Valideren van security ACLâ€™s op Catalyst 9000 Switches

Inhoud

Inleiding

Dit document beschrijft hoe u ACLâ€™s (toegangscontrolelijsten) op Catalyst 9000 Series switches kunt verifiëren en problemen kunt oplossen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware-versies:

- C9200
- C9300
- C9400
- C9500
- C9600

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

> **Opmerking**: raadpleeg de juiste configuratiehandleiding voor de opdrachten die worden gebruikt om deze functies op andere Cisco-platforms in te schakelen.

Achtergrondinformatie

ACLâ€™s-filterverkeer als het door een router of switch gaat en pakketten die bepaalde interfaces doorkruisen, toestaat of ontkent. Een ACL is een opeenvolgend verzamelen van vergunningen en ontkent voorwaarden die op pakketten van toepassing zijn. Wanneer een pakket op een interface wordt ontvangen, vergelijkt de switch de velden in het pakket met alle toegepaste ACLâ€™s om te verifiëren dat het pakket de vereiste rechten heeft om doorgestuurd te worden, gebaseerd op de criteria die in de toegangslijsten zijn gespecificeerd. Eén voor één test het pakketten tegen de voorwaarden in een toegangslijst. De eerste wedstrijd bepaalt of de switch de pakketten accepteert of verwerpt. Omdat de switch na de eerste match stopt met testen, is de volgorde van de condities in de lijst kritiek. Als er geen overeenkomende voorwaarden zijn, wijst de switch het pakket af. Als er geen beperkingen zijn, stuurt de switch het pakket door; anders laat de switch het pakket vallen. De switch kan ACLâ€™s gebruiken op alle pakketten die hij doorstuurt.

U kunt toegangslijsten configureren om basisbeveiliging voor uw netwerk te bieden. Als u geen ACLâ€™s configureert, kunnen alle pakketten die door de switch gaan, worden toegestaan op alle netwerkonderdelen. U kunt ACLâ€™s gebruiken om te bepalen welke hosts toegang kunnen krijgen tot verschillende delen van een netwerk of om te beslissen welke soorten verkeer worden doorgestuurd of geblokkeerd bij routerinterfaces. U kunt bijvoorbeeld e-mailverkeer doorsturen zonder Telnet-verkeer.

Terminologie

ACE	Access Control Entry (ACE) - één regel/lijn binnen een ACL
ACL	Toegangscontrolelijst (ACL) - Een groep ACEâ€™s die op een poort zijn toegepast

DACL	Downloadbare ACL (DACL) - Een ACL die dynamisch wordt gedrukt via het ISE-beveiligingsbeleid
PACL	PoortACL (PAL) - Een ACL toegepast op een Layer 2-interface
RACL	Routed ACL (RACL) - een ACL toegepast op een Layer 3-interface
VACL	VLAN ACL (VACL) - Een ACL toegepast op een VLAN
GACL	Group ACL (GACL) - een ACL die dynamisch wordt toegewezen aan een gebruikersgroep of client op basis van hun identiteit
IP-ACL	Wordt gebruikt voor de classificatie van IPv4/IPv6-pakketten. Deze regels bevatten verschillende Layer-3 en Layer-4 pakketvelden en kenmerken, waaronder, maar niet beperkt tot IPv4-adressen van bron en bestemming, TCP/UDP-bron- en doelpoorten, TCP-vlaggen en DSCP, enzovoort.
MACL	Mac Address ACL (MACL) - Gebruikt om niet-IP pakketten te classificeren. Regels bevatten diverse Layer-2-velden en -kenmerken, waaronder het MAC-adres van de bron/de dest, ether-type, enzovoort.
L4OP	Layer 4 Operator Port (L4OP) - komt overeen met andere logica dan EQ (gelijk aan). GT (groter dan), LT (minder dan), NE (niet gelijk aan) en BEREIK (van-tot)
VCU	Waardevergelijkingseenheid (VCU) - L4OP's worden vertaald in VCU om classificatie op Layer 4-headers uit te voeren
VMR	Value Mask Resultaat (VMR) - Een ACE-vermelding is intern geprogrammeerd in TCAM als een VMR.
CGD	Class Group Database (CGD) - waar FMAN-FP ACL-inhoud opslaat
Klassen	Hoe ACEâ€™s worden geïdentificeerd in CGD
zwaartepunt	Class Group (CG) - Een groep klassen over hoe ACLâ€™s in CGD worden geïdentificeerd
CGE	Class Group Entry (CGE) - Een ACE-vermelding die binnen een Class Group is opgeslagen
FMAN	Forwarding Manager (FMAN) - de programmeerlaag tussen Cisco IOS® XE en hardware

FED	Forwarding Engine Driver (FED) - Het onderdeel dat de hardware van het apparaat programmeert

Voorbeelden van ACL-resourcegebruik

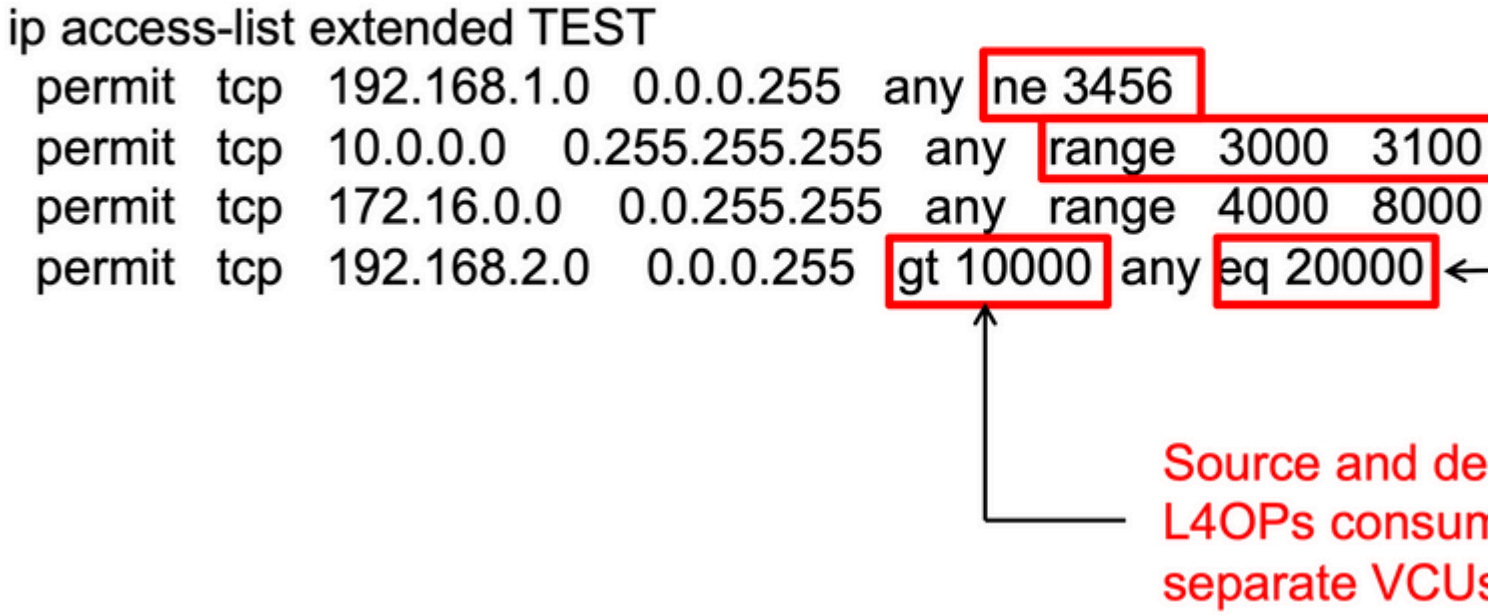
Hier worden drie voorbeelden gegeven om aan te tonen hoe ACLâ€™s TCAM, L4OPâ€™s en VCUâ€™s gebruiken.

Voorbeeld 1. IPv4-TCAM

```
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
```

	TCAM-vermeldingen	**L4OPâ€™s**	**VCUâ€™s**
Verbruik	5	0	0

Voorbeeld 2. IPv4-TCAM/L4OP/VCU



```
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

	TCAM-vermeldingen	**L4OPâ€™s**	**VCUâ€™s**
Verbruik	4	5	7

Voorbeeld 3. IPv6-TCAM/L4OP/VCU

IPv6-ACEâ€™s maken gebruik van twee TCAM-ingangen in vergelijking met één voor IPv4. In dit voorbeeld verbruiken vier ACE's acht TCAM in plaats van vier.

<#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
```

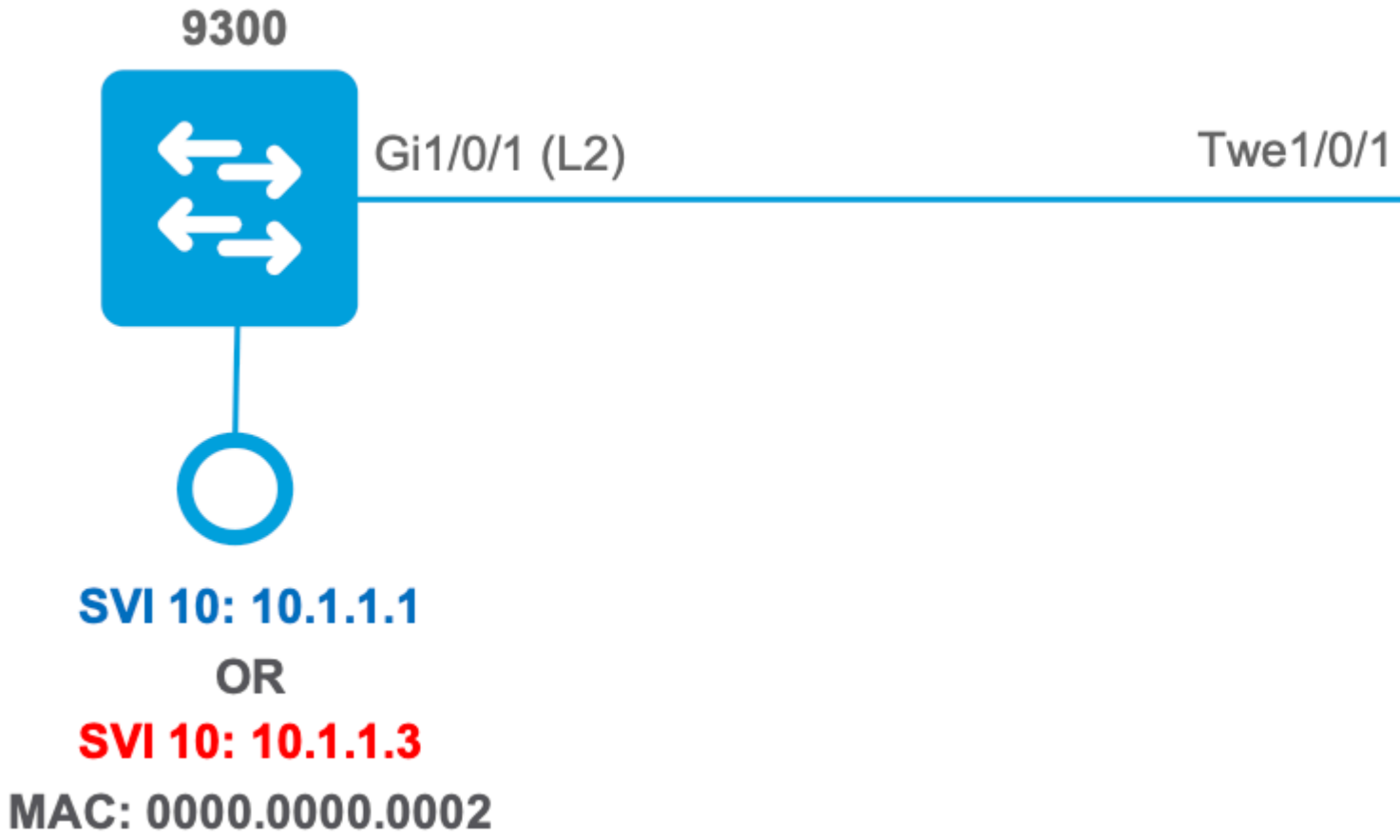
<-- One L4OP & VCU

	TCAM-vermeldingen	**L4OPâ€™s**	**VCUâ€™s**

Verbruik	8	2	2

Topologie

De 9300 VLAN 10 SVI maakt gebruik van een van de twee IP-adressen die in dit beeld worden weergegeven, afhankelijk van de vraag of in de voorbeelden een resultaat voor- of achteruit wordt weergegeven.



Configureren en controleren

Deze sectie behandelt hoe te om ACL programmering in software en hardware te verifiëren en problemen op te lossen.

Scenario 1. PAL (IP-ACL)

PACL's worden toegewezen aan een Layer 2-interface.

- Beveiligingsgrens: poorten of VLANâ€™s
- Bijlage: Layer 2-interface
- Richting: Ingress of Uitgang (een voor een)
- Ondersteunde ACL-typen: MAC ACL en IP ACLâ€™s (standaard of uitgebreid)

PACL met IP ACL configureren

<#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
```

Verifieer PAL

Win de IF_ID terug die aan de interface is gekoppeld.

<#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
```

Controleer de Class group ID (CG ID) die aan de IF_ID is gekoppeld.

```
<#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

ACL-informatie gekoppeld aan de CG-id

<#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)

Beleidsinformatie over de CG ID, evenals welke interfaces de CG ID gebruiken.

<#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------------
```

Bevestig dat PACL werkt.

> **Opmerking:** Wanneer u de show ip access-lists privileged EXEC Met de opdracht wordt het aantal overeenkomsten weergegeven zonder rekening te houden met pakketten die toegangscontrole in hardware zijn. Gebruik de switch van de de showplatform software gevoederde {*switch_num*|active|standby}acl tellers hardware bevoorrecht EXEC bevel om sommige basis hardware ACL statistieken voor geschakelde en gerouteerde pakketten te verkrijgen.

<#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...>
```

Scenario 2. PAL (MAC ACL)

PACL's worden toegewezen aan een Layer 2-interface.

- Beveiligingsgrens: poorten of VLANâ€™s
- Bijlage: Layer 2-interface
- Richting: Ingress of Uitgang (een voor een)
- Ondersteunde ACL-typen: MAC ACL en IP ACLâ€™s (standaard of uitgebreid)

PACL met MAC ACL configureren

<#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

Verifieer PAL

Win de IF_ID terug die aan de interface is gekoppeld.

<#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

Controleer de Class group ID (CG ID) die aan de IF_ID is gekoppeld.

<#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

ACL-informatie gekoppeld aan de CG-id

<#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
```

Beleidsinformatie over de CG ID, evenals welke interfaces de CG ID gebruiken.

<#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------------
```

Bevestig dat PACL werkt:

- De MACL staat alleen bronadres 0001.aaaa.aaaa toe.
- Aangezien dit een MAC ACL is, wordt een ARP-pakket dat geen IP is, verwijderd, waardoor de ping mislukt.

<#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...>
```

Scenario 3. RACL

RACL wordt toegewezen aan een Layer 3-interface zoals een SVI- of Routed-interface.

- Beveiligingsgrens: verschillende subnetten
- Bijlage: Layer 3-interface
- Richting: Ingress of Uitgang
- Ondersteunde ACL-typen: IP-ACLâ€™s (standaard of uitgebreid)

RACL configureren

<#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
```

Controleer RACL

Win de IF_ID terug die aan de interface is gekoppeld.

```
<#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
```

Controleer de Class group ID (CG ID) die aan de IF_ID is gekoppeld.

```
<#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
```

ACL-informatie gekoppeld aan de CG-id

```
<#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)
```

Beleidsinformatie over de CG ID, evenals welke interfaces de CG ID gebruiken.

<#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------------
```

Bevestig dat RACL werkt.

> **Opmerking:** Wanneer u de show ip access-lists privileged EXEC Met de opdracht wordt het aantal overeenkomsten weergegeven zonder rekening te houden met pakketten die toegangscontrole in hardware zijn. Gebruik de show platform software gevoed switch {*switch_num*|active|standby}acl tellerhardwaregeprivilegieerde EXEC-opdracht om bepaalde basishardware-ACL-statistieken te verkrijgen voor switched en routed-pakketten.

<#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...>
```

Scenario 4. VACL

VACLâ€™s worden toegewezen aan een Layer 2 VLAN.

- Beveiligingsgrens: binnen of via een VLAN
- Bijlage: VLAN/VLAN-kaart
- Richting: Zowel ingres als uitgang tegelijk
- Ondersteunde ACL-typen: MAC ACL en IP ACLâ€™s (standaard of uitgebreid)

VACL configureren

```
<#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
```

Controleer VACL

Win de IF_ID terug die aan de interface is gekoppeld.

```
<#root>

9500H#

show platform software fed active ifm interfaces vlan

Interface

IF_ID

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

Vlan10                           0x00420010

        READY
```

Controleer de Class group ID (CG ID) die aan de IF_ID is gekoppeld.

```
<#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
```

ACL-informatie gekoppeld aan de CG-groep-ID.

Er zijn twee ACLâ€™s die in hetzelfde VACL-beleid worden gebruikt, gegroepeerd in deze groep

<#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
```

Beleidsinformatie over de CG ID, evenals welke interfaces de CG ID gebruiken.

```
<#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------------
```

Bevestig dat VACL werkt.

- Probleemoplossing is hetzelfde scenario als PACL en RACl. Verwijs naar deze secties voor details op de ping test.
- Ping van 10.1.1.3 tot 10.1.1.2 ontkend door het toegepaste ACL-beleid.

- Controleer de platformdrop-opdracht.

```
<#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...>
```

Scenario 5. Groep/client-ACL (DACL)

Groep/client-ACLâ€™s worden dynamisch toegepast op een gebruikersgroep of client op basis van hun identiteit. Deze worden ook wel DACL genoemd.

- Beveiligingsgrens: client (clientinterfaceniveau)
- Bijlage: per client-interface
- Richting: alleen ingress
- Ondersteunde ACL-typen: MAC ACL en IP ACLâ€™s (standaard of uitgebreid)

GACL configureren

```
<#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 ar
```

Controleer GACL

Groep CG ID gebonden aan de if-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
```

ACL-informatie gekoppeld aan de groep GC-id

```
<#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
```

Scenario 6. ACL-vastlegging

De apparaatsoftware kan syslogberichten over pakketten verstrekken die door een standaard IP toegangslijst worden toegelaten of worden ontkend. Om het even welk pakket dat ACL aanpast veroorzaakt een informatief logboekbericht over het pakket dat naar de console wordt verzonden. Het niveau van de aan de console geregistreerde berichten wordt bepaald door delogboekconsoleopdrachten die de Syslog-berichten besturen.

- ACL-logberichten worden niet ondersteund voor ACLâ€™s die worden gebruikt met Unicast Reverse Path Forwarding (uRPF). Het wordt alleen ondersteund voor RACL.
- ACL-aanmelding in de uitgangsrichting wordt niet ondersteund voor pakketten die worden gegenereerd vanaf het besturingsplane van het apparaat.
- Routing wordt gedaan in hardware en het inloggen software, zodat als een groot aantal pakketten overeenkomen met een vergunning of ontkennen ACE die een logkeyword bevat, de software niet kan overeenkomen met de hardware verwerkingssnelheid, en niet alle pakketten kunnen worden geregistreerd.
- Het eerste pakket dat de ACL activeert, veroorzaakt meteen een logbericht, en de volgende pakketten

worden verzameld over intervallen van 5 minuten voordat ze verschijnen of worden vastgelegd. Het logbericht bevat het nummer van de toegangslijst, of het pakket is toegestaan of geweigerd, het IP-bronadres van het pakket en het aantal pakketten uit die bron dat in het vorige 5-minuten interval is toegestaan of geweigerd.

- Zie de juiste Security Configuration Guide, Cisco IOS XE zoals aangegeven in het gedeelte Verwante informatie voor volledige informatie over het gedrag en de beperkingen van ACL-logbestanden.

Voorbeeld van een logboek:

Dit voorbeeld toont een negatieve case, waarbij het ACL-type en het logwoord niet samenwerken.

```
<#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
```

Log Voorbeeld van 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
```

Voorbeeld van een RACL (Permit):
Wanneer een logverklaring voor een vergunningsverklaring wordt gebruikt, tonen de softwaretellerhits dubbel het aantal verzonden pakketten.

<#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)
```

Problemen oplossen

ACL-statistieken

Wanneer u een probleem met ACL oplost, is het essentieel om te begrijpen hoe en waar ACL-statistieken door het apparaat worden gemeten.

- ACL-statistieken worden verzameld op een geaggregeerd niveau en niet per ACE-niveau.
- Hardware heeft niet de mogelijkheid om per ACE of per ACL stats toe te staan.
- Statistieken zoals doorgestuurde pakketten van Deny, Log en CPU worden verzameld.
- Statistieken voor MAC-, IPv4- en IPv6-pakketten worden afzonderlijk verzameld.
- show platform software fed switch active acl counters hardware kan worden gebruikt om samengestelde statistieken weer te geven.

ACL-statistieken wissen

Wanneer het oplossen van problemen een ACL kwestie, kan het nuttig zijn om de diverse ACL tellers te ontruimen om verse basislijntellingen te krijgen.

- Met deze opdrachten kunt u de software en hardware ACL-tellerstatistieken wissen.
- Wanneer u problemen met ACL-overeenkomsten/treffers oplost, wordt aanbevolen de relevante ACL te wissen van basislijnovereenkomsten die recent of relevant zijn.

<#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)
```

Wat gebeurt er wanneer ACL TCAM is uitgeput?

- ACLâ€™s worden altijd toegepast in hardware-TCAM. Als TCAM al wordt gebruikt door eerder geconfigureerde ACLâ€™s, krijgen de nieuwe ACLâ€™s niet de vereiste ACL-bronnen die nodig zijn om te programmeren.

- Als een ACL wordt toegevoegd nadat TCAM is uitgeput, worden alle pakketten gelaten vallen voor de interface het in bijlage is.

- De handeling van het houden van ACL in software wordt genoemd **het Onladen**.
- Wanneer er bronnen beschikbaar komen, probeert de switch automatisch de ACLâ€™s in de hardware te programmeren. Als dit lukt, worden de ACLâ€™s naar de hardware gedrukt en beginnen de pakketten vooruit te gaan.
- De actie van het programmeren van een software-held ACL in TCAM wordt **herladen** genoemd.

- PACL, VACL, RACL en GACL kunnen onafhankelijk van elkaar worden gelost/opnieuw geladen.

ACL-TCAM-uitputting

- De interface waarop de nieuw toegevoegde ACL wordt toegepast, begint pakketten te laten vallen totdat hardwareresources beschikbaar zijn.
- GACL-clients worden in de staat van de VN-autorisatie geplaatst.

VCU-uitputting

- Eenmaal boven de L4OPs limiet of uit VCU's, voert de software ACL-uitbreiding uit en creëert nieuwe ACE-vermeldingen om gelijkwaardige actie uit te voeren zonder VCU's te gebruiken.
- Zodra dit gebeurt kan TCAM uitgeput raken van deze toegevoegde items.

Fouten in ACL-synchronisatie

Als een bepaalde beveiligingsACL-bron is uitgeput, worden SYSLOG-berichten gegenereerd door het systeem (interface, VLAN, label enzovoort, waarden kunnen verschillen).

ACL-logbericht	Definitie	Terugvorderingsactie
%ACL_ERRMSG-4-UNLOLOAD: Switch 1 gevoed: ingangssignaal <ACL> op interface <interface> is niet geprogrammeerd in hardware en het verkeer wordt verbroken.	ACL wordt leeggemaakt (in software)	Onderzoek de TCAM-schaal. Als voorbij schaal, herontwerp ACLs.
%ACL_ERRMSG-6-VERWIJDERD: 1 fed: de ongeladen configuratie voor Invoer <ACL> op interface <interface> is verwijderd voor label <label>Basic<number>.	De onbelaste ACL-configuratie wordt uit de interface	ACL is al verwijderd, geen actie om te ondernemen

	verwijderd	
%ACL_ERRMSG-6-RELOLOAD: 1 gevoed: ingangssignaal <ACL> op interface <interface> is nu geladen in de hardware voor label <label> op basis van <nummer>.	ACL is nu geïnstalleerd in hardware	Het probleem met ACL is nu opgelost in hardware, geen actie om te nemen
%ACL_ERRMSG-3-ERROR: 1 ingevoerd: <ACL> IP ACL <NAME>-configuratie is niet toegepast op <interface> bij bind order <number>.	Andere soorten ACL-fouten (zoals dot1x ACL-installatiefout)	Bevestig dat de ACL-configuratie wordt ondersteund en dat TCAM niet buiten de schaal valt
%ACL_ERRMSG-6-GACL_INFO: Switch 1 R0/0: ingevoerd: vastlegging wordt niet ondersteund voor GACL.	GACL heeft een logoptie geconfigureerd	GACL ondersteunt geen logbestanden. Verwijder logverklaringen uit GACL.
%ACL_ERRMSG-6-PACL_INFO: Switch 1 R0/0: fed: vastlegging wordt niet ondersteund voor PACL.	PACL heeft een logoptie geconfigureerd	PACL ondersteunt geen logbestanden. Verwijder logverklaringen van PACL.
%ACL_ERRMSG-3-ERROR: Switch 1 R0/0: fed: Invoer IPv4 Groep ACL impliciet_deny:<name>: configuratie is niet toegepast op client MAC 0000.000.0000.	(dot1x) ACL is niet van toepassing op de doelpoort	Bevestig dat de ACL-configuratie wordt ondersteund en dat TCAM niet buiten de schaal valt

Scenario's en herstelacties buiten het resourcesysteem

Scenario 1. ACL-binding	Terugvorderingsactie
• ACL wordt gemaakt en toegepast op een interface of VLAN. • Bind mislukt vanwege 'out of resource' omstandigheden, zoals TCAM-uitputting. • Geen ACE's binnen ACL kunnen in TCAM worden geprogrammeerd. ACL blijft in **LEEGGEMAAKTE** toestand. • In de staat **UNLOLOAD** daalt al het verkeer (inclusief controlepakketten) op de interface totdat de kwestie is opgelost.	Herontwerp ACL om het gebruik van TCAM te verminderen.
Scenario 2. ACL-bewerking	**Terugvorderingsactie**
• Er wordt een ACL gemaakt en toegepast op een interface en er worden meer ACE-vermeldingen	Herontwerp ACL om het gebruik van TCAM te verminderen.

aan deze ACL toegevoegd terwijl deze op de interface(s) worden toegepast. • Als TCAM geen bronnen heeft, mislukt de bewerking. • Geen ACE's binnen ACL kunnen in TCAM worden geprogrammeerd. ACL blijft in **LEGE** toestand. • In de **UNLOLOAD-**staat valt al het verkeer (inclusief controlepakketten) op de interface tot de kwestie is opgelost. • De bestaande ACL-vermeldingen mislukken ook in de **LEEGGEMAAKTE** staat tot deze is hersteld.	
Scenario 3. ACL-opnieuw binden	**Terugvorderingsactie**
• ACL Re-bind is de actie van het toevoegen van een ACL aan een interface, dan het toevoegen van een andere ACL aan dezelfde interface zonder de eerste ACL los te maken. • Eerste ACL wordt gemaakt en met succes als bijlage toegevoegd. • Er wordt een grotere ACL met een andere naam en hetzelfde protocol (IPv4/IPv6) gemaakt en als bijlage aan dezelfde interface toegevoegd. • Het apparaat maakt met succes de eerste ACL los en probeert de nieuwe ACL aan deze interface toe te voegen. • Als TCAM niet over resources beschikt, wordt de handeling opnieuw binden mislukt. • Geen ACE's binnen ACL kunnen in TCAM worden geprogrammeerd. ACL blijft in **LEEGGEMAAKTE** toestand. • In de staat **UNLOLOAD** daalt al het verkeer (inclusief controlepakketten) op de interface totdat de kwestie is opgelost.	Herontwerp ACL om het gebruik van TCAM te verminderen.
Scenario 4. Lege (leeg) ACL binden	**Terugvorderingsactie**
• Een ACL die geen ACE-vermeldingen heeft, wordt gemaakt en aan een interface gekoppeld. • Het systeem maakt deze ACL intern met een vergunning "om het even welk ACE", en maakt het aan de interface in hardware (al verkeer wordt toegelaten in deze staat) vast. • De ingangen van ACE worden dan toegevoegd aan ACL met de zelfde naam of het aantal. Het systeem programmeert TCAM zoals elke ACE wordt toegevoegd. • Als TCAM onvoldoende middelen heeft om	Herontwerp ACL om het gebruik van TCAM te verminderen.

ACE-vermeldingen toe te voegen, wordt ACL naar de **LEEGGEMAAKTE** staat verplaatst. • In de staat **UNLOLOAD** daalt al het verkeer (inclusief controlepakketten) op de interface totdat de kwestie is opgelost. • De bestaande ACL-vermeldingen mislukken ook in de **LEEGGEMAAKTE** staat tot deze is hersteld.	

Controleer ACL-schaal

In deze sectie worden opdrachten behandeld om de ACL-schaal en het TCAM-gebruik te bepalen.

Samenvatting van FMAN-toegangslijst:

Identificeer geconfigureerd ACLâ€™s en totaal aantal ACE-cellen per 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

ACL-gebruik:

<#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 cor

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

TCAM-gebruik (17.x):

TCAM gebruikscommando heeft significante verschillen tussen 16.x en 17.x treinen.

```
<#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)
```

TCAM-gebruik (16.x):

TCAM gebruikscommando heeft significante verschillen tussen 16.x en 17.x treinen.

```
<#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...>
```

Aangepaste SDM-sjabloon (TCAM-hertoewijzing)

Cisco IOS XE Bengaluru 17.4.1 gebruiken u kunt een aangepaste SDM-sjabloon voor ACL-functies configureren met de sdm prefer custom acluit.

Gegevens over het configureren en verifiëren van deze functie worden besproken in de configuratiehandleiding voor systeembeheer, Cisco IOS XE Bengaluru 17.4.x (Catalyst 9500 Switches).

In deze sectie worden enige basisconfiguratie en -verificatie vermeld.

Controleer de huidige SDM-sjabloon:

<#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
```

Wijzig de huidige SDM-sjabloon:

- 9500H (configuratie)#**sdm prefereert aangepaste acl**
  9500H (configuratie-sdm-acl)#**acl-ingress 26 prioriteit 1 <â€" pas nieuwe 26K waarde toe. (prioriteit besproken in de configuratiehandleiding)**
  9500H (configuratie-sdm-acl)#**acl-egress 20-prioriteit 2**
  9500H (configuratie-sdm-acl)#**uitgang**
  Gebruik show sdm prefer custom om de voorgestelde waarden en sdm prefer custom commit om 'bekijk de wijzigingen' toe te passen via deze CLI.
- Controleer de wijzigingen in het SDM-profiel.
- Nexus 9500H#**sdm tonen liever aangepast**

SDM-sjablooninformatie weergeven:

Dit is de aangepaste sjabloon met zijn details.
Ingress Security Access Control Entries*: **12288 (huidig) - 26624 (voorgesteld) <â€” Huidig en voorgesteld gebruik (26K voorgesteld)**
Uitgaande security toegangscontrolelijsten*: **15360 (huidig) - 20480 (voorgesteld)**

Nexus 9500H#**SDM weergeven Aangepaste invoer van gebruiker verkiezen**

GEBRUIKERSINVOER VAN ACL-FUNCTIE
Invoerwaarden gebruiker
==========

PRIORITEIT FUNCTIENAAM **SCHAAL**

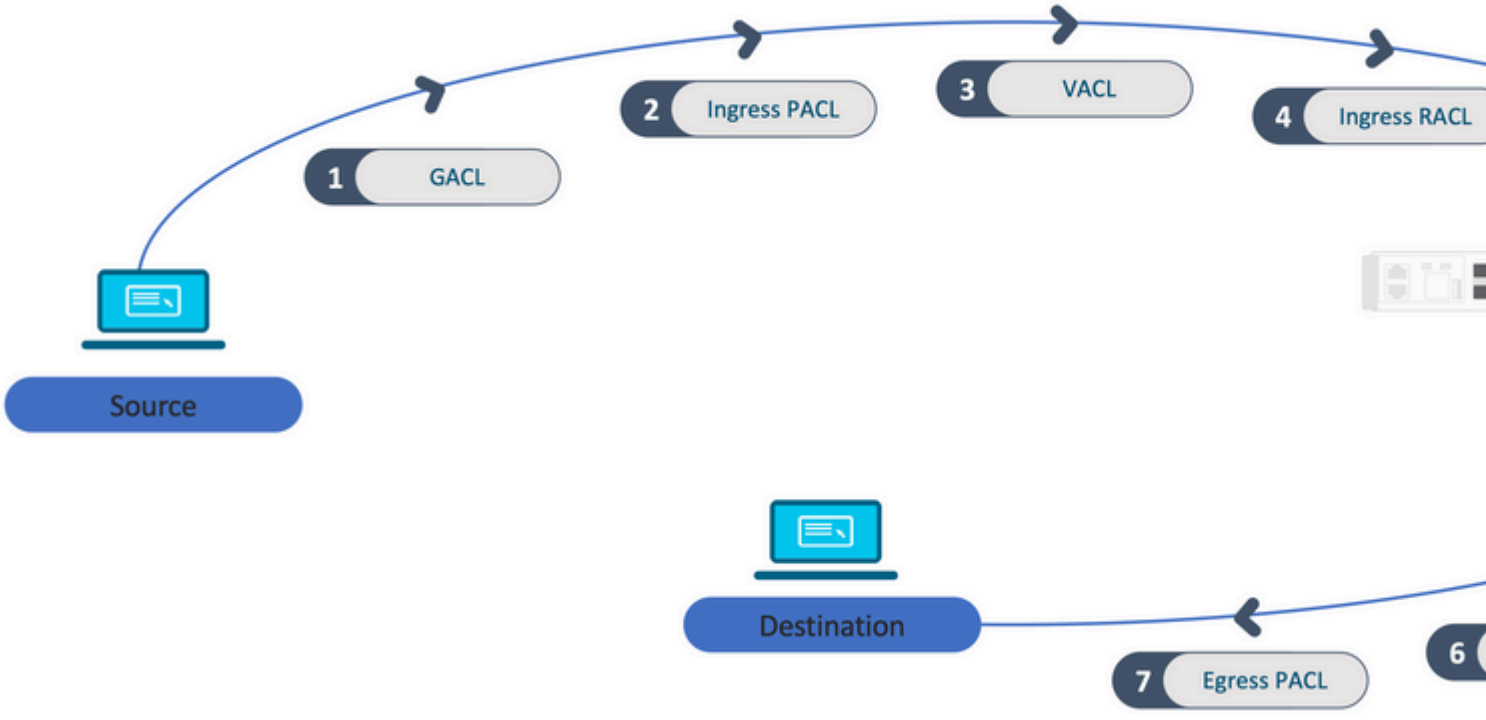
Ingress Security-toegangscontrolelijsten: **1 26*1024 <â€” Gewijzigd door gebruikersinvoer tot 26 x 1024 (26K)**
Vermeldingen voor toegangscontrole voor uitgaande beveiliging: **2 20*1024 <â€” Gewijzigd door gebruikersinvoer tot 20 x 1024 (20K)**

- Wijzigingen toepassen op het SDM-profiel.
- 9500H (configuratie)#**sdm prefereert custom commit**
  Veranderingen in de lopende SDM-voorkeuren worden opgeslagen en worden van kracht bij het volgende opnieuw laden. **<â€” Na herladen wordt ACL-TCAM toegewezen aan aangepaste waarde.**

Lees ook:

ACL-verwerkingsvolgorde:

ACLâ€™s worden in deze volgorde verwerkt van Bron naar Bestemming.



ACLâ€™s die in een stack zijn geprogrammeerd:

- ACLâ€™s die niet op poorten zijn gebaseerd (bijvoorbeeld VACL, RACL) worden op elk verkeer op elke switch toegepast en zijn geprogrammeerd op alle switches in de stack.
- Op poorten gebaseerde ACLâ€™s worden alleen toegepast op het verkeer op een poort en zijn alleen geprogrammeerd op de switch die eigenaar is van de interface.
- ACLâ€™s worden geprogrammeerd door de actieve switch en vervolgens toegepast op de switches van de leden.
- Dezelfde regels gelden voor andere redundantieopties, zoals ISSU/SVL.

ACL-uitbreiding:

- ACL-uitbreiding gebeurt wanneer het apparaat geen L4OPâ€™s, tabellen of VCUâ€™s meer heeft. Het apparaat moet meerdere equivalente ACE's creëren om dezelfde logica te bereiken en om TCAM snel uit te putten.
- **### L4OPs zijn bij schaal en dit ACL wordt gemaakt ##**
  9500H (configuratie)#**ip toegangslijst - uitgebreide TEST**
  9500H (config-ext-nacl)#**vergunning tcp 10.0.0.0 0.255.255.255 elke GT 150 <â€” komt overeen met poorten 151 en hoger**

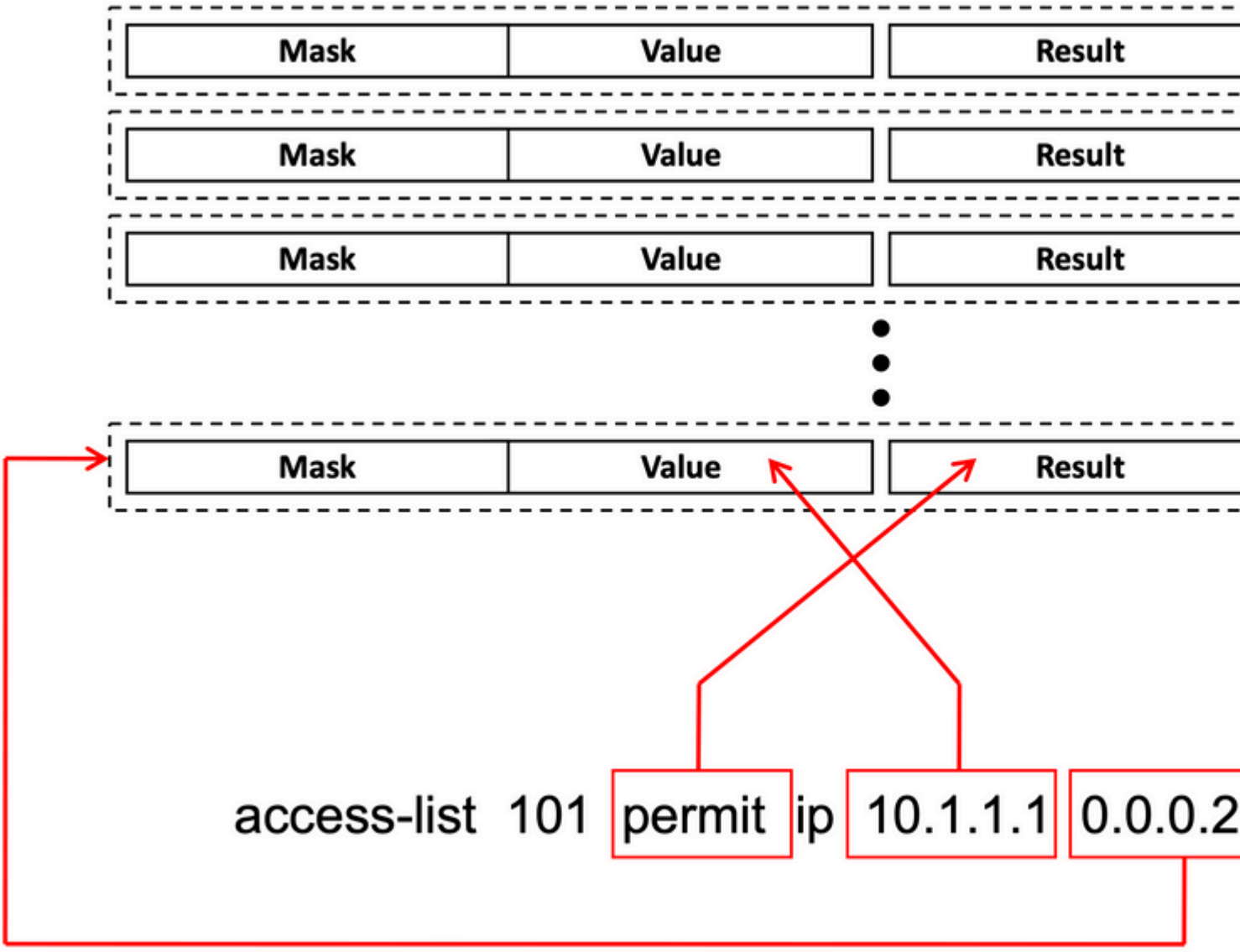
  ### Dit moet worden uitgebreid tot meerdere ACEâ€™s die geen L4OP ### gebruiken
  9500H (config-ext-nacl)#**license-tcp 10.0.0.0 0.255.255.255 elke eq 151**
  9500H (config-ext-nacl)#**license-tcp 10.0.0 0.255.255.255 elke eq 152**
  9500H (config-ext-nacl)#**license-tcp 10.0.0 0.255.255.255 elke eq 153**
  9500H (config-ext-nacl)#**license-tcp 10.0.0.0 0.255.255.255 elke eq 154**
  ... en zo verder ....

TCAM-verbruik en labeldeling:

- Elk ACL-beleid wordt intern door een label van verwijzingen voorzien.
- Wanneer het ACL-beleid (Security ACL zoals GACL, PACL, VACL, RACL) wordt toegepast op meerdere interfaces of VLAN, gebruikt het hetzelfde label.
- Ingress/uitgaande ACL gebruikt verschillende labelruimtes.
- IPv4, IPv6 en MAC ACL gebruiken andere labelruimtes.
- Dezelfde PAL wordt toegepast op de toegang van interface-A en de uitgang van interface-A. Er zijn twee exemplaren van de PACL in de TCAM, elk met een uniek label voor Ingress en Egress.
- Als dezelfde PACL met een L4OP wordt toegepast op meerdere ingangsinterfaces die op elke kern bestaan, zijn er twee instanties van dezelfde PACL geprogrammeerd in TCAM, één per elke kern.

Beschrijving van de VMR:

Een ACE is intern geprogrammeerd in TCAM als een 'VMR' - ook bekend als Value, Mask, Result. Elke ACE-ingang kan VMR's consumeren en VCU's consumeren.



ACL-schaalbaarheid:

Beveiligings-ACL-bronnen zijn gewijd aan security ACLâ€™s. Ze worden niet gedeeld met andere functies.

ACL-TCAM-bronnen	Cisco Catalyst 9600 switch	Cisco Catalyst 9500 switch	Cisco Catalyst 9400 switch	Cisco Catalyst 9300 switch	Cisco Catalyst 9200 switch			
IPv4-vermeldingen	Ingress: 12000*	Uitgang: 15000*	C950: 18000*	C9500 hoogwaardige software Ingress: 12000* Uitgang: 15000*	18000*	C9300: 5000	C9300B 18000	C9300X:8

IPv6-vermeldingen	De helft van de IPv4-vermeldingen	De helft van de IPv4-vermeldingen		De helft van de IPv4-vermeldingen	De helft van de IPv4-vermeldingen		
Eén type IPv4 ACL-vermeldingen kan niet meer bedragen dan	12000	C9500: 18000	C9500 hoogwaardige producten: 15000	18000	C9300: 5000	C9300B: 18000	C9300X: 8000
Eén type IPv6 ACL-vermeldingen kan niet meer bedragen dan	6000	C9500: 9000	C9500 hoogwaardige producten: 7500	9000	2500/9000/4000		
L4OPâ€™s/Label	8	8		8	8		
Ingress-VCUâ€™s	192	192		192	192		
Uitgaande VCUâ€™s	96	96		96	96		

Gerelateerde informatie

- Security Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9200 Switches)
- Security Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches)
- Security Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9400 Switches)
- Security Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9500 Switches)
- Security Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9600 Switches)
- Configuratiehandleiding voor systeembeheer, Cisco IOS XE Bengaluru 17.4.x (Catalyst 9500 Switches)
- Cisco technische ondersteuning en downloads

Opdrachten voor debuggen en overtrekken

Aantal	Opdracht	Opmerking
1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	Dump de Exception-tellers op de ASIC-#N.
2	show platform software fed [switch] active acl	Deze opdracht drukt de informatie over alle geconfigureerde ACLâ€™s op het vak af, samen met interface- en

		beleidsinformatie.
3	show platform software fed [switch] active acl policy 18	Deze opdracht drukt alleen de informatie over beleid 18 af. U kunt deze beleidsID van bevel 2 krijgen.
4	show platform software fed [switch] active acl interface intftype pacl	Deze opdracht drukt de informatie over de ACL af op basis van interfacetype (pacl/vacl/racl/gacl/sgacl enzovoort).
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Deze opdracht drukt de informatie over de ACL op basis van interfacetype (pacl/vacl/racl/gacl/sgacl enzovoort) en ook filters protocol-wise (ipv4/ipv6/mac enzovoort).
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Deze opdracht drukt de informatie over interfaces af.
7	show platform software fed [switch] active acl interface 0x9	Deze opdracht drukt de korte informatie van ACL af die op de interface wordt toegepast, op basis van de IIF-ID (opdracht vanaf 6).
8	show platform software fed [switch] active acl definition	Deze opdracht drukt de informatie over de op het vak geconfigureerde ACLâ€™s af en de aanwezigheid ervan in de CGD.
9	show platform software fed [switch] active acl iifid 0x9	Deze opdracht drukt de gedetailleerde informatie van ACL af die op de interface wordt toegepast, op basis van de IIF-ID.
10	show platform software fed [switch] active acl usage	Deze opdracht drukt het aantal VMR's af dat elke ACL gebruikt op basis van het functietype.
11	show platform software fed [switch] active acl policy intftype pacl vcu	Deze opdracht geeft u de beleidsinformatie en ook de VCU-informatie op basis van het interfacetype (pacl/vacl/racl/gacl/sgacl enzovoort).
12	show platform software fed [switch] active acl policy intftype pacl cam	Deze opdracht geeft u de beleidsinformatie en details over de VMRs in de CAM, gebaseerd op het interfacetype (pacl/valc/racl/gacl/sgacl etc.).
13	show platform software interface [switch] [active] R0 brief	Deze opdracht geeft u details over de interface op de doos.
14	show platform software fed [switch] active port if_id 9	Deze opdracht drukt de details over de poort af op basis van de IIF-ID.

15	show platform software fed [switch] active vlan 30	Deze opdracht drukt de gegevens over VLAN 30 af.
16	show platform software fed [switch] active acl cam asic 0	Deze opdracht drukt de volledige ACL-camera af op ASIC 0 die wordt gebruikt.
17	show platform software fed [switch] active acl counters hardware	Deze opdracht drukt alle ACL-tellers af van de hardware.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	Als u de vermeldingen voor de PBR-sectie afdrukt, kunt u verschillende secties geven zoals ACL en CPP in plaats van PBR.
19	show platform software fed [switch] active punt cpuq [1|2|3 â€¦]	Om de activiteit op een van de CPU-wachtrijen te controleren, hebt u ook opties om de status van de wachtrij voor debugging te wissen.
20	show platform software fed [switch] active ifm mappings gpn	Druk de interfacekaart met IIF-ID en GPN's af
21	show platform software fed [switch active ifm if-id	Druk de informatie over de interfaceconfiguratie, en affiniteit met ASIC af. Deze opdracht is handig om te controleren op welke interface de ASIC en CORE zijn.
22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error â€¦]	Het instellen van het spoor voor een specifieke functie in de FED.
23	request platform software trace rotate all	De sporenbuffer verwijderen.
24	show platform software trace message fed [switch] active	De sporenbuffer voor de FED afdrukken.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error â€¦]	De sporen voor FMAN inschakelen.
26	show platform software trace message forwarding-manager [switch] [active] f0	De sporenbuffer voor FMAN afdrukken.
27	debug platform software infrastructure punt detail	Stel het debuggen in op het PUNT.
28	debug ip cef packet all input rate 100	CEF-pakketdebugging is ingeschakeld.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.