Validar ACL de seguridad en switches Catalyst 9000

Contenido

Introducción

Este documento describe cómo verificar y resolver problemas de ACL (listas de control de acceso) en los switches Catalyst 9000 Series.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de hardware:

- C9200
- C9300
- C9400
- C9500
- C9600

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

> **Nota**: Consulte la guía de configuración correspondiente para conocer los comandos utilizados para habilitar estas funciones en otras plataformas de Cisco.

Antecedentes

Las ACL filtran el tráfico a medida que pasa a través de un router o switch y permiten o deniegan paquetes que cruzan interfaces especificadas. Una ACL es una colección secuencial de condiciones de permiso y denegación que se aplican a los paquetes. Cuando se recibe un paquete en una interfaz, el switch compara los campos en el paquete con cualquier ACL aplicada para verificar que el paquete tiene los permisos requeridos para ser reenviado, según los criterios especificados en las listas de acceso. Uno por uno, prueba los paquetes contra las condiciones de una lista de acceso. La primera coincidencia decide si el switch acepta o rechaza los paquetes. Debido a que el switch deja de probar después de la primera coincidencia, el orden de las condiciones en la lista es crítico. Si no coincide ninguna condición, el switch rechaza el paquete. Si no hay restricciones, el switch reenvía el paquete; de lo contrario, el switch descarta el paquete. El switch puede utilizar ACL en todos los paquetes que reenvía.

Puede configurar listas de acceso para proporcionar seguridad básica a su red. Si no configura las ACL, todos los paquetes que pasan a través del switch se pueden permitir en todas las partes de la red. Puede utilizar las ACL para controlar qué hosts pueden acceder a diferentes partes de una red o para decidir qué tipos de tráfico se reenvían o bloquean en las interfaces del router. Por ejemplo, puede reenviar el tráfico de correo electrónico, pero no el tráfico Telnet.

Terminology

AS	Entrada de control de acceso (ACE): una única regla/línea dentro de una ACL
ACL	Lista de control de acceso (ACL): grupo de ACE aplicadas a un puerto

DACL	ACL descargable (DACL): ACL transmitida de forma dinámica mediante la política de seguridad de ISE
PACL	ACL de puerto (PACL): ACL aplicada a una interfaz de capa 2
RACL	ACL enrutada (RACL): ACL aplicada a una interfaz de capa 3
VACL	VLAN ACL (VACL): ACL aplicada a una VLAN
GACL	ACL de grupo (GACL): ACL asignada dinámicamente a un grupo de usuarios o cliente en función de su identidad
ACL IP	Se utiliza para clasificar paquetes IPv4/IPv6. Estas reglas contienen varios campos y atributos de paquetes de capa 3 y capa 4, entre los que se incluyen, entre otros, las direcciones IPv4 de origen y destino, los puertos de origen y destino TCP/UDP, los indicadores TCP y DSCP.
MACL	Mac Address ACL (MACL): se utiliza para clasificar paquetes que no son IP. Las reglas contienen varios campos y atributos de capa 2, incluida la dirección MAC de origen/destino, el tipo de Ether, etc.
L4OP	Puerto de operador de capa 4 (L4OP): Coincide con la lógica distinta de EQ (igual a). GT (mayor que), LT (menor que), NE (no igual a) y RANGE (de a)
VCU	Unidad de comparación de valor (VCU): las L4OP se convierten en VCU para realizar la clasificación en los encabezados de capa 4
VMR	Resultado de la máscara de valor (VMR): una entrada ACE se programa internamente en TCAM como VMR.
CGD	Base de datos de grupos de clases (CGD): donde FMAN-FP almacena contenido de ACL
Clases	Cómo se identifican las ACE en CGD
CG	Grupo de clases (CG): grupo de clases sobre cómo se identifican las ACL en CGD
CGE	Entrada de grupo de clases (CGE): entrada ACE almacenada en un grupo de clases
FMAN	Forwarding Manager (FMAN): capa de programación entre Cisco IOS® XE y el hardware.
FED	Controlador de motor de reenvío (FED): componente que programa el hardware del dispositivo

Ejemplos de Utilización de Recursos ACL

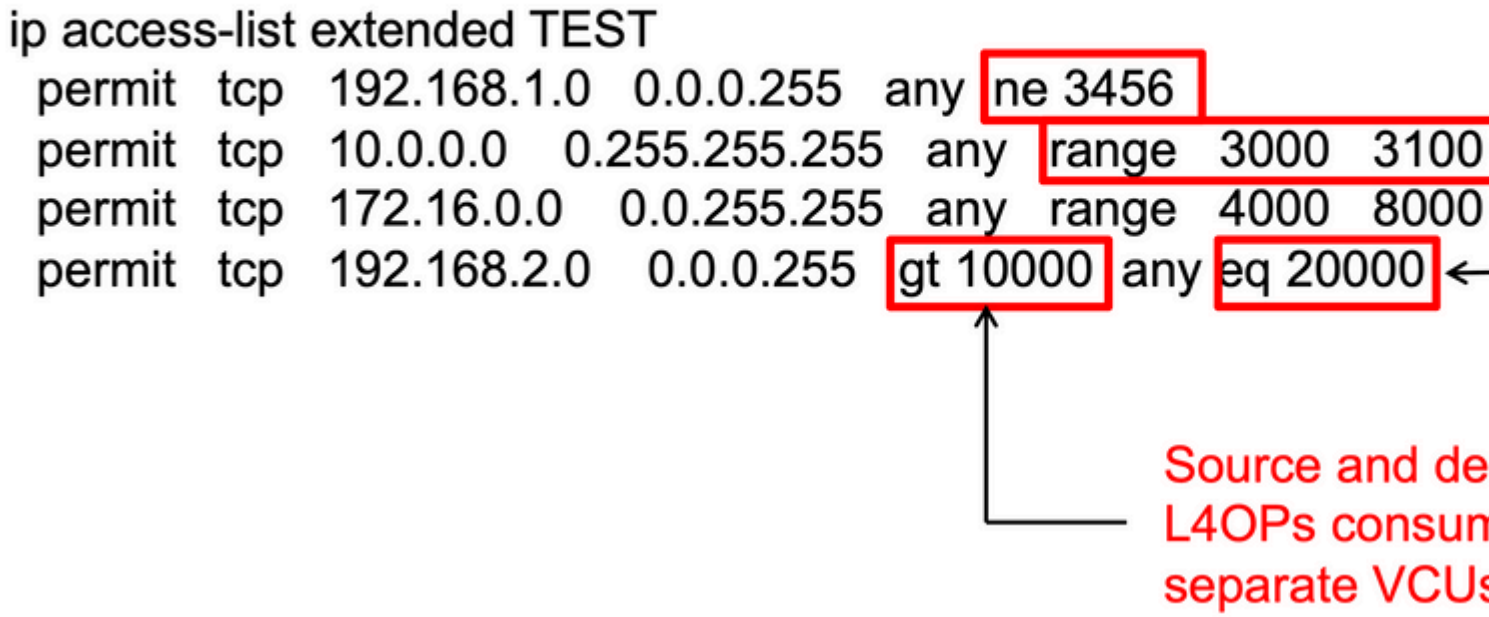
Aquí se dan tres ejemplos para demostrar cómo las ACL consumen TCAM, L4OP y VCU.

Ejemplo 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
```

	Entradas TCAM	**L4OP**	**VCU**
Consumo	5	0	0

Ejemplo 2. TCAM/L4OP/VCU IPv4



<#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

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

Ejemplo 3. TCAM/L4OP/VCU IPv6

Las ACE IPv6 utilizan dos entradas TCAM frente a una para IPv4. En este ejemplo, cuatro ACE consumen ocho TCAM en lugar de cuatro.

<#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

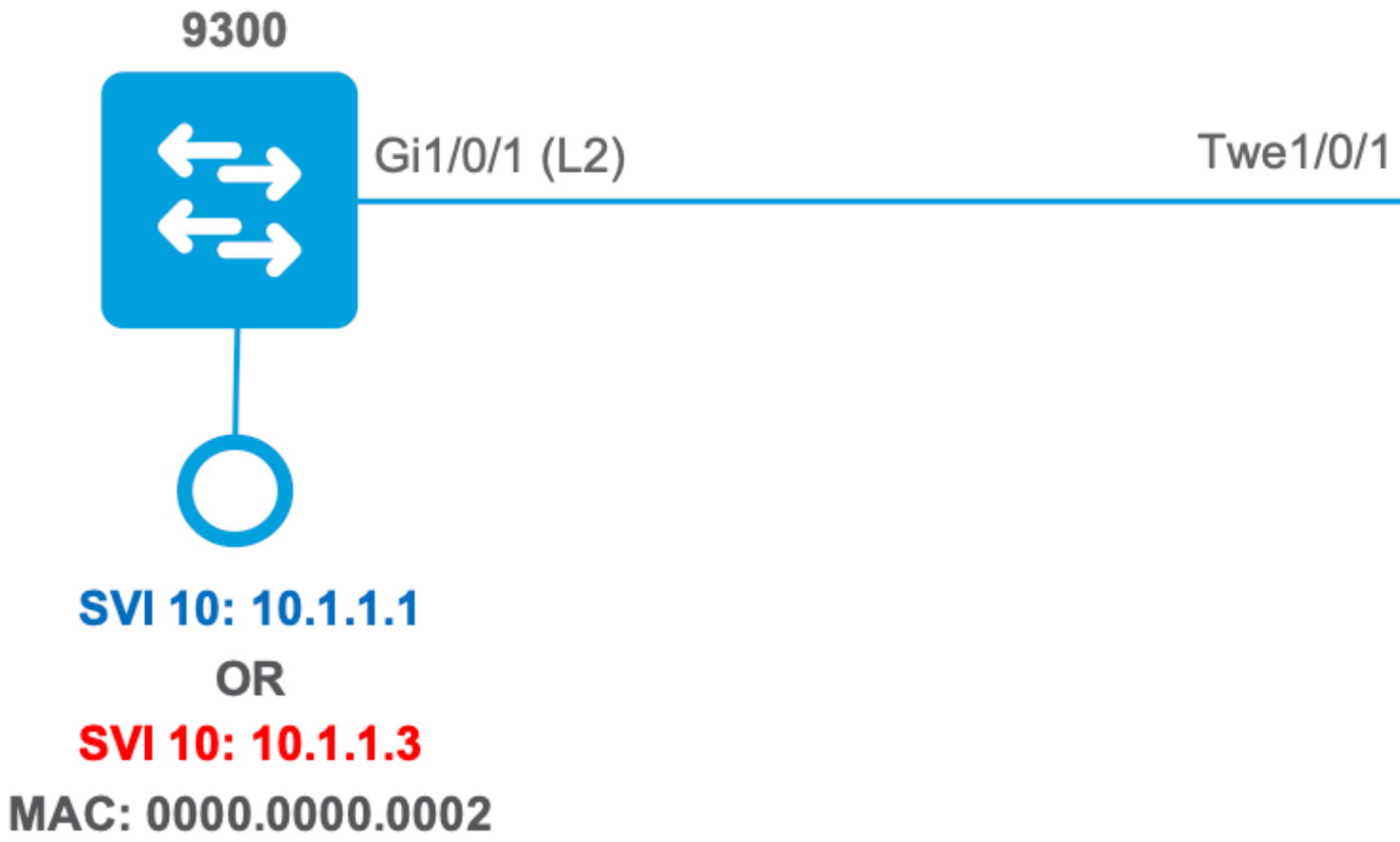
host 2001:DB8:C18:2:1::1

<-- One L4OP & VCU

	Entradas TCAM	**L4OP**	**VCU**
Consumo	8	2	2

Topología

La SVI 9300 VLAN 10 utiliza una de las dos direcciones IP que se muestran en esta imagen, en función de si se muestra un resultado de reenvío o descarte en los ejemplos.



Configurar y verificar

Esta sección trata sobre cómo verificar y resolver problemas de programación ACL en software y hardware.

Escenario 1. PACL (IP ACL)

Las PACL se asignan a una interfaz de capa 2.

- Límite de seguridad: puertos o VLAN
- Adjunto: interfaz de capa 2
- Dirección: entrada o salida (de uno en uno)
- Tipos de ACL compatibles: ACL MAC y ACL IP (estándar o ampliada)

Configuración de 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
```

Verificar PACL

Recupere el IF_ID asociado a la interfaz.

```
<#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
```

Verifique el ID de grupo de clase (ID de CG) enlazado al 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
```

Información de ACL asociada a la ID de 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)
```

Información de política sobre el ID de CG, así como qué interfaces utilizan el ID de CG.

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

Confirme que PACL funciona.

> **Nota:** Al introducir el show ip access-lists privileged EXEC , el conteo de coincidencias mostrado no tiene en cuenta los paquetes que tienen acceso controlado en el hardware. Utilice el comando show platform software fed switch {*switch_num*|active|standby}acl counters hardware privilegedEXEC para obtener algunas estadísticas básicas de ACL de hardware para paquetes conmutados y enrutados.

<#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...>
```

Situación hipotética 2. PACL (MAC ACL)

Las PACL se asignan a una interfaz de capa 2.

- Límite de seguridad: puertos o VLAN
- Adjunto: interfaz de capa 2
- Dirección: entrada o salida (de uno en uno)
- Tipos de ACL compatibles: ACL MAC y ACL IP (estándar o ampliada)

Configuración de PACL con MAC ACL

```
<#root>
9500H#
show run | sec mac access-list

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


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


9500H#
show access-lists MAC-TEST

Extended MAC access list MAC-TEST
    permit host 0001.aaaa.aaaa any
9500H#
```

```
show running-config interface twentyFiveGigE 1/0/1


Building configuration...

interface TwentyFiveGigE1/0/1
switchport access vlan 10
switchport mode access
mac access-group MAC-TEST in                <-- Applied MACL to layer 2 interface
```

Verificar PACL

Recupere el IF_ID asociado a la interfaz.

```
<#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
```

Verifique el ID de grupo de clase (ID de CG) enlazado al 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
```

Información de ACL asociada a la ID de 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

Información de política sobre el ID de CG, así como qué interfaces utilizan el ID de CG.

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

Confirme que PACL funciona:

- La MACL sólo permite la dirección de origen 0001.aaaa.aaaa.
- Dado que se trata de una ACL MAC, se descarta un paquete ARP que no es de IP y, por lo tanto, el ping falla.

```
<#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...>

Situación hipotética 3. RACL

RACL se asigna a una interfaz de Capa 3 como una interfaz SVI o una interfaz ruteada.

- Límite de seguridad: diferentes subredes
- Adjunto: interfaz de capa 3
- Dirección: entrada o salida
- Tipos de ACL compatibles: ACL IP (estándar o ampliada)

Configurar 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
```

Verificar RACL

Recupere el IF_ID asociado a la interfaz.

```
<#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
```

Verifique el ID de grupo de clase (ID de CG) enlazado al 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

Información de ACL asociada a la ID de 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)

Información de política sobre el ID de CG, así como qué interfaces utilizan el ID de CG.

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

Confirme que RACL funciona.

> **Nota:** Al introducir el show ip access-lists privileged EXEC , el conteo de coincidencias mostrado no tiene en cuenta los paquetes que tienen acceso controlado en el hardware. Utilice el switch show platform software fed{*switch_num*|active|standby}*acl counters hardware*comando EXEC privilegiado para obtener algunas estadísticas básicas de ACL de hardware para paquetes conmutados y enrutados.

<#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...>
```

Situación hipotética 4. VACL

Las VACL se asignan a una VLAN de Capa 2.

- Límite de seguridad: dentro de una VLAN o a través de ella
- Archivo adjunto: VLAN/VLAN Map
- Dirección: tanto entrada como salida a la vez
- Tipos de ACL compatibles: ACL MAC y ACL IP (estándar o ampliada)

Configuración de 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
```

Verificar VACL

Recupere el IF_ID asociado a la interfaz.

```
<#root>
9500H#
```

show platform software fed active ifm interfaces vlan

Interface

IF_ID

State

Vlan10 0x00420010

READY

Verifique el ID de grupo de clase (ID de CG) enlazado al 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
```

Información de ACL asociada a la ID del grupo CG.

Hay dos ACL utilizadas en la misma política VACL denominada, agrupadas en este grupo de 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

Información de política sobre el ID de CG, así como qué interfaces utilizan el ID de CG.

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

Confirme que VACL funciona.

- La resolución de problemas es el mismo escenario que las secciones PACL y RACl. Consulte estas secciones para obtener detalles sobre la prueba de ping.
- Ping de 10.1.1.3 a 10.1.1.2 denegado por la política ACL aplicada.
- Verifique el 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...>
```

Situación hipotética 5. ACL de grupo/cliente (DACL)

Las ACL de grupo/cliente se aplican dinámicamente a un grupo de usuarios o cliente en función de su identidad. A veces también se denominan DACL.

- Límite de seguridad: Cliente (nivel de interfaz de cliente)
- Adjunto: por interfaz de cliente
- Dirección: solo entrada
- Tipos de ACL compatibles: ACL MAC y ACL IP (estándar o ampliada)

Configuración de 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
```

Verificar GACL

ID de CG de grupo enlazado al 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
```

Información de ACL asociada con el ID de GC del grupo.

```
<#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
```

Situación hipotética 6. Registro ACL

El software del dispositivo puede proporcionar mensajes syslog sobre los paquetes permitidos o denegados por una lista de acceso IP estándar. Cualquier paquete que coincida con la ACL hace que se envíe un mensaje de registro informativo sobre el paquete a la consola. El nivel de mensajes registrados en la consola es controlado por ellogging consolecomandos que controlan los mensajes de Syslog.

- Los mensajes de registro de ACL no son compatibles con las ACL utilizadas con Unicast Reverse Path Forwarding (uRPF). Sólo es compatible con RACL.

- El registro ACL en la dirección de salida no es compatible con los paquetes que se generan desde el plano de control del dispositivo.

- El ruteo se realiza en el hardware y en el software de registro, por lo que si una gran cantidad de paquetes coinciden con una ACE permit o deny que contiene una palabra clave de registro, el software no puede coincidir con la velocidad de procesamiento del hardware y no se pueden registrar todos los paquetes.
- El primer paquete que acciona la ACL provoca un mensaje de registro de inmediato, y los paquetes subsiguientes se recopilan en intervalos de 5 minutos antes de que aparezcan o se registren. El mensaje de registro incluye el número de la lista de acceso, si el paquete fue permitido o denegado, la dirección IP de origen del paquete y el número de paquetes de ese origen permitidos o denegados en el intervalo de 5 minutos anterior.
- Consulte la Guía de Configuración de Seguridad adecuada, Cisco IOS XE, como se indica en la sección Información Relacionada para obtener detalles completos sobre el comportamiento y las restricciones del registro de ACL.

Ejemplo de registro PACL:

Este ejemplo muestra un caso negativo, donde el tipo de ACL y la palabra clave log no funcionan juntos.

```
<#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
```

Ejemplo de Log RACL (Denegar):

```
<#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
```

Ejemplo de Log RACL (Permit):
Cuando se utiliza una sentencia de registro para una sentencia permit, los aciertos del contador de software muestran el doble del número de paquetes enviados.

```
<#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)
```

Troubleshoot

Estadísticas de ACL

Al resolver un problema de ACL, es esencial entender cómo y dónde el dispositivo mide las estadísticas de ACL.

- Las estadísticas de ACL se recopilan en un nivel agregado, no por nivel ACE.
- El hardware no tiene la capacidad de permitir por ACE o por estadísticas de ACL.
- Se recopilan estadísticas tales como Denegación, Registro y paquetes reenviados de CPU.
- Las estadísticas de los paquetes MAC, IPv4 e IPv6 se recopilan por separado.
- show platform software fed switch active acl counters hardware se puede utilizar para mostrar estadísticas agregadas.

Borrado de Estadísticas ACL

Cuando se resuelve un problema de ACL, puede ser útil borrar los diversos contadores de ACL para obtener nuevos recuentos de línea de base.

- Estos comandos le permiten borrar las estadísticas del contador ACL de software y hardware.
- Cuando se resuelven los eventos de coincidencia/acierto de ACL, se recomienda borrar la ACL relevante para las coincidencias de línea base que son recientes o relevantes.

<#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)
```

¿Qué sucede cuando se agota el TCAM de ACL?

- Las ACL siempre se aplican en el TCAM de hardware. Si TCAM ya está siendo utilizado por ACL previamente configuradas, las nuevas ACL no obtienen los recursos de ACL necesarios para programar.

- Si se agrega una ACL después de agotar TCAM, se descartan todos los paquetes para la interfaz a la que está conectada.

- La acción de mantener una ACL en el software se denomina **Descarga**.
- Cuando los recursos están disponibles, el switch automáticamente intenta programar las ACL en el hardware. Si es exitoso, las ACL se envían al hardware y los paquetes comienzan a reenviarse.
- La acción de programar una ACL controlada por software en TCAM se denomina **Recarga**.

- PACL, VACL, RACL y GACL pueden descargarse/recargarse independientemente entre sí.

Agotamiento de ACL TCAM

- La interfaz a la que se aplica la ACL recién agregada comienza a descartar paquetes hasta que los recursos de hardware estén disponibles.
- Los clientes GACL se colocan en el estado UnAuth.

Agotamiento de VCU

- Una vez superado el límite de L4OP o fuera de las VCU, el software realiza la expansión de ACL y crea nuevas entradas ACE para realizar una acción equivalente sin utilizar las VCU.
- Una vez que esto sucede, TCAM puede agotarse a partir de estas entradas agregadas.

Errores de Syslog ACL

Si se queda sin un recurso de ACL de seguridad determinado, el sistema genera mensajes SYSLOG (los valores pueden variar según la interfaz, la VLAN, la etiqueta, etc.).

mensaje de registro de ACL	Definición	Acción de recuperación
%ACL_ERRMSG-4-UNLOADED: Fuente del switch 1: la entrada <ACL> en la interfaz <interface> no está programada en el hardware y el tráfico se descarta.	ACL descargada (en el software)	Investigue la escala TCAM. Si está fuera de escala, rediseñe las ACL.
%ACL_ERRMSG-6-REMOVED: 1 feed: La configuración descargada para la entrada <ACL> en la interfaz <interface> se ha eliminado para la etiqueta <label>asic<number>.	La configuración de ACL descargada se elimina de la interfaz	La ACL ya se ha eliminado, no hay ninguna acción que realizar
%ACL_ERRMSG-6-RELOADED: 1 feed: La entrada <ACL> en la interfaz <interface> se ha cargado ahora en el hardware para la etiqueta <label> en asic<number>.	ACL está ahora instalado en el hardware	El problema con ACL ahora está resuelto en el hardware, no hay ninguna acción que tomar

%ACL_ERRMSG-3-ERROR: 1 feed: La configuración de entrada <ACL> IP ACL <NAME> no se aplica en <interface> en el orden de enlace <number>.	Otros tipos de error de ACL (como el error de instalación de ACL dot1x)	Se admite la confirmación de la configuración de ACL y TCAM no está fuera de escala
%ACL_ERRMSG-6-GACL_INFO: Switch 1 R0/0: feed: El registro no es compatible con GACL.	GACL tiene una opción de registro configurada	GACL no admite registros. Elimine las sentencias de registro de GACL.
%ACL_ERRMSG-6-PACL_INFO: Switch 1 R0/0: feed: No se admite el registro para PACL.	PACL tiene una opción de registro configurada	PACL no admite registros. Elimine las sentencias de registro de PACL.
%ACL_ERRMSG-3-ERROR: Switch 1 R0/0: feed: Input IPv4 Group ACL implicit_deny:<name>: la configuración no se aplica en el cliente MAC 0000.0000.0000.	(dot1x) La ACL no se puede aplicar en el puerto de destino	Se admite la confirmación de la configuración de ACL y TCAM no está fuera de escala

Escenarios sin recursos y acciones de recuperación

Escenario 1. Enlace de ACL	**Acción de recuperación**
• ACL se crea y se aplica a una interfaz o VLAN. • El enlace falla debido a condiciones de 'sin recursos', como agotamiento de TCAM. • No se pueden programar ACE dentro de la ACL en TCAM. ACL permanece en el estado **UNLOADED**. • En el estado **UNLOADED**, todo el tráfico (incluidos los paquetes de control) cae en la interfaz hasta que se soluciona el problema.	Rediseñe la ACL para reducir el uso de TCAM.
Situación hipotética 2. Edición de ACL	**Acción de recuperación**
• Se crea una ACL y se aplica a una interfaz, y se agregan más entradas ACE a esta ACL mientras se aplica a las interfaces. • Si TCAM no tiene recursos, la operación de edición falla. • No se pueden programar ACE dentro de la ACL en TCAM. ACL permanece en el estado **UNLOADED**. • En el estado **UNLOADED**, todo el tráfico (incluidos los paquetes de control) se descarta en la interfaz hasta que se soluciona el problema.	Rediseñe la ACL para reducir el uso de TCAM.

• Las entradas de ACL existentes también fallan en el estado **UNLOADED** hasta que esto se corrige.	
Situación hipotética 3. Reenlace de ACL	**Acción de recuperación**
• El reenlace de ACL es la acción de conectar una ACL a una interfaz y, a continuación, conectar otra ACL a la misma interfaz sin desconectar la primera ACL. • La primera ACL se crea y se adjunta correctamente. • Se crea una ACL más grande con un nombre diferente y el mismo protocolo (IPv4/IPv6) y se conecta a la misma interfaz. • El dispositivo desconecta la primera ACL correctamente e intenta conectar la nueva ACL a esta interfaz. • Si TCAM no tiene recursos, la operación de reenlace falla. • No se pueden programar ACE dentro de la ACL en TCAM. ACL permanece en el estado **UNLOADED**. • En el estado **UNLOADED**, todo el tráfico (incluidos los paquetes de control) cae en la interfaz hasta que se soluciona el problema.	Rediseñe la ACL para reducir el uso de TCAM.
Situación hipotética 4. Enlazar ACL vacía (nula)	**Acción de recuperación**
• Una ACL que no tiene entradas ACE se crea y se asocia a una interfaz. • El sistema crea esta ACL internamente con un permiso 'any ACE' y la conecta a la interfaz en el hardware (todo el tráfico está permitido en este estado). • A continuación, las entradas ACE se agregan a la ACL con el mismo nombre o número. El sistema programa TCAM a medida que se agrega cada ACE. • Si TCAM se queda sin recursos al agregar entradas ACE, ACL se mueve al estado **UNLOADED**. • En el estado **UNLOADED**, todo el tráfico (incluidos los paquetes de control) cae en la interfaz hasta que se soluciona el problema. • Las entradas de ACL existentes también fallan en el estado **UNLOADED** hasta que esto se corrige.	Rediseñe la ACL para reducir el uso de TCAM.

Verificar la escalabilidad ACL

Esta sección trata sobre los comandos para determinar la escala ACL y la utilización TCAM.

Resumen de la lista de acceso FMAN:

Identifique las ACL configuradas y el recuento total de ACE por 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 de 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
```

Uso de TCAM (17.x):

El comando de uso TCAM tiene diferencias significativas entre los trenes 16.x y 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

  0

        7168       18    0.25%       18         0       0         0
 Security ACL Non Ipv4   TCAM        0        8192       27    0.33%        0       22       0         5

<...snip...>

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

Uso de TCAM (16.x):

El comando de uso TCAM tiene diferencias significativas entre los trenes 16.x y 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...>
```

Plantilla SDM personalizada (reasignación TCAM)

Con Cisco IOS XE Bengaluru 17.4.1, puede configurar una plantilla de SDM personalizada para las funciones de ACL mediante el sdm prefer custom aclcomando.

Los detalles sobre cómo configurar y verificar esta función se encuentran en la Guía de Configuración de Administración del Sistema, Cisco IOS XE Bengaluru 17.4.x (Switches Catalyst 9500).

En esta sección se describen algunos aspectos básicos de la configuración y la verificación.

Verificar la plantilla SDM actual:

```
<#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
```

Modificar la plantilla SDM actual:

- 9500H(config)#**SDM prefer custom ACL**
  9500H(config-sdm-acl)#**acl-ingress 26 priority 1 <â€” apply new 26K value. (prioridad descrita en la guía de configuración)**
  9500H(config-sdm-acl)#**acl-egress 20 priority 2**
  9500H(config-sdm-acl)#**salir**
  Uso show sdm prefer custom para ver los valores propuestos y sdm prefer custom commit para aplicar 'ver los cambios' a través de esta CLI.
- Verifique los cambios en el perfil de SDM.
- 9500H#**show sdm prefer custom**

Visualización de la información de plantilla de SDM:

Esta es la plantilla personalizada con sus detalles.
Entradas de control de acceso de seguridad de entrada*: **12288 (actual) - 26624 (propuesta) <â€” Uso actual y propuesto (26 000 propuestas)**
Entradas de control de acceso de seguridad de salida*: **15360 (actual) - 20480 (propuesta)**

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

ENTRADA DE USUARIO DE FUNCIÓN ACL
Valores de entrada de usuario

==========

PRIORIDAD DE NOMBRE DE FUNCIÓN **ESCALAR**

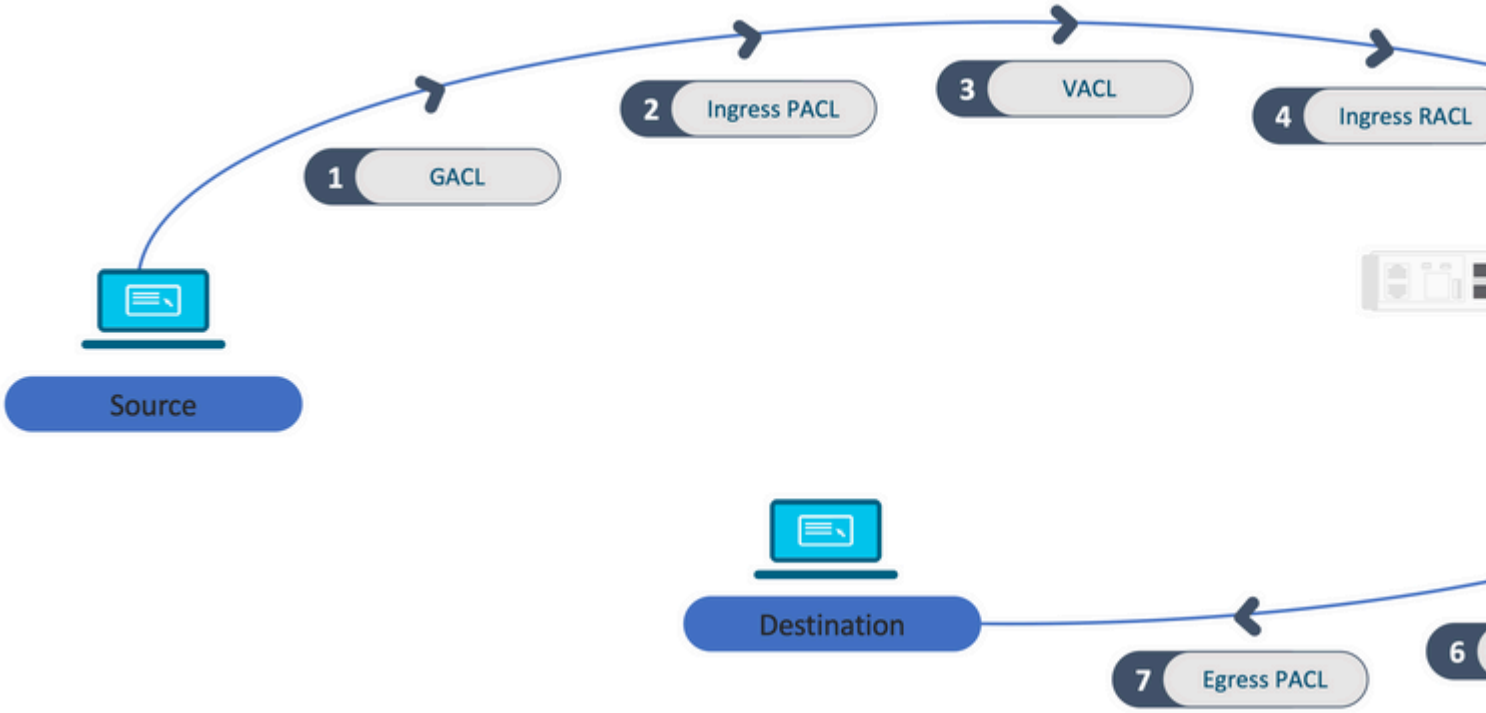
Entradas de control de acceso de seguridad de entrada: **1 26*1024 <â€” Modificado por la entrada del usuario a 26 x 1024 (26 K)**
Entradas de control de acceso de seguridad de salida: **2 20*1024 <â€” Modificado por la entrada del usuario a 20 x 1024 (20 000)**

- Aplicar cambios al perfil de SDM.
- 9500H(config)#**sdm prefer custom commit**
  Los cambios en las preferencias de SDM en ejecución se almacenan y surten efecto en la próxima recarga. **<â€” Una vez recargado, el TCAM de ACL se asigna a un valor personalizado.**

Lectura adicional:

Orden de procesamiento de ACL:

Las ACL se procesan en este orden de origen a destino.



ACL programadas en una pila:

- Las ACL que no están basadas en puertos (por ejemplo, VACL, RACL) se aplican al tráfico en cualquier switch y se programan en todos los switches de la pila.
- Las ACL basadas en puerto se aplican solamente al tráfico en un puerto y se programan solamente en el switch que posee la interfaz.
- Las ACL son programadas por el switch activo y posteriormente se aplican a los switches miembros.
- Las mismas reglas se aplican a otras opciones de redundancia, como ISSU/SVL.

Expansión de ACL:

- La expansión de ACL se produce cuando el dispositivo se queda sin L4OPs, Lables o VCUs. El dispositivo debe crear múltiples ACE equivalentes para lograr la misma lógica y para agotar rápidamente TCAM.
- **### Los L4OP están a escala y se crea esta ACL ##**
  9500H(config)#**ip access-list extended TEST**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any gt 150 <â€” coincide con los puertos 151 y superiores**

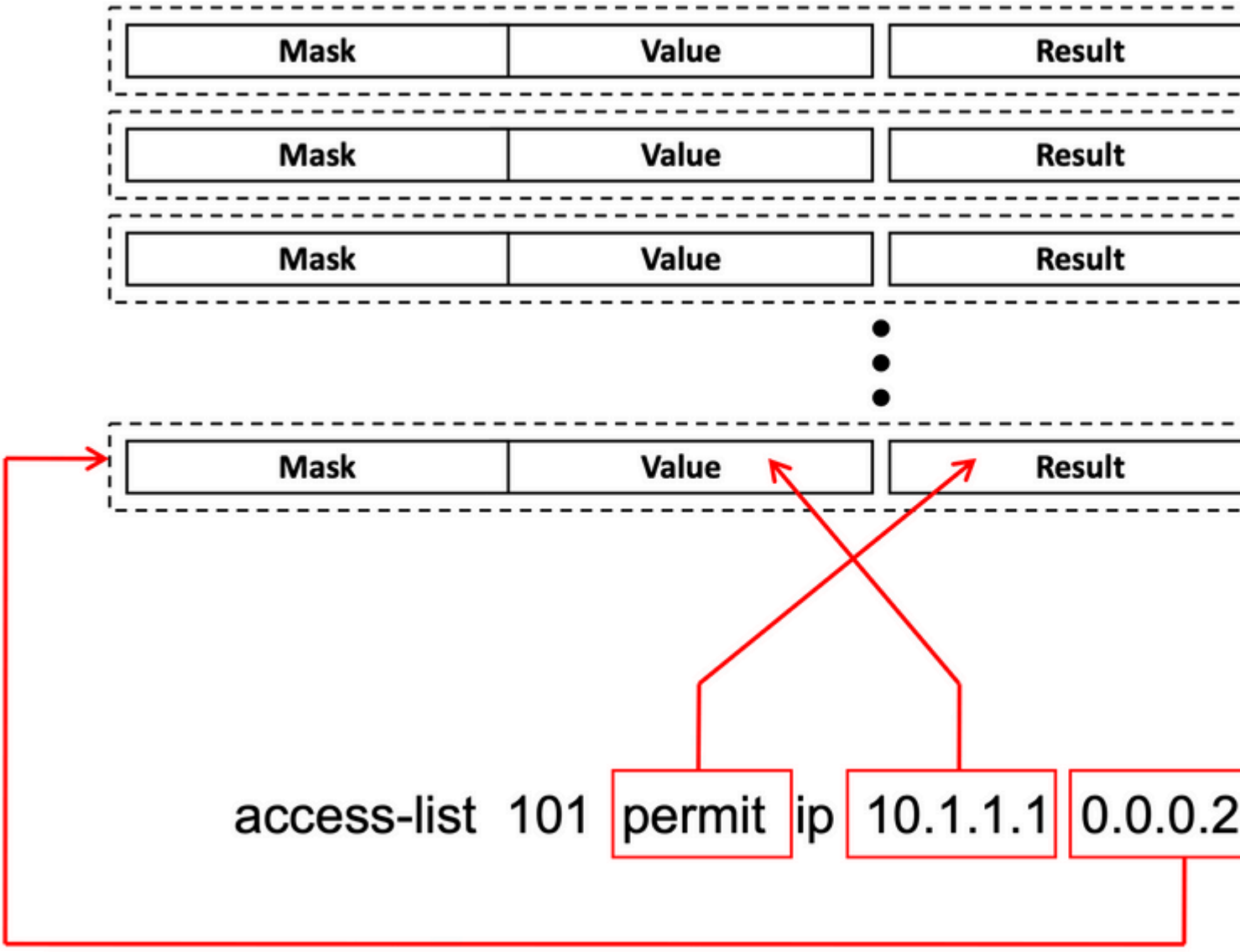
  ### Debe expandirse en varias ACE que no utilicen un L4OP ###
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 151**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 152**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 153**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 154**
  ...y más....

Consumo de TCAM y uso compartido de etiquetas:

- Una etiqueta hace referencia a cada política ACL internamente.
- Cuando se aplica una política de ACL (ACL de seguridad como GACL, PACL, VACL, RACL) a varias interfaces o VLAN, utiliza la misma etiqueta.
- La ACL de entrada/salida utiliza espacios de etiqueta diferentes.
- IPv4, IPv6 y MAC ACL utilizan otros espacios de etiquetas.
- La misma PACL se aplica a la entrada de la interfaz A y a la salida de la interfaz A. Hay dos instancias del PACL en el TCAM, cada una con una etiqueta única para Ingreso y Egreso.
- Si el mismo PACL con un L4OP se aplica a múltiples interfaces de ingreso que existen en cada núcleo, hay dos instancias del mismo PACL programadas en TCAM, una por cada núcleo.

Descripción de VMR:

Una ACE se programa internamente en TCAM como un 'VMR', también conocido como valor, máscara, resultado. Cada entrada ACE puede consumir VMR y VCU.



Escalabilidad de ACL:

Los recursos de ACL de seguridad están dedicados a las ACL de seguridad. No se comparten con otras funciones.

Recursos TCAM de ACL	Cisco Catalyst 9600	Cisco Catalyst 9500	Cisco Catalyst 9400	Cisco Catalyst 9300	Cisco Catalyst 9200				
Entradas IPv4	Entrada: 12000*	Egress: 15000*	C9500: 18000*	C9500 de alto rendimiento Entrada: 12000* Salida: 15000*	18000*	C9300: 5000	C9300B: 18000	C9300X:8000	1000

Entradas IPv6	La mitad de las entradas de IPv4	La mitad de las entradas de IPv4		La mitad de las entradas de IPv4	La mitad de las entradas de IPv4			La mita de la entra de IP
Un tipo de entradas de ACL IPv4 no puede exceder	12000	C9500: 18000	Alto rendimiento de C9500: 15000	18000	C9300: 5000	C9300B: 18000	C9300X: 8000	1000
Un tipo de entradas de ACL IPv6 no puede exceder	6000	C9500: 9000	Alto rendimiento de C9500: 7500	9000	2500/9000/4000			500
L4OPs/Etiqueta	8	8		8	8			8
VCU de entrada	192	192		192	192			192
VCU de salida	96	96		96	96			96

Información Relacionada

- Guía de configuración de seguridad, Cisco IOS XE Amsterdam 17.3.x (switches Catalyst 9200)
- Guía de configuración de seguridad, Cisco IOS XE Amsterdam 17.3.x (switches Catalyst 9300)
- Guía de configuración de seguridad, Cisco IOS XE Amsterdam 17.3.x (switches Catalyst 9400)
- Guía de configuración de seguridad, Cisco IOS XE Amsterdam 17.3.x (switches Catalyst 9500)
- Guía de configuración de seguridad, Cisco IOS XE Amsterdam 17.3.x (switches Catalyst 9600)
- Guía de configuración de administración del sistema, Cisco IOS XE Bengaluru 17.4.x (switches Catalyst 9500)
- Asistencia técnica y descargas de Cisco

Comandos Debug y Trace

Núm	Comando	Observación
1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	Vuelque los contadores de excepciones en el ASIC #N.
2	show platform software fed [switch] active acl	Este comando imprime la información sobre todas las ACL configuradas en el cuadro junto con la información de la

		interfaz y la política.
3	show platform software fed [switch] active acl policy 18	Este comando imprime sólo la información sobre la directiva 18. Puede obtener este ID de política del comando 2.
4	show platform software fed [switch] active acl interface intftype pacl	Este comando imprime la información sobre la ACL basada en el tipo de interfaz (pacl/vacl/racl/gacl/sgacl y así sucesivamente).
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Este comando imprime la información sobre la ACL basada en el tipo de interfaz (pacl/vacl/racl/gacl/sgacl, etc.) y también filtra en función del protocolo (ipv4/ipv6/mac, etc.).
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Este comando imprime la información sobre las interfaces.
7	show platform software fed [switch] active acl interface 0x9	Este comando imprime la información corta de ACL aplicada en la interfaz, basada en el IF-ID (comando de 6).
8	show platform software fed [switch] active acl definition	Este comando imprime la información sobre las ACL configuradas en el cuadro y cuya presencia está en el CGD.
9	show platform software fed [switch] active acl iifid 0x9	Este comando imprime la información detallada de ACL aplicada en la interfaz, basada en el IF-ID.
10	show platform software fed [switch] active acl usage	Este comando imprime el número de VMR que utiliza cada ACL en función del tipo de función.
11	show platform software fed [switch] active acl policy intftype pacl vcu	Este comando le proporciona la información de política y también la información de VCU basada en el tipo de interfaz (pacl/vacl/racl/gacl/sgacl y así sucesivamente).
12	show platform software fed [switch] active acl policy intftype pacl cam	Este comando le brinda la información y los detalles de la política sobre los VMR en el CAM, según el tipo de interfaz (pacl/valc/racl/gacl/sgacl y así sucesivamente).
13	show platform software interface [switch] [active] R0 brief	Este comando le da detalles acerca de la interfaz en el cuadro.
14	show platform software fed [switch] active port if_id 9	Este comando imprime los detalles sobre el puerto basándose en el IIF-ID.

15	show platform software fed [switch] active vlan 30	Este comando imprime los detalles sobre la VLAN 30.
16	show platform software fed [switch] active acl cam asic 0	Este comando imprime la cámara ACL completa en ASIC 0 que se está utilizando.
17	show platform software fed [switch] active acl counters hardware	Este comando imprime todos los contadores ACL del hardware.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	Imprimiendo las entradas para la sección PBR, puede dar diferentes secciones como ACL y CPP en lugar de PBR.
19	show platform software fed [switch] active punt cpuq [1|2|3 â€¦]	Para verificar la actividad en una de las colas de CPU, también tiene opciones para borrar las estadísticas de cola para la depuración.
20	show platform software fed [switch] active ifm mappings gpn	Imprimir la asignación de interfaz con el ID de interfaz y GPN
21	show platform software fed [switch active ifm if-id	Imprima la información sobre la configuración de la interfaz y la afinidad con el ASIC. Este comando es útil para verificar en qué interfaz están ASIC y CORE.
22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error â€¦]	Establecer el seguimiento de una característica específica en FED.
23	request platform software trace rotate all	Borrando el búfer de seguimiento.
24	show platform software trace message fed [switch] active	Imprimiendo el búfer de seguimiento para FED.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error â€¦]	Habilitación de los seguimientos para FMAN.
26	show platform software trace message forwarding-manager [switch] [active] f0	Imprimiendo el búfer de seguimiento para FMAN.
27	debug platform software infrastructure punt detail	Establezca la depuración en PUNT.
28	debug ip cef packet all input rate 100	La depuración de paquetes CEF está activada.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).