.
- Vérifiez la commande platform drop.

```
<#root>

9500H#

show platform software fed active acl counters hardware | inc VACL Drop


Ingress IPv4 VACL Drop

              (0x23000006):

1011 frames      <-- Hardware level command displays drops against VACL


<...snip...>
```

Scénario 5. ACL groupe/client (DACL)

Les listes de contrôle dâ€™accès groupe/client sont appliquées dynamiquement à un groupe dâ€™utilisateurs ou à un client en fonction de leur identité. Elles sont également parfois appelées DACL.

- Frontière de sécurité : Client (niveau interface client)
- Pièce jointe : par interface client
- Direction : entrée uniquement
- Types de listes de contrôle d'accès pris en charge : ACL MAC et ACL IP (standard ou étendues)

Configurer la GACL

```
<#root>

Cat9400#

show run interface gigabitEthernet 2/0/1

Building configuration...

Current configuration : 419 bytes
!
interface GigabitEthernet2/0/1
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 5


ip access-group ACL-ALLOW in                    <-- This is the pre-authenticated ACL (deny ip any any)

 authentication periodic
```

```
 authentication timer reauthenticate server
 access-session control-direction in
 access-session port-control auto
 no snmp trap link-status
 mab
 dot1x pae authenticator
 spanning-tree portfast


service-policy type control subscriber ISE_Gi2/0/1

end

Cat9400#

show access-session interface gigabitEthernet 2/0/1 details

            Interface:  GigabitEthernet2/0/1


 IIF-ID:  0x1765EB2C               <-- The IF_ID used in this example is dynamic


 MAC Address:  000a.aaaa.aaaa            <-- The client MAC

         IPv6 Address:  Unknown
         IPv4 Address:  10.10.10.10
            User-Name:  00-0A-AA-AA-AA-AA


Status:  Authorized               <-- Authorized client

               Domain:  VOICE
       Oper host mode:  multi-auth
     Oper control dir:  in
      Session timeout:  300s (server), Remaining: 182s
       Timeout action:  Reauthenticate
    Common Session ID:  27B17A0A000003F499620261
      Acct Session ID:  0x000003e7
               Handle:  0x590003ea
       Current Policy:  ISE_Gi2/0/1



Server Policies:

              ACS ACL:

xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

  <-- The ACL pushed from ISE server



Method status list:
       Method           State
        dot1x           Stopped


 mab           Authc Success                                    <-- Authenticated via MAB (Mac authent


Cat9400#

show ip access-lists xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e
```

```
Extended IP access list xACSACLx-IP-MAB-FULL-ACCESS-GOOD-59fb6e5e

 1 permit ip any any                                                    <-- ISE pushed a permit ip any an
```

Vérifier la GACL

ID de groupe de centralisation lié à iif-id.

```
<#root>

Cat9400#

show platform software fed active acl interface 0x1765EB2C                <-- The IF_ID from the access

############################################################
########                                ##################
#######    Printing Interface Infos    #################
########                                ##################
############################################################

INTERFACE: Client MAC

000a.aaaa.aaaa

                                              <-- Client MAC matches the access-session output

MAC

000a.aaaa.aaaa

############################################################
    intfinfo: 0x7f104820cae8
    Interface handle: 0x5a000110

Interface Type: Group                                                     <-- This is a group ident


IIF ID: 0x1765eb2c

    Input IPv4: Policy Handle: 0x9d00011e

  Policy Name: ACL-ALLOW:xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

:

<-- DACL name matches



CG ID: 127760                                                           <-- The ACL group ID

       CGM Feature: [35]

acl-grp

        Bind Order: 0
```

Informations ACL associées à l'ID GC du groupe.

```
<#root>

Cat9400#

show platform software fed active acl info acl-grp-cgid 127760                    <-- the CG ID

##########################################################
#########                             ##################
########      Printing CG Entries      #################
#########                             ##################
##########################################################
====================================
ACL CG (

acl-grp/127760

):

ACL-ALLOW:xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

: type: IPv4

<-- Group ID & ACL name are correct


Total Ref count 1
---------------------------------

1 CGACL                                                                          <-- 1

---------------------------------
  region reg_id: 1
    subregion subr_id: 0
      GCE#:1 #flds: 2 l4:N matchall:N deny:N
        Result: 0x04000000


 ipv4_src: value = 0x00000000, mask = 0x00000000                                  <-- Permits I
        ipv4_dst: value = 0x00000000, mask = 0x00000000

      GCE#:10 #flds: 2 l4:N matchall:N deny:N
        Result: 0x04000000
        ipv4_src: value = 0x00000000, mask = 0x00000000
        ipv4_dst: value = 0x00000000, mask = 0x00000000
```

Scénario 6. Journalisation ACL

Le logiciel du périphérique peut fournir des messages syslog sur les paquets autorisés ou refusés par une liste d'accès IP standard. Tout paquet qui correspond à la liste de contrôle dâ€™accès entraîne lâ€™envoi dâ€™un message de journal dâ€™informations sur le paquet à la console. Le niveau des messages consignés sur la console est contrôlé par leconsole d'enregistrementpour contrôler les messages Syslog.

- Les messages du journal des ACL ne sont pas pris en charge pour les ACL utilisées avec Unicast Reverse Path Forwarding (uRPF). Il est uniquement pris en charge pour RACL.
- Le journal ACL dans la direction de sortie n'est pas pris en charge pour les paquets qui sont générés à partir du plan de contrôle du périphérique.

- Le routage est effectué dans le matériel et le logiciel de connexion, de sorte que si un grand nombre de paquets correspondent à une entrée de contrôle d'accès permit ou deny contenant un mot-clé de journal, le logiciel ne peut pas correspondre au taux de traitement matériel et tous les paquets ne peuvent pas être enregistrés.
- Le premier paquet qui déclenche la liste de contrôle dâ€™accès génère immédiatement un message de consignation et les paquets suivants sont collectés à intervalles de 5 minutes avant dâ€™apparaître ou dâ€™être consignés. Le message du journal comprend le numéro de la liste d'accès, si le paquet a été autorisé ou refusé, l'adresse IP source du paquet et le nombre de paquets provenant de cette source autorisés ou refusés au cours de l'intervalle de 5 minutes précédent.
- Reportez-vous au guide de configuration de la sécurité approprié, Cisco IOS XE, comme indiqué dans la section Informations connexes pour obtenir des détails complets sur le comportement et les restrictions du journal des listes de contrôle dâ€™accès.

Exemple de journal PACL :

Cet exemple montre un cas négatif, où le type de liste de contrôle d'accès et le mot clé log ne fonctionnent pas ensemble.

```
<#root>

9500H#

show access-lists TEST


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any

log             <-- Log keyword applied to ACE entry


    20 deny ip host 10.1.1.3 any

log


9500H(config)#

interface twentyFiveGigE 1/0/1

9500H(config-if)#

ip access-group TEST in           <-- apply logged ACL
Switch Port ACLs are not supported for LOG!        <-- message indicates this is an unsupported combinat
```

Exemple de journal RACL (Deny) :

```
<#root>

9500H#

show access-lists TEST


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any

log            <-- Log keyword applied to ACE entry
```

```
    20 deny ip host 10.1.1.3 any
log


9500H(config)#
interface vlan 10


9500H(config-if)#
ip access-group TEST in          <-- ACL applied to SVI

### Orginate ICMP from 10.1.1.3 to 10.1.1.2 (denied by ACE) ###

C9300#
ping 10.1.1.2 source vlan 10 repeat 110

Type escape sequence to abort.


Sending 10, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.3
..........

Success rate is 0 percent (0/110)


9500H#
show access-list TEST


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any log

 20 deny ip host 10.1.1.3 any log (110 matches)  <-- Matches increment in show access-list command


9500H#
show platform software fed active acl counters hardware | inc RACL

Ingress IPv4 RACL Drop          (0xed000007):            0 frames

Ingress IPv4 RACL Drop and Log  (0x93000009):          110 frames   <-- Aggregate command shows hits on

%SEC-6-IPACCESSLOGDP: list TEST denied icmp 10.1.1.3 -> 10.1.1.2 (8/0), 10 packets  <-- Syslog message i
```

Exemple de journal RACL (Permit) :
Lorsqu'une instruction log est utilisée pour une instruction permit, le compteur logiciel atteint show double the number of packets sent.

```
<#root>

C9300#
```

```
ping 10.1.1.2 source vlan 10 repeat 5          <-- 5 ICMP Requests are sent


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 1/1/1 ms

9500H#

show access-lists TEST


Extended IP access list TEST


 10 permit ip host 10.1.1.1 any log (10 matches)  <-- Hit counter shows 10


    20 deny ip host 10.1.1.3 any log (115 matches)
```

Dépannage

Statistiques ACL

Lorsque vous dépannez un problème de liste de contrôle dâ€™accès, il est essentiel de comprendre comment et où les statistiques de liste de contrôle dâ€™accès sont mesurées par le périphérique.

- Les statistiques ACL sont collectées à un niveau agrégé, et non par niveau ACE.
- Le matériel ne peut pas autoriser les statistiques par ACE ou par ACL.
- Des statistiques telles que les paquets Refuser, Journal et transmis par le processeur sont collectées.
- Les statistiques des paquets MAC, IPv4 et IPv6 sont collectées séparément.
- show platform software fed switch active acl counters hardware peut être utilisé afin d'afficher des statistiques agrégées.

Effacement des statistiques ACL

Lors du dépannage d'un problème de liste de contrôle d'accès, il peut être utile d'effacer les différents compteurs de liste de contrôle d'accès afin d'obtenir de nouveaux décomptes de ligne de base.

- Ces commandes vous permettent d'effacer les statistiques des compteurs de listes de contrôle d'accès logicielles et matérielles.
- Lorsque vous dépannez des événements de correspondance/correspondance de liste de contrôle d'accès, il est recommandé d'effacer la liste de contrôle d'accès appropriée pour les correspondances de base récentes ou pertinentes.

<#root>

```
clear platform software fed active acl counters hardware

 (clears the hardware matched counters)

clear ip access-list counters
```

```
 (clears the software matched counters - IPv4)
```

```
clear ipv6 access-list counters
```

```
 (clears the software matched counters - IPv6)
```

Que se passe-t-il lorsque ACL TCAM est épuisé ?

- Les ACL sont toujours appliquées dans la TCAM matérielle. Si TCAM est déjà utilisé par des listes de contrôle d'accès configurées précédemment, les nouvelles listes de contrôle d'accès n'obtiennent pas les ressources ACL nécessaires à la programmation.

- Si une liste de contrôle d'accès est ajoutée après l'épuisement de la TCAM, tous les paquets sont abandonnés pour l'interface à laquelle elle est connectée.

- L'action de maintenir une liste de contrôle d'accès dans le logiciel est appelée **Déchargement**.
- Lorsque des ressources deviennent disponibles, le commutateur tente automatiquement de programmer les listes de contrôle dâ€™accès dans le matériel. En cas de succès, les listes de contrôle dâ€™accès sont transmises au matériel et les paquets commencent à être transférés.
- L'action de programmation d'une liste de contrôle d'accès détenue par logiciel dans TCAM est appelée **Rechargement**.

- PACL, VACL, RACL et GACL peuvent être déchargés/rechargés indépendamment l'un de l'autre.

Épuisement TCAM ACL

- Lâ€™interface à laquelle la liste de contrôle dâ€™accès nouvellement ajoutée est appliquée commence à abandonner des paquets jusquâ€™à ce que les ressources matérielles deviennent disponibles.
- Les clients GACL passent à l'état UnAuth.

Épuisement VCU

- Une fois la limite des L4OP dépassée ou les VCU dépassées, le logiciel effectue l'extension des ACL et crée de nouvelles entrées ACE afin d'effectuer une action équivalente sans utiliser les VCU.
- Une fois que cela se produit, TCAM peut être épuisé à partir de ces entrées ajoutées.

Erreurs Syslog ACL

Si vous manquez d'une ressource ACL de sécurité particulière, les messages SYSLOG sont générés par le système (interface, VLAN, étiquette, etc., les valeurs peuvent différer).

Message du journal ACL	Définition	Action de récupération
%ACL_ERRMSG-4-UNLOADED : Commutateur 1 alimenté : l'entrée <ACL> sur l'interface <interface> n'est pas programmée dans le matériel et le trafic est abandonné.	La liste de contrôle dâ€™accès est déchargée (conservée dans le logiciel)	Examinez l'échelle TCAM. Si l'échelle est dépassée, reconcevez les ACL.
%ACL_ERRMSG-6-REMOVED : 1 alimentation : la configuration déchargée pour l'entrée <ACL> sur l'interface <interface> a été supprimée pour l'étiquette <label>asic<number>.	La configuration ACL déchargée est supprimée de lâ€™interface	La liste de contrôle d'accès a déjà été supprimée, aucune action à entreprendre
%ACL_ERRMSG-6-RELOADED : 1 alimentation : l'entrée <ACL> sur l'interface <interface> a été chargée dans le matériel pour l'étiquette <label> sur asic<number>.	La liste de contrôle dâ€™accès est maintenant installée dans le matériel	Le problème de la liste de contrôle dâ€™accès est désormais résolu au niveau matériel, aucune action à entreprendre
%ACL_ERRMSG-3-ERROR : 1 alimentation : la configuration d'entrée <ACL> IP ACL <NAME> n'est pas appliquée sur <interface> à l'ordre de liaison <number>.	Autres types dâ€™erreurs ACL (telles que dot1x ACL install failure)	Confirmer que la configuration ACL est prise en charge et que le TCAM est évolutif
%ACL_ERRMSG-6-GACL_INFO : Commutateur 1 R0/0 : fed : la journalisation n'est pas prise en charge pour GACL.	Une option de journal est configurée pour la GACL	GACL ne prend pas en charge les journaux. Supprimer les instructions de journal de la GACL.
%ACL_ERRMSG-6-PACL_INFO : Commutateur 1 R0/0 : fed : la journalisation n'est pas prise en charge pour PACL.	Une option de journal est configurée pour PACL	PACL ne prend pas en charge les journaux. Supprimez les instructions de journal de la liste PACL.
%ACL_ERRMSG-3-ERROR : Commutateur 1 R0/0 : fed : ACL du groupe IPv4 en entrée implicit_deny : <nom> : la configuration n'est pas appliquée sur l'adresse MAC du client 0000.0000.0000.	(dot1x) La liste de contrôle d'accès ne s'applique pas au port cible	Confirmer que la configuration ACL est prise en charge et que le TCAM est évolutif

Scénarios de ressources épuisées et actions de récupération

Scénario 1. Liaison ACL	Action de récupération
• Une liste de contrôle dâ€™accès est créée et appliquée à une interface ou à un VLAN. • La liaison échoue en raison de conditions « hors ressources », telles que l'épuisement de la TCAM. • Aucune ACE de la liste de contrôle d'accès ne peut être programmée dans TCAM. Lâ€™ACL reste à lâ€™état **UNLOADED**. • Dans l'état **UNLOADED**, tout le trafic (y compris les paquets de contrôle) est abandonné sur l'interface jusqu'à ce que le problème soit résolu.	Reconcevez la liste de contrôle d'accès afin de réduire l'utilisation de la TCAM.
Scénario 2. Modification ACL	**Action de récupération**
• Une liste de contrôle d'accès est créée et appliquée à une interface, et d'autres entrées ACE sont ajoutées à cette liste de contrôle d'accès lorsqu'elle est appliquée aux interfaces. • Si TCAM ne dispose pas de ressources, l'opération de modification échoue. • Aucune ACE de la liste de contrôle d'accès ne peut être programmée dans TCAM. L'ACL reste à l'état **UNLOADED**. • Dans l'état **UNLOADED**, tout le trafic (y compris les paquets de contrôle) est abandonné sur l'interface jusqu'à ce que le problème soit résolu. • Les entrées ACL existantes échouent également dans l'état **UNLOADED** jusqu'à ce que cela soit corrigé.	Reconcevez la liste de contrôle d'accès afin de réduire l'utilisation de la TCAM.
Scénario 3. Nouvelle liaison ACL	**Action de récupération**
• La reconnexion dâ€™une liste de contrôle dâ€™accès consiste à attacher une liste à une interface, puis à attacher une autre liste à la même interface sans détacher la première liste. • La première liste de contrôle dâ€™accès est créée et attachée. • Une liste de contrôle d'accès plus grande, portant un nom différent et le même protocole (IPv4/IPv6), est créée et connectée à la même interface. • Le périphérique a réussi à détacher la première liste de contrôle dâ€™accès et tente de joindre la nouvelle à cette interface.	Reconcevez la liste de contrôle d'accès afin de réduire l'utilisation de la TCAM.

• Si TCAM ne dispose pas de ressources, l'opération de reconnexion échoue. • Aucune ACE de la liste de contrôle d'accès ne peut être programmée dans TCAM. Lâ€™ACL reste à lâ€™état **UNLOADED**. • Dans l'état **UNLOADED**, tout le trafic (y compris les paquets de contrôle) est abandonné sur l'interface jusqu'à ce que le problème soit résolu.	
Scénario 4 . Lier une liste de contrôle d'accès vide (Null)	**Action de récupération**
• Une liste de contrôle dâ€™accès sans entrée ACE est créée et attachée à une interface. • Le système crée cette liste de contrôle d'accès en interne avec une autorisation « any ACE » et l'attache à l'interface dans le matériel (tout le trafic est autorisé dans cet état). • Les entrées ACE sont ensuite ajoutées à la liste de contrôle d'accès avec le même nom ou numéro. Le système programme TCAM à mesure que chaque ACE est ajouté. • Si TCAM manque de ressources lors de l'ajout d'entrées ACE, l'ACL passe à l'état **UNLOADED**. • Dans l'état **UNLOADED**, tout le trafic (y compris les paquets de contrôle) est abandonné sur l'interface jusqu'à ce que le problème soit résolu. • Les entrées ACL existantes échouent également dans l'état **UNLOADED** jusqu'à ce que cela soit corrigé.	Reconcevez la liste de contrôle d'accès afin de réduire l'utilisation de la TCAM.

Vérifier lâ€™échelle ACL

Cette section traite des commandes permettant de déterminer lâ€™échelle des listes de contrôle dâ€™accès et lâ€™utilisation de TCAM.

Résumé de la liste d'accès FMAN :

Identifiez les ACL configurées et le nombre total d'ACE par ACL.

```
<#root>

9500H#

show platform software access-list f0 summary


Access-list
```

```
                          Index        Num Ref
 Num ACEs

-------------------------------------------------------------------------
TEST

                                    1            1             2
<-- ACL TEST contains 2 ACE entries


ELSE                                2            1             1
DENY                                3            0             1
```

Utilisation ACL :

<#root>

9500H#

show platform software fed active acl usage

```
##########################################################
########                                ##################
#######      Printing Usage Infos      ##################
########                                ##################
##########################################################
#####
```

ACE Software VMR max:196608 used:283   <-- Value/Mask/Result entry usage

```
##########################################################
==========================================================================================================
```

Feature Type

ACL Type

Dir

Name

Entries Used

```
VACL                    IPV4            Ingress          VACL                    4
```

<-- Type of ACL Feature, type of ACL, Direction ACL applied, name of ACL, and number of TCAM entries con

```
==========================================================================================================
Feature Type            ACL Type        Dir              Name                    Entries Used
RACL                    IPV4            Ingress          TEST                    5
```

Utilisation de TCAM (17.x) :

La commande d'utilisation TCAM présente des différences significatives entre les trains 16.x et 17.x.

<#root>

9500H#

show platform hardware fed 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

Security ACL Ipv4

TCAM

I

7168

16

0.22%

16 0 0 0

Security ACL Non Ipv4 TCAM I 5120 76 1.48% 0 36 0 40

Security ACL Ipv4 TCAM

O

7168 18 0.25% 18 0 0 0

Security ACL Non Ipv4 TCAM O 8192 27 0.33% 0 22 0 5

<...snip...>

```
<-- Percentage used and other counters about ACL consumption
<-- Dir = ACL direction (Input/Output ACl)
```

Utilisation de TCAM (16.x) :

La commande d'utilisation TCAM présente des différences significatives entre les trains 16.x et 17.x.

```
<#root>

C9300#

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

CAM Utilization for ASIC [0]
 Table                                              Max Values

Used Values


--------------------------------------------------------------------------------


 Security Access Control Entries                     5120

 126         <-- Total used of the Maximum
<...snip...>
```

Modèle SDM personnalisé (réallocation TCAM)

Utilisation de Cisco IOS XE Benghaluru 17.4.1 vous pouvez configurer un modèle SDM personnalisé pour les fonctionnalités ACL en utilisant la sdm prefer custom aclerasecat4000_flash:.

Pour plus d'informations sur la configuration et la vérification de cette fonctionnalité, reportez-vous au Guide de configuration de la gestion du système, Cisco IOS XE Benghaluru 17.4.x (commutateurs Catalyst 9500).

Certaines configurations et vérifications de base sont indiquées dans cette section.

Vérifiez le modèle SDM actuel :

```
<#root>

9500H#

show sdm prefer


Showing SDM Template Info

This is the Core template.                                                    <-- Core SD


  Security Ingress IPv4 Access Control Entries*:         7168  (current) - 7168  (proposed)  <-- IPv4 AC
```

```
  Security Ingress Non-IPv4 Access Control Entries*:     5120  (current) - 5120  (proposed)
  Security Egress IPv4 Access Control Entries*:          7168  (current) - 7168  (proposed)
  Security Egress Non-IPv4 Access Control Entries*:      8192  (current) - 8192  (proposed)

  <...snip...>


9500H#

show sdm prefer custom user-input

Custom Template Feature Values are not modified

<-- No customization to SDM
```

Modifiez le modèle SDM actuel :

- 9500H(config)#**sdm prefer custom acl**
  9500H(config-sdm-acl)#**acl-ingress 26 priority 1 <â€" applique la nouvelle valeur 26K. (priorité traitée dans le guide de configuration)**
  9500H(config-sdm-acl)#**acl-egress 20 priorité 2**
  9500H(config-sdm-acl)#**sortie**
  Utilisation show sdm prefer custom afin de voir les valeurs proposées et sdm prefer custom commit afin d'appliquer « afficher les modifications » via cette CLI.
- Vérifiez les modifications apportées au profil SDM.
- 9500H#**show sdm prefer custom**

Affichage des informations du modèle SDM :

Il s'agit du modèle personnalisé avec ses détails.
Entrées de contrôle d'accès de sécurité en entrée* : **12288 (actuel) - 26624 (proposé) <â€" Utilisation actuelle et proposée (26 Ko proposés)**
Entrées de contrôle d'accès de sécurité en sortie* : **15360 (actuel) - 20480 (proposé)**

9500H#**show sdm prefer custom user-input**

ENTRÉE UTILISATEUR DE FONCTIONNALITÉ ACL
Valeurs d'entrée utilisateur
==========

PRIORITÉ DU NOM DE FONCTION **ÉCHELLE**

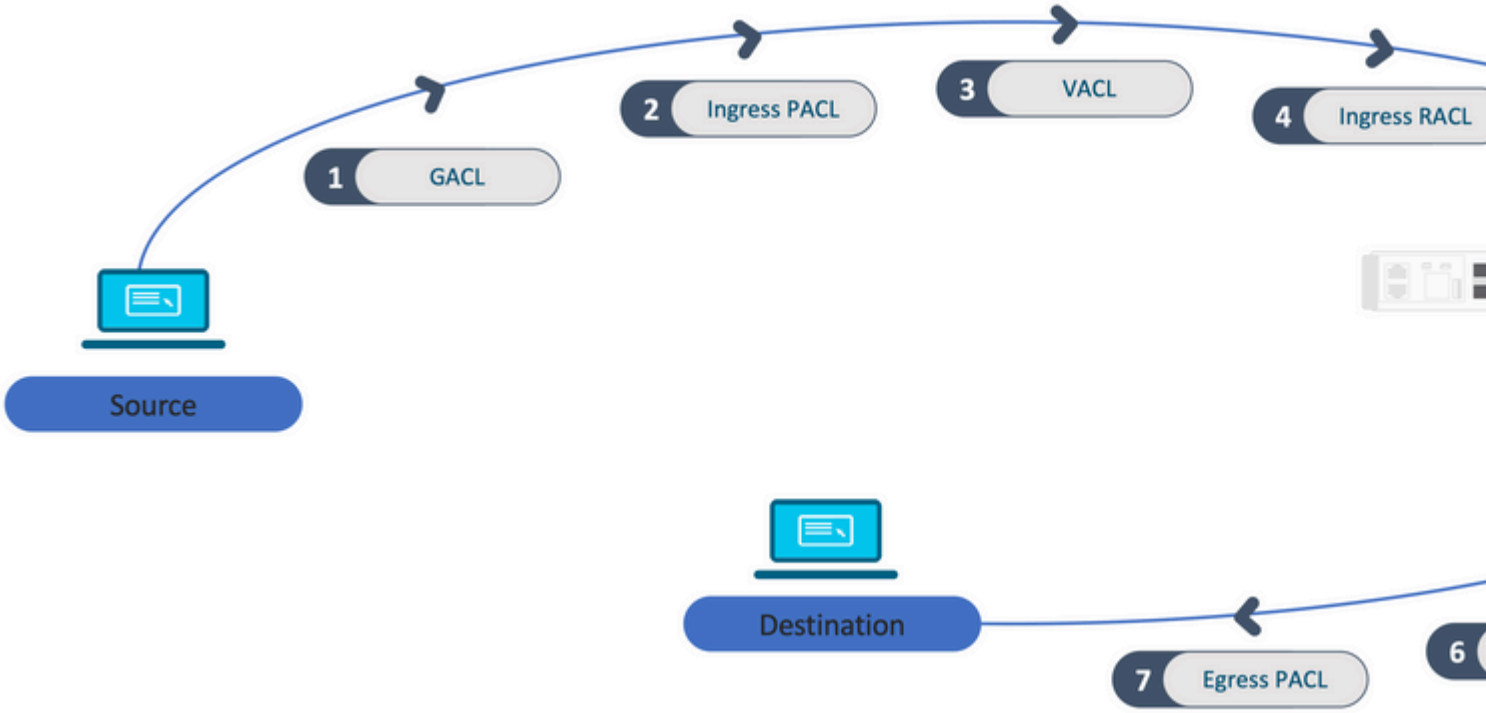
Entrées de contrôle d'accès de sécurité entrantes : **1 26*1024 <â€" Modifié par l'utilisateur en 26 x 1024 (26 Ko)**
Entrées de contrôle d'accès de sécurité en sortie : **2 20*1024 <â€" Modifié par l'entrée utilisateur en 20 x 1024 (20K)**

- Appliquer les modifications au profil SDM.
- 9500H(config)#**sdm prefer custom commit**
  Les modifications apportées aux préférences SDM en cours dâ€™exécution sont enregistrées et prennent effet lors du prochain rechargement. **< : une fois rechargée, la TCAM ACL est allouée à une valeur personnalisée.**

Lectures complémentaires :

Ordre de traitement ACL :

Les listes de contrôle dâ€™accès sont traitées dans cet ordre de la source à la destination.



ACL programmées dans une pile :

- Les listes de contrôle dâ€™accès qui ne sont pas basées sur les ports (par exemple, VACL, RACL) sont appliquées au trafic sur nâ€™importe quel commutateur et sont programmées sur tous les commutateurs de la pile.
- Les listes de contrôle dâ€™accès basées sur les ports sont appliquées uniquement au trafic sur un port et sont programmées uniquement sur le commutateur qui possède lâ€™interface.
- Les listes de contrôle dâ€™accès sont programmées par le commutateur actif et appliquées ensuite aux commutateurs membres.
- Les mêmes règles s'appliquent aux autres options de redondance, telles que ISSU/SVL.

Extension ACL :

- L'extension de la liste de contrôle d'accès se produit lorsque le périphérique manque de L4OP, de Lables ou de VCU. Le périphérique doit créer plusieurs ACE équivalents afin d'accomplir la même logique et d'épuiser rapidement la TCAM.
- **### Les L4OP sont à l'échelle et cette liste de contrôle d'accès est créée ##**
  9500H(config)#**ip access-list extended TEST**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any gt 150 <â€” correspond aux ports 151 et supérieurs**

  ### Ce champ doit être étendu à plusieurs ACE qui n'utilisent pas de L4OP ###
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 151**

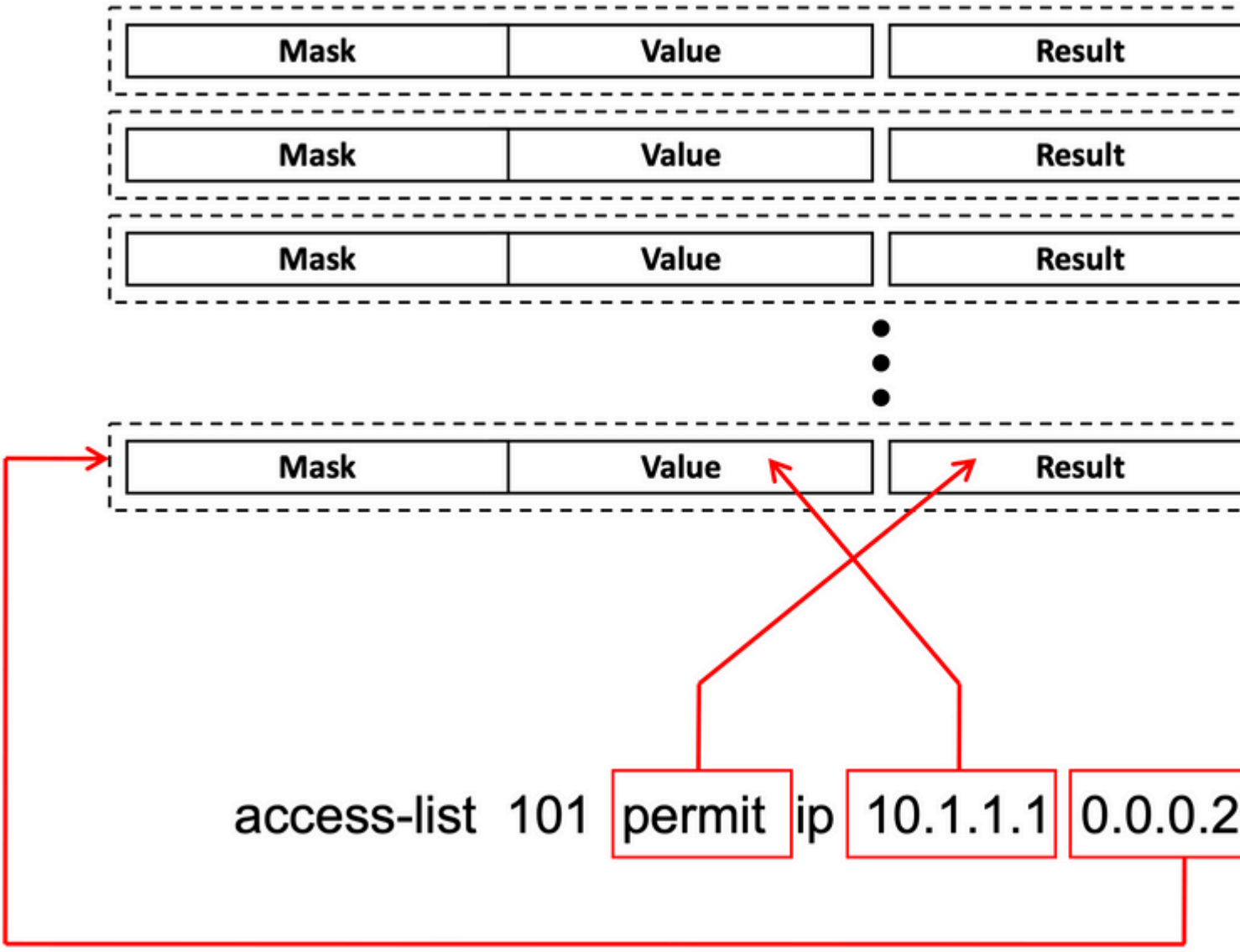
9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 152**
9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 153**
9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 154**
... et ainsi de suite ....

Consommation TCAM et partage d'étiquettes :

- Chaque stratégie ACL est référencée en interne par une étiquette.
- Lorsque la stratégie ACL (ACL de sécurité comme GACL, PACL, VACL, RACL) est appliquée à plusieurs interfaces ou VLAN, elle utilise la même étiquette.
- La liste de contrôle dâ€™accès entrante/sortante utilise différents espaces de libellé.
- Les listes de contrôle d'accès IPv4, IPv6 et MAC utilisent d'autres espaces d'étiquette.
- La même liste de contrôle dâ€™accès est appliquée à lâ€™entrée de lâ€™interface A et à la sortie de lâ€™interface A. Il y a deux instances de la liste de contrôle d'accès dans la TCAM, chacune avec une étiquette unique pour l'entrée et la sortie.
- Si la même PACL avec un L4OP est appliquée à plusieurs interfaces d'entrée qui existent sur chaque coeur, il y a deux instances de la même PACL programmées dans TCAM, une par coeur.

Description VMR :

Un ACE est programmé en interne dans TCAM en tant que « VMR », également connu sous le nom de Valeur, Masque, Résultat. Chaque entrée ACE peut consommer des VMR et des VCU.



Évolutivité ACL :

Les ressources ACL de sécurité sont dédiées aux ACL de sécurité. Elles ne sont pas partagées avec d'autres fonctionnalités.

Ressources ACL TCAM	**Cisco Catalyst 9600**	**Cisco Catalyst 9500**	**Cisco Catalyst 9400**	**Cisco Catalyst 9300**	**Cisco Catalyst 9200**				
Entrées IPv4	Entrée : 12000*	Sortie: 15000 *	C9500 : 18000*	C9500 hautes performances Entrée : 12000* Sortie : 15000*	18000 *	C9300: 5000	C9300B : 18000	C9300X:8000	1000

Entrées IPv6	La moitié des entrées IPv4	La moitié des entrées IPv4		La moitié des entrées IPv4	La moitié des entrées IPv4		La moit des entr IPv4
Un type d'entrées ACL IPv4 ne peut pas dépasser	12000	C9500 : 18000	C9500 hautes performances : 15000	18000	C9300: 5000	C9300B : 18000	C9300X : 8000	1000
Un type d'entrées ACL IPv6 ne peut pas dépasser	6000	C9500: 9000	C9500 hautes performances : 7500	9000	2500/9000/4000			500
L4OP/Étiquette	8	8		8	8			8
VCU en entrée	192	192		192	192			192
VCU de sortie	96	96		96	96			96

Informations connexes

- Guide de configuration de la sécurité, Cisco IOS XE Amsterdam 17.3.x (commutateurs Catalyst 9200)
- Guide de configuration de la sécurité, Cisco IOS XE Amsterdam 17.3.x (commutateurs Catalyst 9300)
- Guide de configuration de la sécurité, Cisco IOS XE Amsterdam 17.3.x (commutateurs Catalyst 9400)
- Guide de configuration de la sécurité, Cisco IOS XE Amsterdam 17.3.x (commutateurs Catalyst 9500)
- Guide de configuration de la sécurité, Cisco IOS XE Amsterdam 17.3.x (commutateurs Catalyst 9600)
- Guide de configuration de la gestion du système, Cisco IOS XE Bangalore 17.4.x (commutateurs Catalyst 9500)
- Assistance technique et téléchargements Cisco

Commandes Debug et Trace

Num	Commande	Faire Remarquer
1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	Videz les compteurs d'exception sur l'ASIC #N.
2	show platform software fed [switch] active acl	Cette commande imprime les informations relatives à toutes les

		listes de contrôle dâ€™accès configurées sur le boîtier, ainsi que les informations dâ€™interface et de stratégie.
3	show platform software fed [switch] active acl policy 18	Cette commande imprime uniquement les informations relatives à la stratégie 18. Vous pouvez obtenir cet ID de stratégie à partir de la commande 2.
4	show platform software fed [switch] active acl interface intftype pacl	Cette commande imprime les informations relatives à la liste de contrôle dâ€™accès en fonction du type dâ€™interface (pacl/vacl/racl/gacl/sgacl, etc.).
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Cette commande imprime les informations relatives à la liste de contrôle d'accès en fonction du type d'interface (pacl/vacl/racl/gacl/sgacl, etc.) et filtre également les protocoles (ipv4/ipv6/mac, etc.).
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Cette commande imprime les informations relatives aux interfaces.
7	show platform software fed [switch] active acl interface 0x9	Cette commande imprime les informations courtes de la liste de contrôle d'accès appliquée sur l'interface, en fonction de l'ID IF (commande de 6).
8	show platform software fed [switch] active acl definition	Cette commande imprime les informations relatives aux listes de contrôle dâ€™accès configurées sur le boîtier et dont la présence est dans le CGD.
9	show platform software fed [switch] active acl iifid 0x9	Cette commande imprime les informations détaillées de la liste de contrôle d'accès appliquée sur l'interface, en fonction de l'ID IF.
10	show platform software fed [switch] active acl usage	Cette commande imprime le nombre de VMR que chaque ACL utilise en fonction du type de fonctionnalité.
11	show platform software fed [switch] active acl policy intftype pacl vcu	Cette commande vous donne les informations de stratégie et également les informations VCU basées sur le type d'interface (pacl/vacl/racl/gacl/sgacl et ainsi de suite).
12	show platform software fed [switch] active acl policy intftype pacl cam	Cette commande vous donne les informations de politique et les détails sur les VMR dans le CAM, en fonction du type d'interface (pacl/valc/racl/gacl/sgacl et ainsi de suite).
13	show platform software interface [switch] [active] R0 brief	Cette commande vous donne des détails sur l'interface de la

		boîte.
14	show platform software fed [switch] active port if_id 9	Cette commande imprime les détails du port en fonction de l'ID IF.
15	show platform software fed [switch] active vlan 30	Cette commande imprime les détails du VLAN 30.
16	show platform software fed [switch] active acl cam asic 0	Cette commande imprime la came ACL complète sur l'ASIC 0 en cours d'utilisation.
17	show platform software fed [switch] active acl counters hardware	Cette commande imprime tous les compteurs ACL du matériel.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	En imprimant les entrées de la section PBR, vous pouvez donner différentes sections comme ACL et CPP au lieu de PBR.
19	show platform software fed [switch] active punt cpuq [1|2|3 â€¦]	Afin de vérifier l'activité sur l'une des files d'attente de CPU, vous avez également des options pour effacer les statistiques de file d'attente pour le débogage.
20	show platform software fed [switch] active ifm mappings gpn	Imprimez le mappage d'interface avec l'ID IF et les GPN
21	show platform software fed [switch active ifm if-id	Imprimez les informations sur la configuration de l'interface et l'affinité avec l'ASIC. Cette commande est utile afin de vérifier sur quelle interface l'ASIC et le CORE sont.
22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error â€¦]	Définition du suivi d'une fonction spécifique dans FED.
23	request platform software trace rotate all	Effacement de la mémoire tampon de suivi.
24	show platform software trace message fed [switch] active	Impression du tampon de suivi pour FED.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error â€¦]	Activation des traces pour FMAN.
26	show platform software trace message	Impression du tampon de suivi pour FMAN.

	forwarding-manager [switch] [active] f0	
27	debug platform software infrastructure punt detail	Définissez le débogage sur le PUNT.
28	debug ip cef packet all input rate 100	Le débogage des paquets CEF est activé.

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.