Convalida degli ACL di sicurezza sugli switch Catalyst 9000

Sommario

Introduzione

In questo documento viene descritto come verificare e risolvere i problemi relativi agli ACL (Access Control List) sugli switch Catalyst serie 9000.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware:

- C9200
- C9300
- C9400
- C9500
- C9600

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota**: per i comandi utilizzati per abilitare queste funzionalità su altre piattaforme Cisco, consultare la guida alla configurazione appropriata.

Premesse

Gli ACL filtrano il traffico mentre passa attraverso un router o uno switch e autorizzano o negano i pacchetti che attraversano le interfacce specificate. Un ACL è una raccolta sequenziale di condizioni di autorizzazione e rifiuto che si applicano ai pacchetti. Quando si riceve un pacchetto su un'interfaccia, lo switch confronta i campi del pacchetto con gli ACL applicati per verificare che il pacchetto abbia le autorizzazioni richieste per essere inoltrato, in base ai criteri specificati negli elenchi degli accessi. Uno alla volta, verifica i pacchetti in base alle condizioni presenti in un elenco degli accessi. La prima corrispondenza determina se lo switch accetta o rifiuta i pacchetti. Poiché lo switch interrompe il test dopo la prima corrispondenza, l'ordine delle condizioni nell'elenco è critico. Se nessuna condizione corrisponde, lo switch rifiuta il pacchetto. Se non ci sono restrizioni, lo switch inoltra il pacchetto; in caso contrario, lo switch scarta il pacchetto. Lo switch può usare gli ACL su tutti i pacchetti inoltrati.

È possibile configurare gli elenchi degli accessi per fornire la sicurezza di base per la rete. Senza gli ACL configurati, tutti i pacchetti che passano attraverso lo switch possono essere autorizzati su tutti i componenti della rete. È possibile utilizzare gli ACL per controllare gli host che possono accedere a diverse parti di una rete o per decidere quali tipi di traffico devono essere inoltrati o bloccati sulle interfacce del router. È ad esempio possibile inoltrare il traffico di posta elettronica ma non il traffico Telnet.

Terminologia

ASSO	Access Control Entry (ACE): una singola regola o riga all'interno di un ACL
ACL	Access Control List (ACL) - Gruppo di ACE applicate a una porta

DACL	DACL (Downloadable ACL) - ACL con push dinamico tramite la policy di sicurezza ISE
PACL	ACL porta (PACL) - ACL applicato a un'interfaccia di layer 2
RACL	ACL con routing (RACL) - ACL applicato a un'interfaccia di layer 3
VACL	VACL (VLAN ACL) - ACL applicato a una VLAN
GACL	GACL (Group ACL) - ACL assegnato dinamicamente a un gruppo di utenti o a un client in base alla loro identità
ACL IP	Viene utilizzato per classificare i pacchetti IPv4/IPv6. Queste regole contengono vari campi e attributi dei pacchetti di layer 3 e layer 4, tra cui indirizzi IPv4 di origine e destinazione, porte di origine e destinazione TCP/UDP, flag TCP e DSCP, ecc.
MACL	MAC Address ACL (MACL) - Utilizzato per classificare pacchetti non IP. Le regole contengono vari campi e attributi di livello 2, tra cui l'indirizzo MAC di origine/destinazione, il tipo e così via.
L4OP	Porta operatore di livello 4 (L4OP) - Corrisponde alla logica diversa da EQ (Uguale a). GT (maggiore di), LT (minore di), NE (non uguale a) e RANGE (da-a)
VCU	Unità di confronto del valore (VCU, Value Comparison Unit) - I4OP vengono convertiti in VCU per eseguire la classificazione sulle intestazioni di layer 4
VMR	Value Mask Result (VMR) - Una voce ACE viene programmata internamente in TCAM come VMR.
CGD	Class Group Database (CGD) - Posizione in cui FMAN-FP memorizza il contenuto ACL
Classi	Identificazione delle voci ACE in CGD
CG	Class Group (CG) - Gruppo di classi che descrive come vengono identificati gli ACL in CGD
CGE	Voce del gruppo di classi (CGE) - Voce ACE memorizzata in un gruppo di classi
FMAN	Forwarding Manager (FMAN) - Il livello di programmazione tra Cisco IOS® XE e l'hardware
FED	Driver motore di inoltro (FED) - Componente che programma l'hardware del dispositivo

Esempi di utilizzo delle risorse ACL

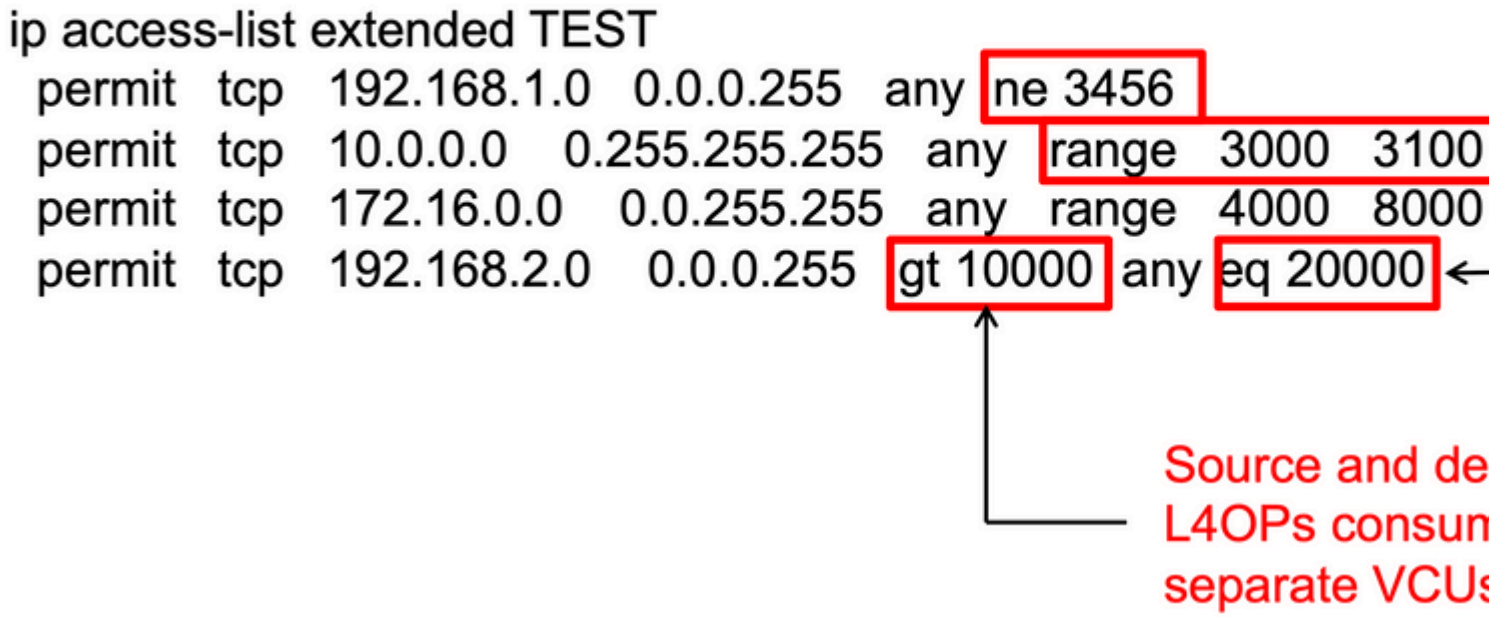
Di seguito vengono riportati tre esempi per dimostrare come gli ACL consumano TCAM, L4OP e VCU.

Esempio 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
```

	Voci TCAM	**L4OP**	**VCU**
Consumo	5	0	0

Esempio 2. TCAM IPv4/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

	Voci TCAM	**L4OP**	**VCU**
Consumo	4	5	7

Esempio 3. TCAM IPv6/L4OP/VCU

Le voci ACE IPv6 utilizzano due voci TCAM rispetto a una per IPv4. In questo esempio, quattro ACE utilizzano otto TCAM invece di quattro.

<#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

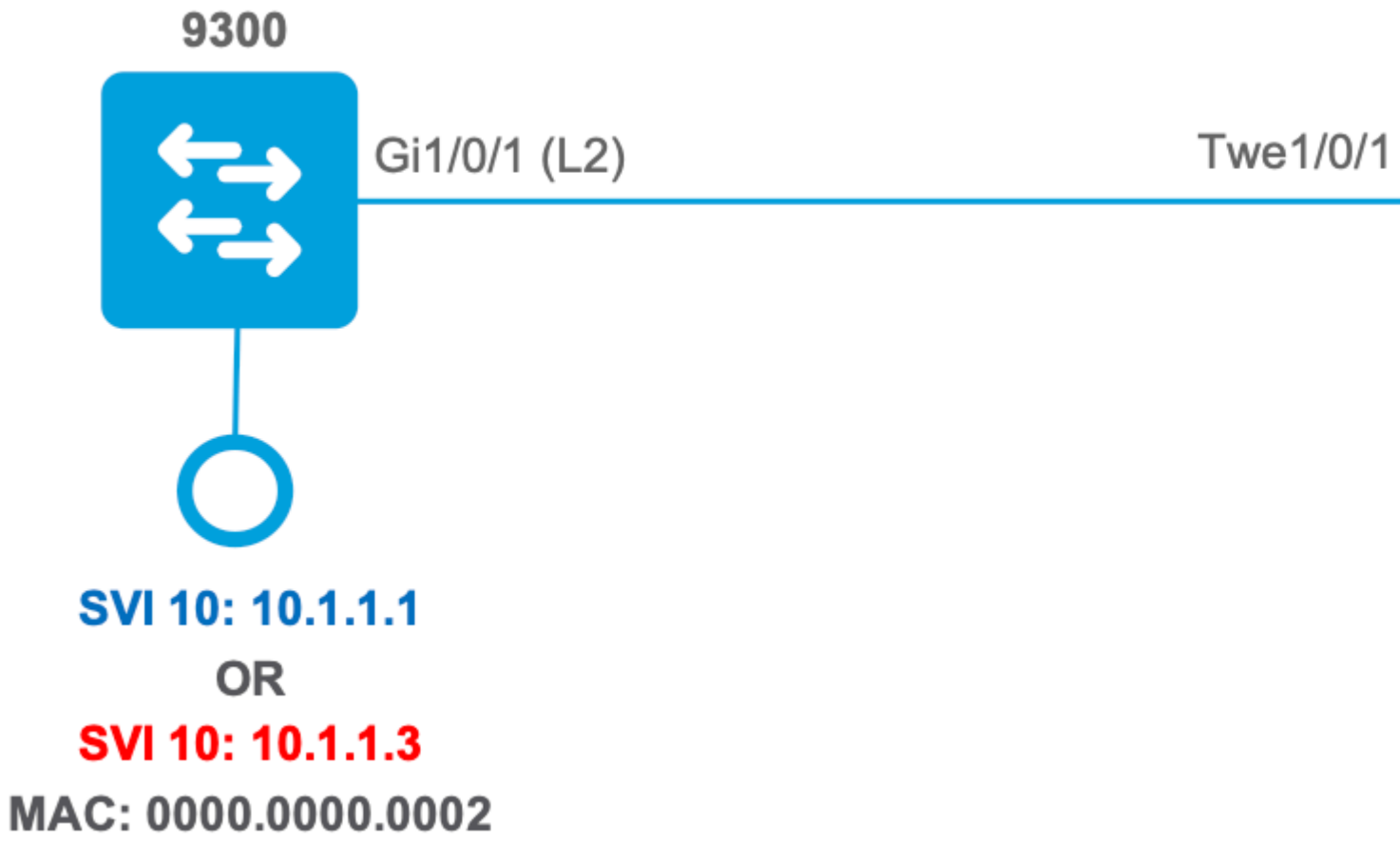
host 2001:DB8:C18:2:1::1

<-- One L4OP & VCU

	Voci TCAM	**L4OP**	**VCU**
Consumo	8	2	2

Topologia

La SVI 9300 VLAN 10 utilizza uno dei due indirizzi IP mostrati in questa immagine, a seconda che negli esempi venga mostrato un risultato in avanti o un risultato negativo.



Configurazione e verifica

In questa sezione viene descritto come verificare e risolvere i problemi relativi alla programmazione degli ACL nel software e nell'hardware.

Scenario 1. PACL (ACL IP)

I PACL vengono assegnati a un'interfaccia di layer 2.

- Limiti di sicurezza: porte o VLAN
- Allegato: interfaccia di layer 2
- Direzione: in entrata o in uscita (una alla volta)
- Tipi di ACL supportati: ACL MAC e ACL IP (standard o estesi)

Configurazione di PACL con ACL IP

<#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
```

Verifica PACL

Recuperate il valore IF_ID associato all'interfaccia.

```
<#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
```

Verificare l'ID del gruppo di classi (ID CG) associato a 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
```

Informazioni ACL associate all'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)

Informazioni sulla policy CG ID, nonché sulle interfacce che usano CG ID.

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

Confermare il funzionamento di PACL.

> **Nota:** Quando si immette il show ip access-lists privileged EXEC , il numero di corrispondenze visualizzato non tiene conto dei pacchetti ad accesso controllato nell'hardware. Per ottenere alcune statistiche di base sugli ACL dell'hardware per i pacchetti *commutati* e indirizzati, usare il comando show platform software *feed switch* {*switch_num*|active|standby}acl.

<#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. PACL (ACL MAC)

I PACL vengono assegnati a un'interfaccia di layer 2.

- Limiti di sicurezza: porte o VLAN
- Allegato: interfaccia di layer 2
- Direzione: in entrata o in uscita (una alla volta)
- Tipi di ACL supportati: ACL MAC e ACL IP (standard o estesi)

Configurare PACL con ACL MAC

```
<#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

Verifica PACL

Recuperate il valore IF_ID associato all'interfaccia.

<#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

Verificare l'ID del gruppo di classi (ID CG) associato a 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
```

Informazioni ACL associate all'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

Informazioni sulla policy CG ID, nonché sulle interfacce che usano CG ID.

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

Conferma funzionamento PACL:

- Il MACL consente solo l'indirizzo di origine 0001.aaaa.aaaa.
- Poiché si tratta di un ACL MAC, un pacchetto ARP non IP viene scartato e quindi il ping ha esito negativo.

```
<#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 è assegnato a un'interfaccia di layer 3, ad esempio un'interfaccia SVI o Routed.

- Limite di sicurezza: subnet diverse
- Allegato: interfaccia di layer 3
- Direzione: in ingresso o in uscita
- Tipi di ACL supportati: ACL IP (standard o estesi)

Configurazione di 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
```

Verifica RACL

Recuperate il valore IF_ID associato all'interfaccia.

```
<#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
```

Verificare l'ID del gruppo di classi (ID CG) associato a 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

Informazioni ACL associate all'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)
```

Informazioni sulla policy CG ID, nonché sulle interfacce che usano CG ID.

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

Confermare il funzionamento di RACL.

Nota: Quando si immette il show ip access-lists privileged EXEC , il numero di corrispondenze visualizzato non tiene conto dei pacchetti ad accesso controllato nell'hardware. Usare i contatori show platform software feed switch{*switch_num*|active|standby}aclin modalità di esecuzione privilegiata, per ottenere alcune statistiche di base sugli ACL hardware dei pacchetti commutati e indirizzati.

<#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

I VACL vengono assegnati a una VLAN di layer 2.

- Limiti di sicurezza: all'interno di una VLAN o attraverso una VLAN
- Allegato: mappa VLAN/VLAN
- Direzione: sia in entrata che in uscita contemporaneamente
- Tipi di ACL supportati: ACL MAC e ACL IP (standard o estesi)

Configura 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
```

Verifica VACL

Recuperate il valore IF_ID associato all'interfaccia.

<#root>

```
9500H#
```

show platform software fed active ifm interfaces vlan

Interface

IF_ID

State

Vlan10 0x00420010

READY

Verificare l'ID del gruppo di classi (ID CG) associato a 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
```

Informazioni ACL associate all'ID del gruppo CG.

Esistono due ACL utilizzati nello stesso criterio VACL denominato, raggruppati in questo gruppo di ACL

<#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
```

Informazioni sulla policy CG ID, nonché sulle interfacce che usano CG ID.

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

Confermare il funzionamento di VACL.

- La risoluzione dei problemi è lo stesso scenario delle sezioni PACL e RACl. Fare riferimento a queste sezioni per i dettagli sul test ping.
- Ping da 10.1.1.3 a 10.1.1.2 negato dai criteri ACL applicati.
- Controllare il comando 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...>
```

Scenario 5. ACL gruppo/client (DACL)

Gli ACL di gruppo/client vengono applicati dinamicamente a un gruppo di utenti o a un client in base alla loro identità. Questi elementi vengono talvolta denominati anche DACL.

- Limite di sicurezza: client (livello interfaccia client)
- Allegato: interfaccia per client
- Direzione: solo in ingresso
- Tipi di ACL supportati: ACL MAC e ACL IP (standard o estesi)

Configurazione di 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 ar
```

Verifica GACL

ID gruppo CG associato a 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
```

Informazioni ACL associate all'ID GC del gruppo.

```
<#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. Registrazione ACL

Il software del dispositivo può fornire messaggi syslog relativi a pacchetti autorizzati o rifiutati da un elenco di accesso IP standard. Se un pacchetto corrisponde all'ACL, viene inviato alla console un messaggio informativo sul pacchetto. Il livello dei messaggi registrati nella console è controllato dalconsole di registrazionecomandi che controllano i messaggi Syslog.

- I messaggi di log ACL non sono supportati per gli ACL utilizzati con Unicast Reverse Path Forwarding (uRPF). È supportato solo per RACL.
- Il log ACL nella direzione di uscita non è supportato per i pacchetti generati dal control plane del dispositivo.
- Il routing viene eseguito nell'hardware e nel software di accesso, quindi se un numero elevato di pacchetti corrisponde a un'autorizzazione o a una negazione di ACE contenente una parola chiave di accesso, il software non è in grado di corrispondere alla velocità di elaborazione dell'hardware e non tutti i pacchetti possono essere registrati.
- Il primo pacchetto che attiva l'ACL genera immediatamente un messaggio di registro e i pacchetti successivi vengono raccolti in intervalli di 5 minuti prima di essere visualizzati o registrati. Il messaggio log include il numero dell'elenco degli accessi, se il pacchetto è stato autorizzato o rifiutato, l'indirizzo IP di origine del pacchetto e il numero di pacchetti provenienti da quell'origine consentiti o rifiutati nei 5 minuti precedenti.
- Per i dettagli completi sul comportamento e le restrizioni del log ACL, consultare la guida alla configurazione della sicurezza di Cisco IOS XE, come indicato nella sezione Informazioni correlate.

Esempio di log PACL:

Nell'esempio viene mostrato un caso negativo, in cui il tipo di ACL e la parola chiave log non funzionano

insieme.

```
<#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
```

Esempio di log 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
```

Esempio di registro RACL (Permit):
Quando si utilizza un'istruzione log per un'istruzione allow, i risultati del contatore software mostrano il doppio del numero di pacchetti inviati.

<#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)
```

Risoluzione dei problemi

Statistiche ACL

Quando si risolve un problema con un ACL, è essenziale capire come e dove le statistiche ACL vengono misurate dal dispositivo.

- Le statistiche ACL vengono raccolte a un livello aggregato e non a livello ACE.
- L'hardware non è in grado di consentire per stato ACE o ACL.
- Vengono raccolte statistiche quali Nega, Registra e Pacchetti inoltrati dalla CPU.
- Le statistiche relative ai pacchetti MAC, IPv4 e IPv6 vengono raccolte separatamente.
- show platform software fed switch active acl counters hardware può essere utilizzato per visualizzare le statistiche aggregate.

Cancellazione delle statistiche ACL

Quando si risolve un problema relativo ad un ACL, può essere utile cancellare i vari contatori dell'ACL per ottenere nuovi conteggi della baseline.

- Questi comandi consentono di cancellare le statistiche dei contatori degli ACL software e hardware.
- Quando si risolvono i problemi di corrispondenze con gli ACL, si consiglia di cancellare gli ACL rilevanti dalle corrispondenze della baseline recenti o rilevanti.

<#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)
```

Cosa succede quando ACL TCAM è esaurito?

- Gli ACL vengono sempre applicati nell'hardware TCAM. Se il software TCAM è già usato dagli ACL configurati in precedenza, i nuovi ACL non ricevono le risorse ACL necessarie per la programmazione.

- Se si aggiunge un ACL dopo aver esaurito il TCAM, tutti i pacchetti vengono scartati per l'interfaccia a cui sono collegati.

- L'azione di mantenere un ACL nel software è chiamata **Unload** (scaricamento).
- Quando le risorse diventano disponibili, lo switch cerca automaticamente di programmare gli ACL nell'hardware. Se il processo ha esito positivo, gli ACL vengono trasferiti all'hardware e i pacchetti iniziano a essere inoltrati.
- L'azione di programmazione di un ACL software-held in TCAM è chiamata **Ricaricamento**.

- È possibile scaricare e ricaricare i pacchetti PACL, VACL, RACL e GACL indipendentemente l'uno dall'altro.

Esaurimento ACL TCAM

- L'interfaccia a cui viene applicato l'ACL appena aggiunto inizia a eliminare i pacchetti finché non diventano disponibili le risorse hardware.
- I client GACL vengono messi nello stato UnAuth.

Esaurimento VCU

- Una volta superato il limite L4OPs o usciti dalle VCU, il software esegue l'espansione ACL e crea nuove voci ACE per eseguire un'azione equivalente senza usare le VCU.
- In tal caso, il TCAM può esaurirsi a causa di queste voci aggiunte.

Errori syslog ACL

Se una particolare risorsa ACL di sicurezza si esaurisce, il sistema genera messaggi SYSLOG (interfaccia, VLAN, etichetta e così via, i valori possono essere diversi).

Messaggio di log ACL	Definizione	Azione di ripristino
%ACL_ERRMSG-4-UNLOADED: alimentazione switch 1: l'input <ACL> sull'interfaccia <interface> non è programmato nell'hardware e il traffico viene interrotto.	ACL scaricato (tenuto nel software)	Esaminate la scala TCAM. Se la scalabilità è superiore, riprogettare gli ACL.
%ACL_ERRMSG-6-REMOVED: 1 feed: la configurazione scaricata per Input <ACL> sull'interfaccia <interface> è stata rimossa per label <label>asic<number>.	La configurazione ACL scaricata è stata rimossa dall'interfaccia	L'ACL è già stato rimosso. Nessuna azione da eseguire
%ACL_ERRMSG-6-RELOADED: feed 1: l'input <ACL> sull'interfaccia <interface> è stato caricato nell'hardware per l'etichetta <label> su asic<number>.	L'ACL è ora installato nell'hardware	Il problema con l'ACL è stato risolto. Nessuna azione da eseguire

%ACL_ERRMSG-3-ERROR: feed 1: la configurazione dell'ACL IP <ACL> di input <NAME> non è applicata a <interface> all'ordine di binding <number>.	Altri tipi di errore ACL (ad esempio, errore di installazione ACL dot1x)	Verificare che la configurazione ACL sia supportata e che TCAM non superi la scalabilità
%ACL_ERRMSG-6-GACL_INFO: Switch 1 R0/0: feed: la registrazione non è supportata per GACL.	Per GACL è configurata un'opzione di registro	GACL non supporta i registri. Rimuovere le istruzioni di registro da GACL.
%ACL_ERRMSG-6-PACL_INFO: opzione 1 R0/0: feed: registrazione non supportata per PACL.	Per il file PACL è configurata un'opzione di registro	Il PACL non supporta i registri. Rimuovere le istruzioni di registro da PACL.
%ACL_ERRMSG-3-ERROR: switch 1 R0/0: feed: gruppo IPv4 di input ACL implicit_deny:<nome>: configurazione non applicata al client MAC 0000.000.0000.	(dot1x) Impossibile applicare l'ACL alla porta di destinazione	Verificare che la configurazione ACL sia supportata e che TCAM non superi la scalabilità

Scenari di risorse e azioni di ripristino insufficienti

Scenario 1. Binding ACL	Azione di ripristino
• L'ACL viene creato e applicato a un'interfaccia o a una VLAN. • Il binding non riesce a causa di condizioni di 'risorse esaurite', ad esempio esaurimento TCAM. • Nessuna voce di controllo di accesso all'interno dell'ACL può essere programmata in TCAM. L'ACL rimane nello stato **UNLOADED**. • In stato **UNLOADED** (SCARICATO), tutto il traffico (inclusi i pacchetti di controllo) sull'interfaccia viene interrotto fino a quando il problema non viene risolto.	Riprogettare l'ACL in modo da ridurre l'uso di TCAM.
Scenario 2. Modifica ACL	**Azione di ripristino**
• Viene creato un ACL che viene applicato a un'interfaccia. Inoltre, a questo ACL vengono aggiunte altre voci ACE mentre viene applicato alle interfacce. • Se TCAM non dispone di risorse, l'operazione di modifica non riesce.	Riprogettare l'ACL in modo da ridurre l'uso di TCAM.

• Nessuna voce di controllo di accesso all'interno dell'ACL può essere programmata in TCAM. L'ACL rimane nello stato **UNLOADED**. • Nello stato **UNLOADED** (SCARICATO), tutto il traffico (inclusi i pacchetti di controllo) sull'interfaccia diminuisce finché il problema non viene risolto. • Anche le voci ACL esistenti hanno esito negativo nello stato **UNLOADED** finché non vengono corrette.	
Scenario 3. Riassociazione ACL	**Azione di ripristino**
• Per riassociazione di ACL si intende il collegamento di un ACL a un'interfaccia e quindi il collegamento di un altro ACL alla stessa interfaccia senza scollegare il primo ACL. • Creazione e collegamento del primo ACL completati. • Viene creato un ACL di dimensioni maggiori con un nome diverso e lo stesso protocollo (IPv4/IPv6), che viene quindi associato alla stessa interfaccia. • Il dispositivo scollega correttamente il primo ACL e tenta di collegarlo a questa interfaccia. • Se TCAM non dispone di risorse, l'operazione di riassociazione non riesce. • Nessuna voce di controllo di accesso all'interno dell'ACL può essere programmata in TCAM. L'ACL rimane nello stato **UNLOADED**. • In stato **UNLOADED** (SCARICATO), tutto il traffico (inclusi i pacchetti di controllo) sull'interfaccia viene interrotto fino a quando il problema non viene risolto.	Riprogettare l'ACL in modo da ridurre l'uso di TCAM.
Scenario 4. Associare un ACL vuoto (Null)	**Azione di ripristino**
• Un ACL senza voci ACE viene creato e collegato a un'interfaccia. • Il sistema crea internamente questo ACL con un'autorizzazione 'any ACE' e lo collega all'interfaccia nell'hardware (tutto il traffico è autorizzato in questo stato). • Le voci ACE vengono quindi aggiunte all'ACL con lo stesso nome o numero. Il sistema programma TCAM man mano che viene aggiunta ogni voce ACE. • Se il TCAM esaurisce le risorse quando si aggiungono voci ACE, l'ACL viene spostato nello stato **UNLOADED**.	Riprogettare l'ACL in modo da ridurre l'uso di TCAM.

• In stato **UNLOADED** (SCARICATO), tutto il traffico (inclusi i pacchetti di controllo) sull'interfaccia viene interrotto fino a quando il problema non viene risolto. • Anche le voci ACL esistenti hanno esito negativo nello stato **UNLOADED** finché non vengono corrette.	

Verifica della scala ACL

In questa sezione vengono illustrati i comandi per determinare la scala ACL e l'utilizzo del TCAM.

Riepilogo elenco accessi FMAN:

Identificare gli ACL configurati e il numero totale di ACE 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
```

Uso 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

Utilizzo TCAM (17,x):

Il comando TCAM usage ha differenze significative tra i treni 16.x e 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)

Utilizzo TCAM (16,x):

Il comando TCAM usage ha differenze significative tra i treni 16.x e 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...>

Modello SDM personalizzato (riallocazione TCAM)

Uso di Cisco IOS XE Bengaluru 17.4.1, è possibile configurare un modello SDM personalizzato per le funzionalità degli ACL usando sdm prefer custom acl

Per informazioni dettagliate su come configurare e verificare questa funzionalità, consultare la guida alla configurazione della gestione del sistema, Cisco IOS XE Bengaluru 17.4.x (switch Catalyst 9500).

In questa sezione vengono illustrati alcuni tipi di configurazione e verifiche di base.

Verificare il modello SDM corrente:

```
<#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
```

Modificare il modello SDM corrente:

- 9500H(config)#**sdm: preferenza per l'acl personalizzato**
  9500H (config-sdm-acl)#**acl-ingress 26 priority 1 <â€" applica il nuovo valore 26K. (priorità discussa nella guida alla configurazione)**
  9500H (config-sdm-acl)#**acl-egress 20 priorità 2**
  9500H (config-sdm-acl)#**esci**
  Utilizzo show sdm prefer custom per vedere i valori proposti e sdm prefer custom commit per applicare la "visualizzazione delle modifiche" tramite questa CLI.
- Verificare le modifiche al profilo SDM.
- 9500H#**mostra sdm preferenza personalizzata**

Visualizzazione delle informazioni sul modello SDM:

Modello personalizzato con i relativi dettagli.
Voci di controllo di accesso per la sicurezza in ingresso*: **12288 (corrente) - 26624 (proposta) <â€”**
Utilizzo corrente e proposto (26.000 proposti)
Voci di controllo dell'accesso di sicurezza in uscita*: **15360 (corrente) - 20480 (proposta)**

9500H#**show sdm preferisce l'input dell'utente personalizzato**

INPUT UTENTE FUNZIONALITÀ ACL
Valori input utente
==========

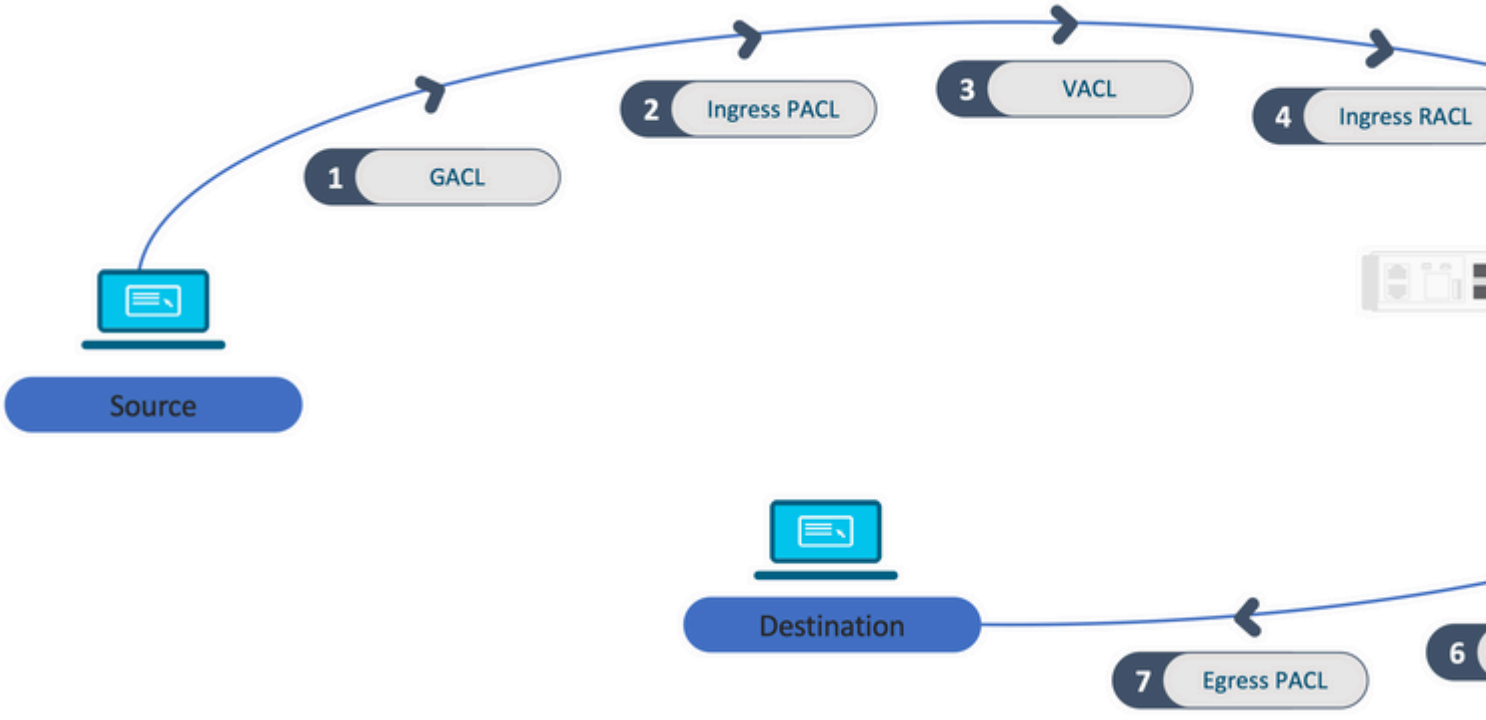
PRIORITÀ NOME FUNZIONALITÀ **SCALA**
â€”
Voci di controllo di accesso di protezione in ingresso: **1 26*1024 <â€” modificato dall'ingresso utente a 26 x 1024 (26K)**
Voci di controllo dell'accesso di sicurezza in uscita: **2 20*1024 <â€” modificato dall'input dell'utente a 20 x 1024 (20K)**

- Applica le modifiche al profilo SDM.
- 9500H(config)#**sdm preferisce il commit personalizzato**
  Le modifiche apportate alle preferenze SDM in esecuzione vengono memorizzate e diventano effettive al successivo caricamento. **<â€” Una volta ricaricato, ACL TCAM viene allocato al valore personalizzato.**

Ulteriori informazioni:

Ordine di elaborazione ACL:

Gli ACL vengono elaborati in questo ordine, dall'origine alla destinazione.



ACL programmati in uno stack:

- Gli ACL non basati sulle porte (ad esempio, VACL, RACL) vengono applicati al traffico di uno switch e vengono programmati su tutti gli switch dello stack.
- Gli ACL basati sulle porte vengono applicati solo al traffico su una porta e vengono programmati solo sullo switch che possiede l'interfaccia.
- Gli ACL vengono programmati dallo switch Active e successivamente applicati agli switch Member.
- Le stesse regole si applicano ad altre opzioni di ridondanza, ad esempio ISSU/SVL.

Espansione ACL:

- L'espansione degli ACL si verifica quando il dispositivo esaurisce gli L4OP, le etichette o le VCU. Il dispositivo deve creare più ACE equivalenti per eseguire la stessa logica e per eseguire rapidamente lo scarico di TCAM.
- **### Gli ACL4OP sono in scala e questo ACL è stato creato ##**
  9500H(config)#**ip access-list extended TEST**
  9500H (config-ext-nacl)#**consenti tcp 10.0.0.0.255.255.255 qualsiasi gt 150 <â€" corrisponde alle porte 151 e superiori**

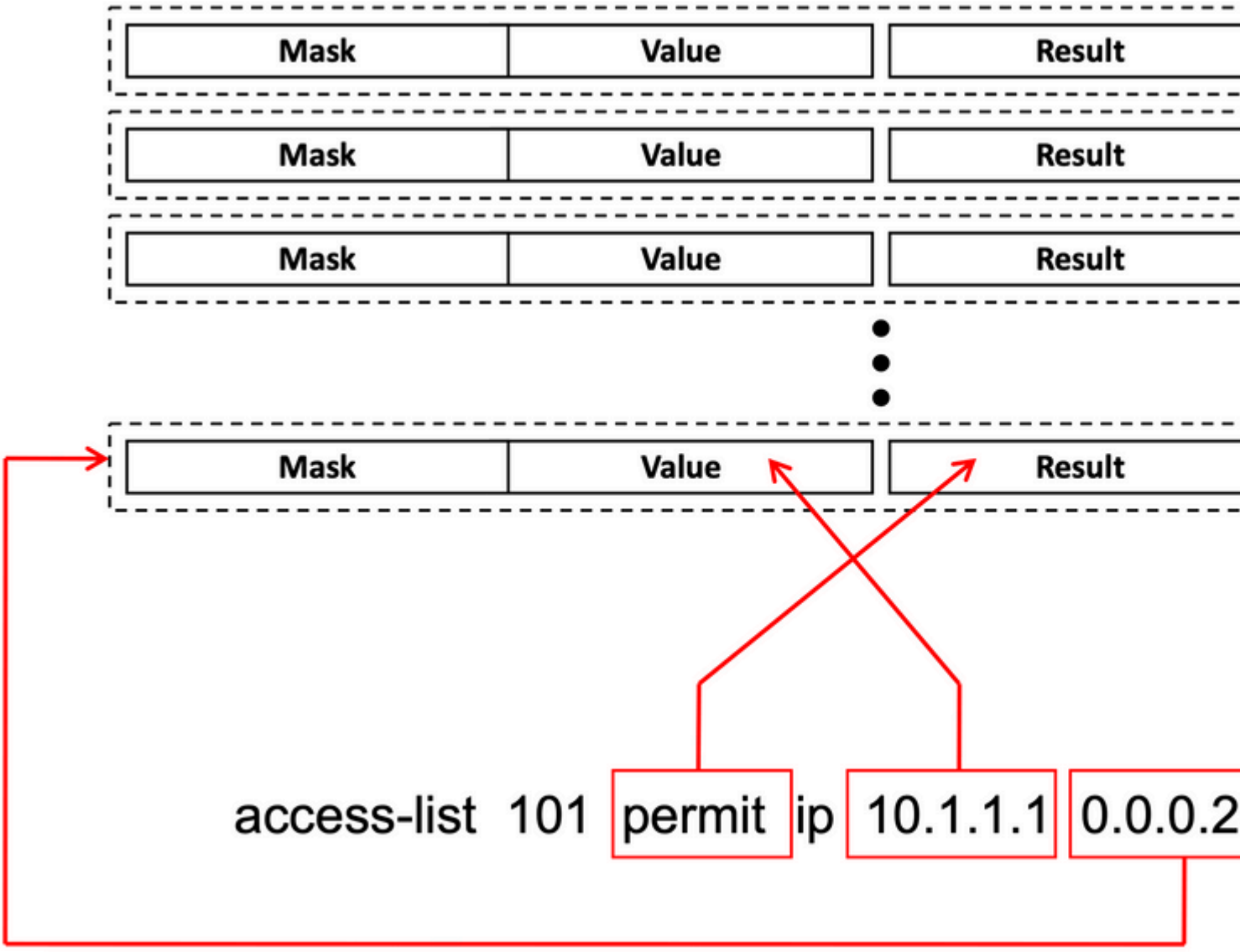
  ### Deve essere espanso in più ACE che non utilizzano un L4OP ###
  9500H(config-ext-nacl)#**allow tcp 10.0.0.0 0.255.255.255 any eq 151**
  9500H(config-ext-nacl)#**allow tcp 10.0.0.0 0.255.255.255 any eq 152**
  9500H(config-ext-nacl)#**allow tcp 10.0.0.0 0.255.255.255 any eq 153**
  9500H(config-ext-nacl)#**allow tcp 10.0.0.0 0.255.255.255 any eq 154**
  ... e così via....

Consumo TCAM e condivisione di etichette:

- A ciascun criterio ACL fa riferimento internamente un'etichetta.
- Quando si applicano i criteri ACL (ACL di sicurezza come GACL, PACL, VACL, RACL) a più interfacce o VLAN, viene usata la stessa etichetta.
- Gli ACL in entrata/in uscita usano spazi di etichetta diversi.
- IPv4, IPv6 e ACL MAC utilizzano altri spazi di etichette.
- Lo stesso PACL viene applicato all'entrata dell'interfaccia A e all'uscita dell'interfaccia A. Ci sono due istanze del PACL nel TCAM, ognuna con un'etichetta univoca per Ingress ed Egress.
- Se lo stesso PACL con un L4OP viene applicato a più interfacce in entrata esistenti su ciascun core, esistono due istanze dello stesso PACL programmate in TCAM, una per ciascun core.

Descrizione VMR:

Un ACE viene programmato internamente in TCAM come 'VMR' - noto anche come Valore, Maschera, Risultato. Ogni voce ACE può utilizzare VMR e VCU.



Scalabilità ACL:

Le risorse ACL di sicurezza sono dedicate agli ACL di sicurezza. Non vengono condivise con altre funzionalità.

Risorse ACL TCAM	**Cisco Catalyst 9600**	**Cisco Catalyst 9500**	**Cisco Catalyst 9400**	**Cisco Catalyst 9300**	**Cisco Catalyst 9200**				
Voci IPv4	In ingresso: 12000*	In uscita: 15000*	C9500: 18000*	Prestazioni elevate C9500 In ingresso: 12000* In uscita: 15000*	18000*	C9300: 5000	C9300B 18000	C9300X:8000	1000

Voci IPv6	Metà delle voci IPv4	Metà delle voci IPv4		Metà delle voci IPv4	Metà delle voci IPv4			Metà delle voci IPv4
Un tipo di voci ACL IPv4 non può superare	12000	C9500: 18000	Prestazioni elevate di C9500: 15000	18000	C9300: 5000	C9300B: 18000	C9300X: 8000	1000
Un tipo di voci ACL IPv6 non può superare	6000	C9500: 9000	Prestazioni elevate di C9500: 7500	9000	2500/9000/4000			500
L4OP/Etichetta	8	8		8	8			8
VCU in ingresso	192	192		192	192			192
VCU in uscita	96	96		96	96			96

Informazioni correlate

- Guida alla configurazione della sicurezza, Cisco IOS XE Amsterdam 17.3.x (switch Catalyst 9200)
- Guida alla configurazione della sicurezza, Cisco IOS XE Amsterdam 17.3.x (switch Catalyst 9300)
- Guida alla configurazione della sicurezza, Cisco IOS XE Amsterdam 17.3.x (switch Catalyst 9400)
- Guida alla configurazione della sicurezza, Cisco IOS XE Amsterdam 17.3.x (switch Catalyst 9500)
- Guida alla configurazione della sicurezza, Cisco IOS XE Amsterdam 17.3.x (switch Catalyst 9600)
- Guida alla configurazione della gestione del sistema, Cisco IOS XE Bengaluru 17.4.x (switch Catalyst 9500)
- Supporto tecnico e download Cisco

Comandi Debug e Trace

Num.	Comando	Osservazioni
1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	Eseguire il dump dei contatori Exception sull'ASIC #N.
2	show platform software fed [switch] active acl	Con questo comando vengono stampate sulla casella le informazioni su tutti gli ACL configurati, insieme alle informazioni sull'interfaccia e sui criteri.

3	show platform software fed [switch] active acl policy 18	Questo comando stampa solo le informazioni relative al criterio 18. È possibile ottenere questo ID criterio dal comando 2.
4	show platform software fed [switch] active acl interface intftype pacl	Questo comando stampa le informazioni sull'ACL in base al tipo di interfaccia (pacl/vacl/racl/gacl/sgacl e così via).
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Questo comando stampa le informazioni sull'ACL in base al tipo di interfaccia (pacl/vacl/racl/gacl/sgacl e così via) e filtra anche in base al protocollo (ipv4/ipv6/mac e così via).
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Questo comando stampa le informazioni sulle interfacce.
7	show platform software fed [switch] active acl interface 0x9	Questo comando stampa le brevi informazioni dell'ACL applicato all'interfaccia, in base all'IIF-ID (comando da 6).
8	show platform software fed [switch] active acl definition	Questo comando stampa le informazioni sugli ACL configurati nella casella e la cui presenza è nel CGD.
9	show platform software fed [switch] active acl iifid 0x9	Questo comando stampa le informazioni dettagliate dell'ACL applicato all'interfaccia, in base all'ID IIF.
10	show platform software fed [switch] active acl usage	Con questo comando viene stampato il numero di VMR utilizzati da ciascun ACL in base al tipo di funzione.
11	show platform software fed [switch] active acl policy intftype pacl vcu	Questo comando fornisce le informazioni sui criteri e le informazioni VCU in base al tipo di interfaccia (pacl/vacl/racl/gacl/sgacl e così via).
12	show platform software fed [switch] active acl policy intftype pacl cam	Questo comando fornisce le informazioni sulla policy e i dettagli sui VMR nel CAM, in base al tipo di interfaccia (pacl/valc/racl/gacl/sgacl e così via).
13	show platform software interface [switch] [active] R0 brief	Questo comando fornisce informazioni dettagliate sull'interfaccia della confezione.
14	show platform software fed [switch] active port if_id 9	Con questo comando vengono stampati i dettagli sulla porta in base all'ID IIF-ID.
15	show platform software fed [switch] active vlan 30	Con questo comando vengono stampati i dettagli sulla VLAN 30.

16	show platform software fed [switch] active acl cam asic 0	Questo comando stampa la camma ACL completa sull'ASIC 0 in uso.
17	show platform software fed [switch] active acl counters hardware	Questo comando stampa tutti i contatori ACL dell'hardware.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	Stampando le voci per la sezione PBR, potete fornire diverse sezioni come ACL e CPP invece di PBR.
19	show platform software fed [switch] active punt cpuq [1|2|3 â€¦]	Per controllare l'attività su una delle code CPU, sono disponibili anche opzioni che consentono di cancellare lo stato delle code per il debug.
20	show platform software fed [switch] active ifm mappings gpn	Stampa il mapping dell'interfaccia con l'ID IIF e i numeri GPN
21	show platform software fed [switch active ifm if-id	Stampare le informazioni sulla configurazione dell'interfaccia e l'affinità con l'ASIC. Questo comando è utile per verificare quale interfaccia siano l'ASIC e il CORE.
22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error â€¦]	Impostazione della traccia per una funzionalità specifica in FED.
23	request platform software trace rotate all	Cancellazione del buffer di traccia.
24	show platform software trace message fed [switch] active	Stampa del buffer di traccia per FED.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error â€¦]	Abilitazione delle tracce per FMAN.
26	show platform software trace message forwarding-manager [switch] [active] f0	Stampa del buffer di traccia per FMAN.
27	debug platform software infrastructure punt detail	Impostare il debug su PUNT.
28	debug ip cef packet all input rate 100	Debug del pacchetto CEF attivato.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).