Validar ACLs de segurança nos switches Catalyst 9000

Contents

Introdução

Este documento descreve como verificar e solucionar problemas de ACLs (listas de controle de acesso) nos Catalyst 9000 Series Switches.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware:

- C9200
- C9300
- C9400
- C9500
- C9600

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Observação**: consulte o guia de configuração apropriado para obter os comandos usados para ativar esses recursos em outras plataformas Cisco.

Informações de Apoio

As ACLs filtram o tráfego à medida que ele passa por um roteador ou switch e permitem ou negam pacotes que cruzam interfaces especificadas. Uma ACL é uma coleção sequencial de condições de permissão e negação que se aplicam aos pacotes. Quando um pacote é recebido em uma interface, o switch compara os campos do pacote com as ACLs aplicadas para verificar se o pacote tem as permissões necessárias para ser encaminhado, com base nos critérios especificados nas listas de acesso. Um por um, ele testa os pacotes em relação às condições em uma lista de acesso. A primeira correspondência decide se o switch aceita ou rejeita os pacotes. Como o switch interrompe o teste após a primeira correspondência, a ordem das condições na lista é crítica. Se nenhuma condição corresponder, o switch rejeitará o pacote. Se não houver restrições, o switch encaminhará o pacote; caso contrário, o switch descartará o pacote. O switch pode usar ACLs em todos os pacotes que encaminhar.

Você pode configurar listas de acesso para fornecer segurança básica à sua rede. Se você não configurar as ACLs, todos os pacotes que passarem pelo switch poderão ter permissão para acessar todas as partes da rede. Você pode usar ACLs para controlar quais hosts podem acessar diferentes partes de uma rede ou para decidir que tipos de tráfego são encaminhados ou bloqueados nas interfaces do roteador. Por exemplo, você pode encaminhar tráfego de e-mail, mas não tráfego Telnet.

Terminologia

ACE	Access Control Entry (ACE) - Uma única regra/linha dentro de uma ACL
ACL	Lista de Controle de Acesso (ACL - Access Control List) - Um grupo de ACEs aplicadas a uma porta

DACL	ACL para download (DACL) - Uma ACL enviada dinamicamente através da política de segurança do ISE
PACL	Porta ACL (PACL) - Uma ACL aplicada a uma interface de Camada 2
RACL	ACL roteada (RACL) - uma ACL aplicada a uma interface de Camada 3
VACL	VLAN ACL (VACL) - Uma ACL aplicada a uma VLAN
GACL	ACL de grupo (GACL) - Uma ACL atribuída dinamicamente a um grupo de usuários ou cliente com base em sua identidade
ACL IP	É usado para classificar pacotes IPv4/IPv6. Essas regras contêm vários campos e atributos de pacotes de Camada 3 e Camada 4, incluindo, mas não se limitando a, endereços IPv4 origem e destino, portas origem e destino TCP/UDP, sinalizadores TCP e DSCP, etc.
MACL	MAC Address ACL (MACL) - Usado para classificar pacotes não IP. As regras contêm vários campos e atributos da camada 2, incluindo endereço MAC de origem/destino, tipo de Ethernet e assim por diante.
L4OP	Porta do Operador de Camada 4 (L4OP) - Corresponde à lógica diferente de EQ (Igual a). GT (maior que), LT (menor que), NE (diferente de) e RANGE (de a)
VCU	Unidade de Comparação de Valores (VCU - Value Comparison Unit) - Os L4OPs são convertidos em VCU para realizar a classificação nos cabeçalhos da Camada 4
VMR	Value Mask Result (VMR) - Uma entrada ACE é programada internamente no TCAM como um VMR.
CGD	Class Group Database (CGD) - Onde o FMAN-FP armazena o conteúdo da ACL
Classes	Como as ACEs são identificadas no CGD
CG	Class Group (CG) - Um grupo de classes sobre como as ACLs são identificadas no CGD
CGE	CGE (Class Group Entry - Entrada de grupo de classes) - Uma entrada ACE armazenada em um grupo de classes
FMAN	Forwarding Manager (FMAN) - A camada de programação entre o Cisco IOS® XE e o hardware

FED	Driver do Mecanismo de Encaminhamento (FED) - O componente que programa o hardware do dispositivo

Exemplos de utilização de recursos da ACL

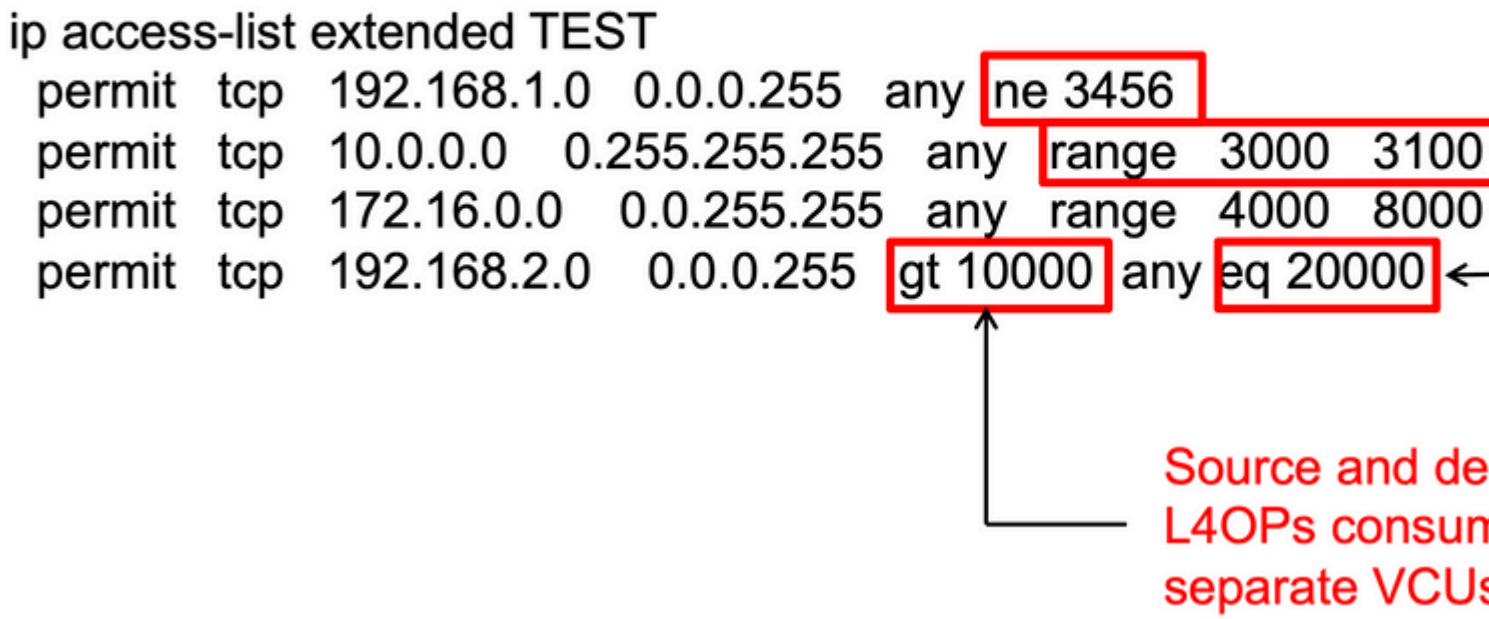
Três exemplos são dados aqui para demonstrar como as ACLs consomem TCAM, L4OPs e VCUs.

Exemplo 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 de TCAM	**L4OP**	**VCUs**
Consumo	5	0	0

Exemplo 2. TCAM/L4OP/VCU IPv4



```
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 de TCAM	L4OP	VCUs
Consumo	4	5	7

Exemplo 3. TCAM/L4OP/VCU IPv6

As ACEs IPv6 usam duas entradas TCAM versus uma para IPv4. Neste exemplo, quatro ACEs consomem oito TCAM em vez de quatro.

<#root>

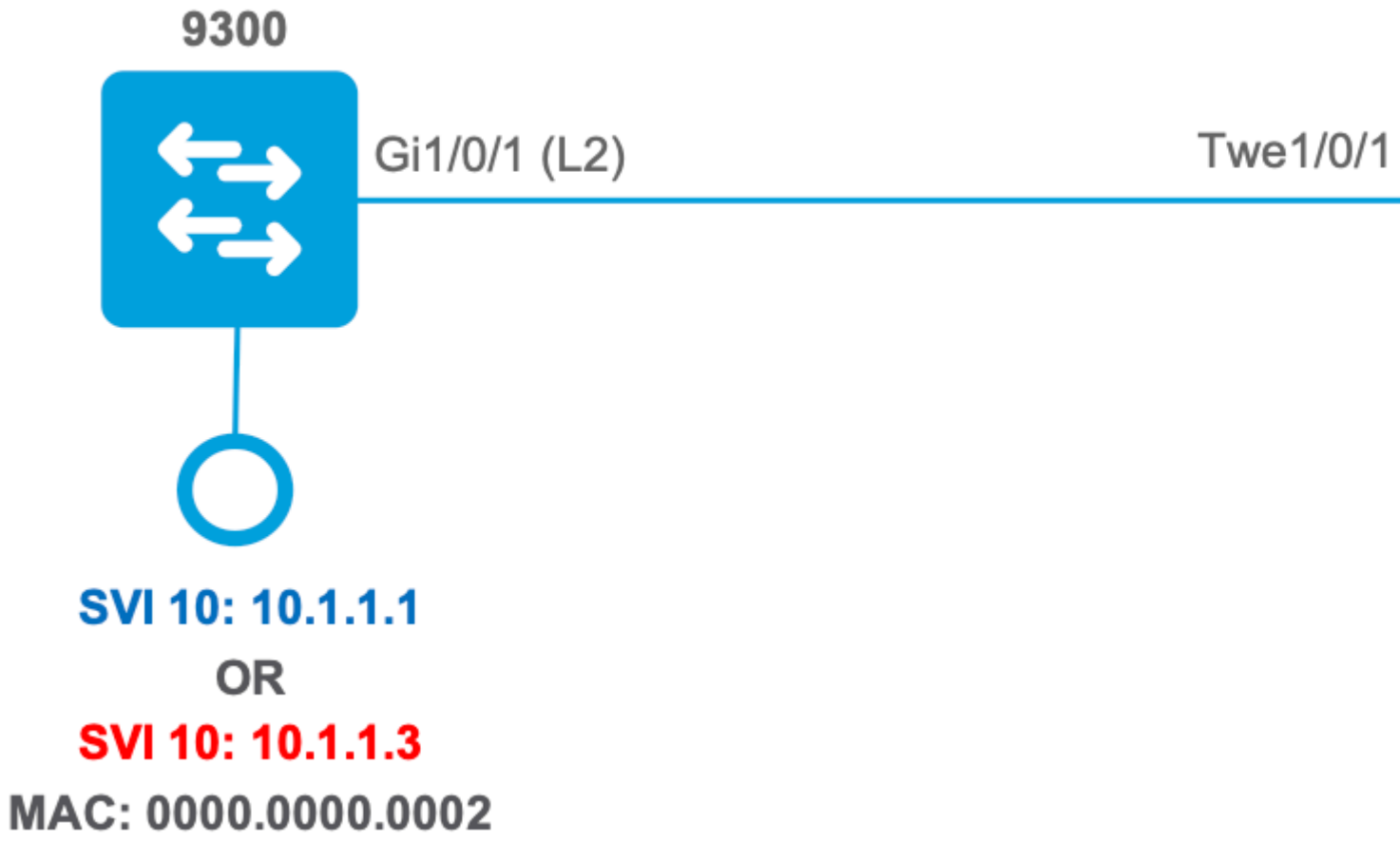
```
ipv6 access-list v6TEST
sequence 10 deny ipv6 any 2001:DB8:C18::/48 fragments
sequence 20 deny ipv6 2001:DB8::/32 any
sequence 30 permit tcp host 2001:DB8:C19:2:1::F host 2001:DB8:C18:2:1::1
eq bgp  <-- One L4OP & VCU


sequence 40 permit tcp host 2001:DB8:C19:2:1::F
eq bgp
 host 2001:DB8:C18:2:1::1
<-- One L4OP & VCU
```

	Entradas de TCAM	L4OP	VCUs

Consumo	8	2	2

Topologia

A SVI da VLAN 10 do 9300 usa um dos dois endereços IP mostrados nesta imagem, com base no fato de um resultado de encaminhamento ou queda ser mostrado nos exemplos.



Configurar e verificar

Esta seção aborda como verificar e solucionar problemas de programação de ACL em software e hardware.

Cenário 1. PACL (ACL IP)

Os PACLs são atribuídos a uma interface de Camada 2.

- Limite de segurança: portas ou VLANs
- Anexo: interface da camada 2
- Direção: entrada ou saída (uma por vez)
- Tipos de ACL suportados: ACL MAC e ACLs IP (padrão ou estendida)

Configurar PACL com 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 o IF_ID associado à interface.

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

Interface
```

```
 IF_ID

               State
--------------------------------------------------------------
TwentyFiveGigE1/0/1


0x00000008

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

Verifique o ID do grupo de classes (CG ID) associado ao 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
```

Informações de ACL associadas à ID do 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)

Informações de política sobre o ID do CG, bem como quais interfaces usam o ID do 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 se o PACL está funcionando.

> **Note**: Quando você digita o comando show ip access-lists privileged EXEC , a contagem de correspondências exibida não leva em conta os pacotes cujo acesso é controlado no hardware. Use o comando EXEC {*switch_num*|*ative*|standby}acl do show platform software fed switch{*switch_num*|*ative*| *standby*}acl counters hardware privileged para obter algumas estatísticas básicas de ACL para pacotes comutados e roteados.

<#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...>
```

Cenário 2. PACL (ACL MAC)

Os PACLs são atribuídos a uma interface de Camada 2.

- Limite de segurança: portas ou VLANs
- Anexo: interface da camada 2
- Direção: entrada ou saída (uma por vez)
- Tipos de ACL suportados: ACL MAC e ACLs IP (padrão ou estendida)

Configurar PACL com 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

Verificar PACL

Recupere o IF_ID associado à interface.

<#root>

9500H#

show platform software fed active ifm interfaces ethernet

Interface

IF_ID

State

TwentyFiveGigE1/0/1

0x00000008

READY

<-- IF_ID value for Tw1/0/1

Verifique o ID do grupo de classes (CG ID) associado ao 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
```

Informações de ACL associadas à ID do 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
```

Informações de política sobre o ID do CG, bem como quais interfaces usam o ID do 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 se o PACL está funcionando:

- A MACL só permite o endereço de origem 0001.aaaa.aaaa.
- Como essa é uma ACL MAC, um pacote ARP não IP é descartado e, portanto, causa a falha do ping.

<#root>

Ping originated from neighbor device with Source MAC 0000.0000.0002

C9300#

ping 10.1.1.2 source vlan 10

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

Success rate is 0 percent (0/5)

C9300#

show ip arp

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

Incomplete

       ARPA

<-- ARP is unable to complete on Source device

Monitor capture configured on Tw 1/0/1 ingress

9500H#

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

9500H#

show monitor cap

Status Information for Capture 1
  Target Type:

Interface: TwentyFiveGigE1/0/1, Direction: IN

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

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

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

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

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

9500H#

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

```
Egress MAC PACL Drop                          (0x0200004c): 0 frames
```

<...snip...>

Cenário 3. RACL

O RACL é atribuído a uma interface de Camada 3, como uma SVI ou uma interface roteada.

- Limite de segurança: sub-redes diferentes
- Anexo: interface da camada 3
- Direção: entrada ou saída
- Tipos de ACL suportados: ACLs IP (padrão ou estendida)

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 o IF_ID associado à interface.

```
<#root>
9500H#
show platform software fed active ifm mappings l3if-le  <-- Retrieve the IF_ID for a Layer 3 SVI type po
Mappings Table
L3IF_LE                   Interface                              IF_ID             Type
-------------------------------------------------------------------------------------------------------
0x00007f8d04983958
Vlan10


0x00000026
        SVI_L3_LE
<-- IF_ID value for SVI 10
```

Verifique o ID do grupo de classes (CG ID) associado ao 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

Informações de ACL associadas à ID do 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)
```

Informações de política sobre o ID do CG, bem como quais interfaces usam o ID do 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 se o RACL está funcionando.

> **Note**: Quando você digita o comando show ip access-lists privileged EXEC , a contagem de correspondências exibida não leva em conta os pacotes cujo acesso é controlado no hardware. Use o hardware dos contadores show platform software fed switch{*switch_num*|*ative*|*standby*}*acl*privilegiado para obter algumas estatísticas básicas de ACL de hardware para pacotes comutados e roteados.

<#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...>
```

Cenário 4. VACL

As VACLs são atribuídas a uma VLAN de Camada 2.

- Limite de segurança: dentro ou através de uma VLAN
- Anexo: Mapa VLAN/VLAN
- Direção: entrada e saída simultaneamente
- Tipos de ACL suportados: ACL MAC e ACLs IP (padrão ou estendida)

Configurar 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 o IF_ID associado à interface.

<#root>

9500H#

show platform software fed active ifm interfaces vlan

Interface

IF_ID

State

Vlan10 0x00420010

READY

Verifique o ID do grupo de classes (CG ID) associado ao 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
```

Informações de ACL associadas à ID do grupo CG.

Há duas ACLs usadas na mesma política de VACL nomeada, agrupadas nesse 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

Informações de política sobre o ID do CG, bem como quais interfaces usam o ID do 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 se a VACL está funcionando.

- A solução de problemas é o mesmo cenário das seções PACL e RACl. Consulte estas seções para obter detalhes sobre o teste de ping.
- Ping de 10.1.1.3 a 10.1.1.2 negado pela política de ACL aplicada.
- Verifique o 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...>
```

Cenário 5. ACL de grupo/cliente (DACL)

As ACLs de grupo/cliente são aplicadas dinamicamente a um grupo de usuários ou cliente com base em sua identidade. Elas também são às vezes chamadas de DACL.

- Limite de segurança: Cliente (nível de interface do cliente)
- Anexo: por interface de cliente
- Direção: somente ingresso
- Tipos de ACL suportados: ACL MAC e ACLs IP (padrão ou estendida)

Configurar 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 do CG do grupo associado ao 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
```

Informações de ACL associadas ao ID de GC do 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
```

Cenário 6. Registro de ACL

O software do dispositivo pode fornecer mensagens de syslog sobre pacotes permitidos ou negados por uma lista de acesso IP padrão. Qualquer pacote que corresponda à ACL faz com que uma mensagem de registro informativa sobre o pacote seja enviada ao console. O nível de mensagens registradas no console é controlado peloconsole de registrocomandos que controlam as mensagens de Syslog.

- As mensagens de log da ACL não são suportadas para ACLs usadas com Unicast Reverse Path Forwarding (uRPF). Ele só é suportado para RACL.

- O log da ACL na direção de saída não é suportado para pacotes gerados a partir do plano de controle do dispositivo.

- O roteamento é feito no hardware e no software de registro, portanto, se um grande número de pacotes corresponder a uma entrada permit ou deny que contenha uma palavra-chave de registro, o software não conseguirá corresponder à taxa de processamento do hardware e nem todos os pacotes poderão ser registrados.
- O primeiro pacote que dispara a ACL causa uma mensagem de registro imediatamente e os pacotes subsequentes são coletados em intervalos de 5 minutos antes de aparecerem ou serem registrados. A mensagem de registro inclui o número da lista de acesso, se o pacote foi permitido ou negado, o endereço IP de origem do pacote e o número de pacotes dessa origem permitidos ou negados no intervalo anterior de 5 minutos.
- Consulte o Guia de configuração de segurança apropriado, Cisco IOS XE, conforme observado na seção Informações relacionadas para obter detalhes completos sobre o comportamento e as restrições

do log da ACL.

Exemplo de registro PACL:

Este exemplo mostra um caso negativo, em que o tipo de ACL e a palavra-chave log não funcionam 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
```

Exemplo de registro RACL (Negar):

```
<#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
```

Exemplo de registro RACL (Permit):
Quando uma instrução log é usada para uma instrução permit, os acertos do contador de software mostram o dobro do número de pacotes 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)
```

Troubleshooting

Estatísticas de ACL

Ao solucionar um problema de ACL, é essencial entender como e onde as estatísticas de ACL são medidas pelo dispositivo.

- As estatísticas da ACL são coletadas em um nível agregado, e não por nível ACE.
- O hardware não pode permitir estatísticas por ACE ou por ACL.
- Estatísticas como pacotes de negação, registro e encaminhamento de CPU são coletadas.
- As estatísticas de pacotes MAC, IPv4 e IPv6 são coletadas separadamente.
- show platform software fed switch active acl counters hardware pode ser usado para exibir estatísticas agregadas.

Limpando estatísticas de ACL

Ao solucionar um problema de ACL, pode ser útil limpar os vários contadores de ACL para obter novas contagens de linha de base.

- Esses comandos permitem limpar as estatísticas do contador de ACL de software e hardware.
- Quando você soluciona problemas de correspondência/acerto de ACL, é recomendável limpar a ACL relevante para as correspondências de linha de base que são recentes ou 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)
```

O que acontece quando a TCAM da ACL é esgotada?

- As ACLs são sempre aplicadas no TCAM de hardware. Se a TCAM já estiver sendo usada por ACLs configuradas anteriormente, as novas ACLs não obterão os recursos de ACL necessários para a programação.

- Se uma ACL for adicionada depois que o TCAM for esgotado, todos os pacotes serão descartados para a interface à qual está conectado.

- A ação de manter uma ACL no software é chamada de **Descarregamento**.
- Quando os recursos ficam disponíveis, o switch tenta programar automaticamente as ACLs no hardware. Se obtiver êxito, as ACLs serão enviadas ao hardware e os pacotes começarão a ser encaminhados.
- A ação de programar uma ACL mantida por software no TCAM é chamada de **Recarregamento**.

- PACL, VACL, RACL e GACL podem ser descarregados/recarregados independentemente um do outro.

Esgotamento de TCAM ACL

- A interface à qual a ACL recém-adicionada é aplicada começa a descartar pacotes até que os recursos de hardware se tornem disponíveis.
- Os clientes GACL são colocados no estado UnAuth.

Esgotamento de VCU

- Uma vez acima do limite de L4OPs ou fora das VCUs, o software executa a expansão da ACL e cria novas entradas ACE para executar uma ação equivalente sem usar VCUs.
- Quando isso acontece, a TCAM pode se esgotar dessas entradas adicionadas.

Erros de Syslog da ACL

Se você ficar sem um recurso de ACL de segurança específico, as mensagens SYSLOG serão geradas pelo sistema (interface, VLAN, rótulo, etc., os valores podem ser diferentes).

Mensagem de log da ACL	Definição	Ação de Recuperação
%ACL_ERRMSG-4-UNLOADED: Switch 1 alimentado: a entrada <ACL> na interface <interface> não está programada no hardware e o tráfego é descartado.	A ACL está descarregada (mantida no software)	Investigue a escala TCAM. Se estiver além da escala, reprojete as ACLs.
%ACL_ERRMSG-6-REMOVED: 1 feed: a configuração descarregada para a Entrada <ACL> na interface <interface> foi removida para o rótulo <label>asic<number>.	A configuração da ACL não carregada é removida da interface	A ACL já foi removida, não há ação a ser tomada
%ACL_ERRMSG-6-RELOADED: 1 alimentado: a	A ACL agora está	O problema com a ACL está agora

entrada <ACL> na interface <interface> foi carregada no hardware para o rótulo <label> no básico<number>.	instalada no hardware	no hardware resolvido, nenhuma ação a ser tomada
%ACL_ERRMSG-3-ERROR: 1 alimentado: a configuração <NAME> da ACL IP de entrada <ACL> não foi aplicada em <interface> na ordem de ligação <number>.	Outros tipos de erro de ACL (como falha de instalação de ACL dot1x)	Confirme se a configuração da ACL é suportada e se o TCAM não está além da escala
%ACL_ERRMSG-6-GACL_INFO: Switch 1 R0/0: fed: não há suporte para registro em log para GACL.	O GACL tem uma opção de log configurada	O GACL não suporta logs. Remova as instruções de log da GACL.
%ACL_ERRMSG-6-PACL_INFO: Switch 1 R0/0: fed: não há suporte para registro em log para PACL.	O PACL tem uma opção de registro configurada	O PACL não suporta logs. Remova as instruções de log do PACL.
%ACL_ERRMSG-3-ERROR: Switch 1 R0/0: fed: Entrada IPv4 Group ACL implicit_deny:<nome>: configuração não aplicada no MAC Cliente 0000.0000.0000.	(dot1x) A ACL não é aplicada na porta de destino	Confirme se a configuração da ACL é suportada e se o TCAM não está além da escala

Cenários sem recursos e ações de recuperação

Cenário 1. Ligação ACL	**Ação de Recuperação**
• A ACL é criada e aplicada a uma interface ou VLAN. • A vinculação falha devido a condições de 'falta de recurso', como esgotamento de TCAM. • Nenhuma ACE dentro da ACL pode ser programada no TCAM. A ACL permanece no estado **UNLOADED**. • No estado **UNLOADED**, todo o tráfego (incluindo pacotes de controle) cai na interface até que o problema seja corrigido.	Recrie a ACL para reduzir a utilização de TCAM.
Cenário 2. Edição de ACL	**Ação de Recuperação**
• Uma ACL é criada e aplicada a uma interface, e mais entradas ACE são adicionadas a essa ACL enquanto são aplicadas à(s) interface(s). • Se o TCAM não tiver recursos, a operação de edição falhará.	Recrie a ACL para reduzir a utilização de TCAM.

• Nenhuma ACE dentro da ACL pode ser programada no TCAM. A ACL permanece no estado **UNLOADED**. • No estado **UNLOADED** todo o tráfego (incluindo pacotes de controle) cai na interface até que o problema seja corrigido. • As entradas ACL existentes também falham no estado **UNLOADED** até que isso seja corrigido.	
Cenário 3. Revinculação de ACL	**Ação de Recuperação**
• A ACL Re-bind é a ação de anexar uma ACL a uma interface e, em seguida, anexar outra ACL à mesma interface sem desanexar a primeira ACL. • A primeira ACL é criada e anexada com êxito. • Uma ACL maior com um nome diferente e o mesmo protocolo (IPv4/IPv6) é criada e conectada à mesma interface. • O dispositivo desanexa a primeira ACL com êxito e tenta anexar a nova ACL a essa interface. • Se o TCAM não tiver recursos, a operação de reassociação falhará. • Nenhuma ACE dentro da ACL pode ser programada no TCAM. A ACL permanece no estado **UNLOADED**. • No estado **UNLOADED**, todo o tráfego (incluindo pacotes de controle) cai na interface até que o problema seja corrigido.	Recrie a ACL para reduzir a utilização de TCAM.
Cenário 4. Vincular ACL vazia (nula)	**Ação de Recuperação**
• Uma ACL sem entradas ACE é criada e anexada a uma interface. • O sistema cria essa ACL internamente com um permit 'any ACE' e a conecta à interface no hardware (todo o tráfego é permitido nesse estado). • As entradas ACE são adicionadas à ACL com o mesmo nome ou número. O sistema programa TCAM conforme cada ACE é adicionada. • Se o TCAM ficar sem recursos ao adicionar entradas ACE, a ACL é movida para o estado **UNLOADED**. • No estado **UNLOADED**, todo o tráfego (incluindo pacotes de controle) cai na interface até que o problema seja corrigido. • As entradas ACL existentes também falham no estado **UNLOADED** até que isso seja corrigido.	Recrie a ACL para reduzir a utilização de TCAM.

Verifique a escala da ACL

Esta seção aborda os comandos para determinar a escala da ACL e a utilização da TCAM.

Resumo da lista de acesso FMAN:

Identificar ACLs configuradas e a contagem 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 da 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):

O comando de uso da TCAM tem diferenças significativas entre as trilhas 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

  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):

O comando de uso da TCAM tem diferenças significativas entre as trilhas 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...>
```

Modelo de SDM personalizado (realocação de TCAM)

Usando o Cisco IOS XE Bengaluru 17.4.1, você pode configurar um modelo SDM personalizado para recursos ACL usando o comando sdm prefer custom aclcomando.

Detalhes sobre como configurar e verificar esse recurso são abordados no Guia de Configuração de Gerenciamento do Sistema, Cisco IOS XE Bengaluru 17.4.x (Catalyst 9500 Switches).

Algumas configurações e verificações básicas são observadas nesta seção.

Verifique o modelo de SDM atual:

<#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
```

Modifique o modelo de SDM atual:

- 9500H(config)#**sdm prefer custom acl**
  9500H(config-sdm-acl)#**acl-ingress 26 priority 1 <â€” aplique o novo valor de 26K. (prioridade discutida no guia de configuração)**
  9500H(config-sdm-acl)#**acl-egress 20 priority 2**
  9500H(config-sdm-acl)#**sair**
  Uso show sdm prefer custom para ver os valores propostos e sdm prefer custom commit para aplicar 'exibir as alterações' através desta CLI.
- Verifique as alterações no perfil SDM.
- Nº 9500H**show sdm prefer custom**

Mostrando Informações do Modelo de SDM:

Este é o modelo personalizado com seus detalhes.
Entradas de controle de acesso de segurança de ingresso*: **12288 (atual) - 26624 (proposto) <â€” Uso atual e proposto (26.000 proposto)**
Entradas de controle de acesso de segurança de saída*: **15360 (atual) - 20480 (proposta)**

Nº 9500H**show sdm prefer custom user-input**

ENTRADA DO USUÁRIO DO RECURSO ACL
Valores de entrada do usuário
==========

PRIORIDADE DO NOME DO RECURSO **ESCALA**

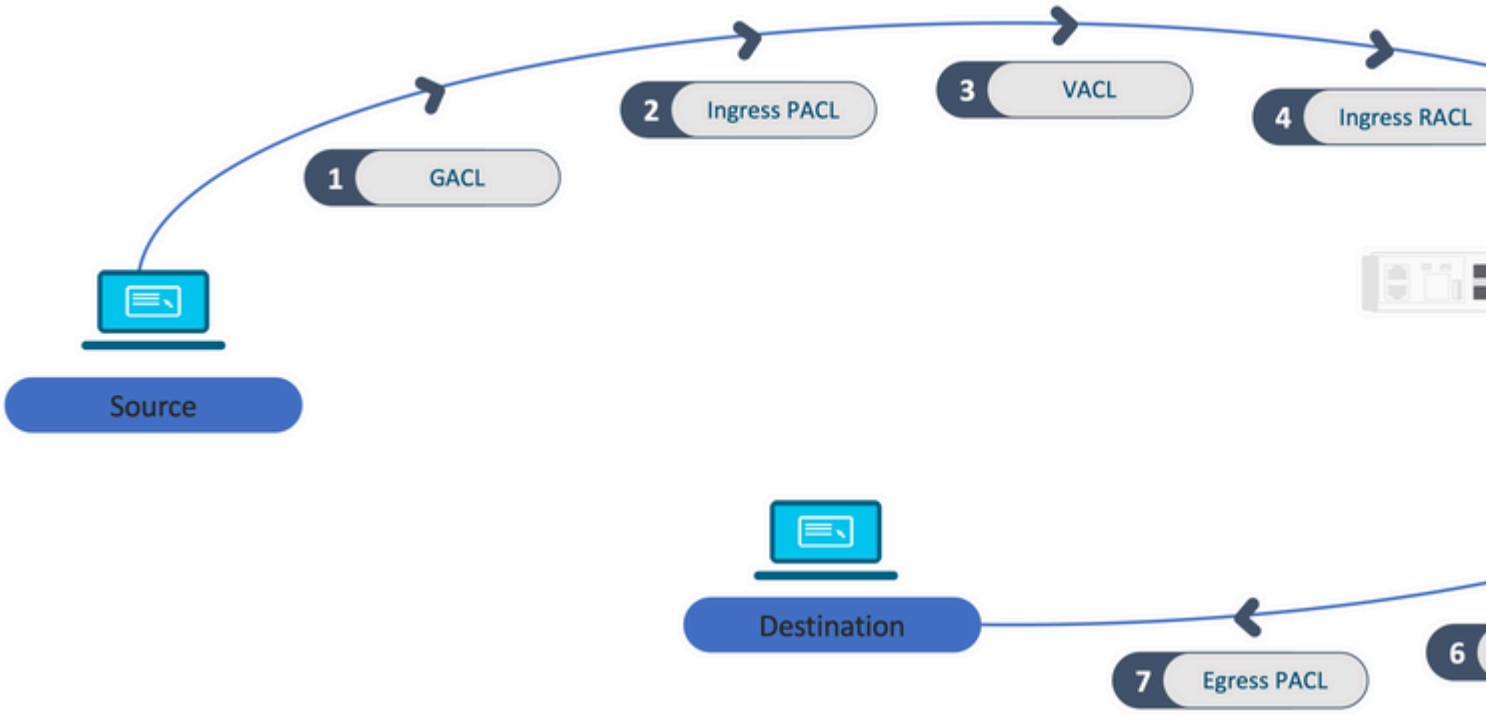
Entradas de Controle de Acesso de Segurança de Ingresso: **1 26*1024 <â€" Modificado pela entrada do usuário para 26 x 1024 (26K)**
Entradas de Controle de Acesso de Segurança de Saída: **2 20*1024 <â€" Modificado pela entrada do usuário para 20 x 1024 (20K)**

- Aplique as alterações ao perfil SDM.
- 9500H(config)#**sdm prefer custom commit**
  As alterações nas preferências de SDM em execução são armazenadas e entram em vigor na próxima recarga. **<â€" Depois de recarregada, a TCAM da ACL é alocada para um valor personalizado.**

Leitura adicional:

Ordem de processamento da ACL:

As ACLs são processadas nessa ordem, da origem para o destino.



ACLs programadas em uma pilha:

- As ACLs que não são baseadas em porta (por exemplo, VACL, RACL) são aplicadas ao tráfego em qualquer switch e são programadas em todos os switches da pilha.
- As ACLs baseadas em porta são aplicadas somente ao tráfego em uma porta e são programadas somente no switch que possui a interface.
- As ACLs são programadas pelo switch ativo e aplicadas subsequentemente aos switches membros.
- As mesmas regras se aplicam a outras opções de redundância, como ISSU/SVL.

Expansão da ACL:

- A expansão da ACL acontece quando o dispositivo fica sem L4OPs, Rótulos ou VCUs. O dispositivo deve criar várias ACEs equivalentes para realizar a mesma lógica e para esgotar rapidamente a TCAM.
- **### Os L4OPs estão em escala e esta ACL é criada ##**
  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€” corresponde às portas 151 e superiores**

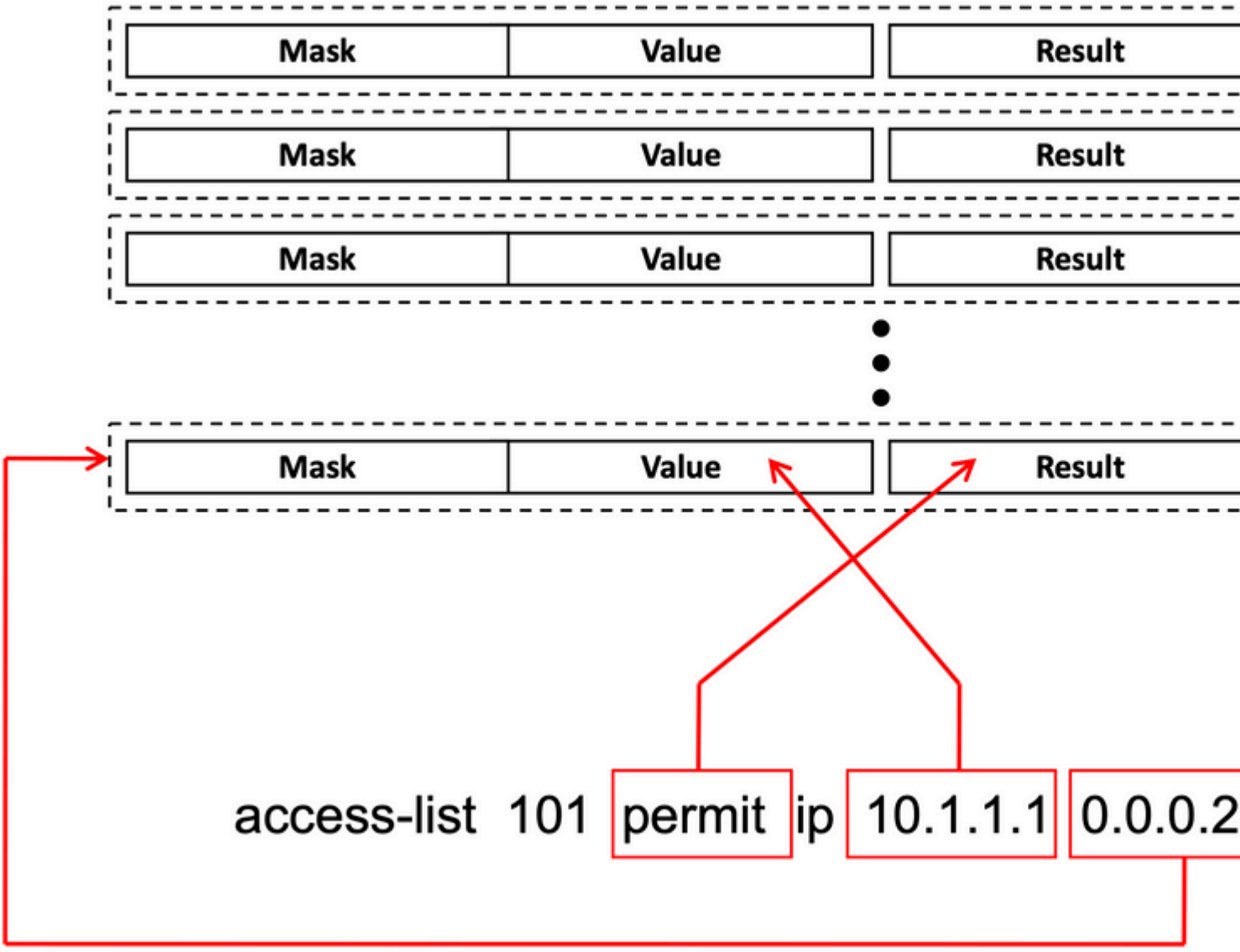
  ### Isso deve ser expandido em várias ACEs que não usam um L4OP ###
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 151**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 152**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 153**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 154**
  ...etc....

Consumo de TCAM e compartilhamento de rótulo:

- Cada política de ACL é referenciada internamente por um rótulo.
- Quando a política de ACL (ACL de segurança como GACL, PACL, VACL, RACL) é aplicada a várias interfaces ou VLAN, ela usa o mesmo rótulo.
- A ACL Ingress/Egress usa espaços de rótulo diferentes.
- IPv4, IPv6 e ACL MAC usam outros espaços de rótulo.
- O mesmo PACL é aplicado à entrada da interface A e à saída da interface A. Há duas instâncias do PACL no TCAM, cada uma com um rótulo exclusivo para Ingress e Egress.
- Se o mesmo PACL com um L4OP for aplicado a várias interfaces de ingresso que existem em cada núcleo, haverá duas instâncias do mesmo PACL programadas no TCAM, uma para cada núcleo.

Descrição do VMR:

Uma ACE é programada internamente no TCAM como um 'VMR' - também conhecido como Valor, Máscara, Resultado. Cada entrada ACE pode consumir VMRs e VCUs.



Escalabilidade da ACL:

Os recursos de ACL de segurança são dedicados às ACLs de segurança. Eles não são compartilhados com outros recursos.

Recursos TCAM ACL	**Cisco Catalyst 9600**	**Cisco Catalyst 9500**	**Cisco Catalyst 9400**	**Cisco Catalyst 9300**	**Cisco Catalyst 9200**				
Entradas IPv4	Entrada: 12000*	Saída: 15000 *	C9500: 18000*	Alto desempenho do C9500 Entrada: 12000* Saída: 15000*	18000 *	C9300: 5000	C9300B: 18000	C9300X:8000	1000

Entradas IPv6	Metade das entradas IPv4	Metade das entradas IPv4		Metade das entradas IPv4	Metade das entradas IPv4			Metad das entrad IPv4
Um tipo de entrada ACL IPv4 não pode exceder	12000	C9500: 18000	Alto desempenho do C9500: 15000	18000	C9300: 5000	C9300B: 18000	C9300X: 8000	1000
Um tipo de entrada ACL IPv6 não pode exceder	6000	C9500: 9000	Alto desempenho do C9500: 7500	9000	2500/9000/4000			500
L4OPs/Rótulo	8	8		8	8			8
VCUs de ingresso	192	192		192	192			192
VCUs de saída	96	96		96	96			96

Informações Relacionadas

- Guia de configuração de segurança, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9200)
- Guia de configuração de segurança, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9300)
- Guia de configuração de segurança, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9400)
- Guia de configuração de segurança, Cisco IOS XE Amsterdam 17.3.x (switches Catalyst 9500)
- Guia de configuração de segurança, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9600)
- Guia de configuração de gerenciamento de sistema, Cisco IOS XE Bengaluru 17.4.x (switches Catalyst 9500)
- Suporte técnico e downloads da Cisco

Comandos debug e trace

Número	Comando	Lembrete
1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	Descarte os contadores de exceção no #N ASIC.
2	show platform software fed [switch] active acl	Esse comando imprime as informações sobre todas as ACLs configuradas na caixa junto com as informações de interface

		e política.
3	show platform software fed [switch] active acl policy 18	Esse comando imprime somente as informações sobre a política 18. Você pode obter essa ID de política a partir do comando 2.
4	show platform software fed [switch] active acl interface intftype pacl	Esse comando imprime as informações sobre a ACL com base no tipo de interface (pacl/vacl/racl/gacl/sgacl e assim por diante).
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Esse comando imprime as informações sobre a ACL com base no tipo de interface (pacl/vacl/racl/gacl/sgacl e assim por diante) e também filtra o protocolo (ipv4/ipv6/mac e assim por diante).
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Esse comando imprime as informações sobre as interfaces.
7	show platform software fed [switch] active acl interface 0x9	Esse comando imprime as informações curtas da ACL aplicada na interface, com base no IIF-ID (comando de 6).
8	show platform software fed [switch] active acl definition	Esse comando imprime as informações sobre as ACLs configuradas na caixa e cuja presença está no CGD.
9	show platform software fed [switch] active acl iifid 0x9	Esse comando imprime as informações detalhadas da ACL aplicada na interface, com base no IIF-ID.
10	show platform software fed [switch] active acl usage	Esse comando imprime o número de VMRs que cada ACL usa com base no Tipo de recurso.
11	show platform software fed [switch] active acl policy intftype pacl vcu	Esse comando fornece informações de política e também informações de VCU com base no tipo de interface (pacl/vacl/racl/gacl/sgacl e assim por diante).
12	show platform software fed [switch] active acl policy intftype pacl cam	Esse comando fornece informações de política e detalhes sobre os VMRs no CAM, com base no tipo de interface (pacl/valc/racl/gacl/sgacl e assim por diante).
13	show platform software interface [switch] [active] R0 brief	Esse comando fornece detalhes sobre a interface na caixa.
14	show platform software fed [switch] active port if_id 9	Esse comando imprime os detalhes sobre a porta com base no IIF-ID.

15	show platform software fed [switch] active vlan 30	Esse comando imprime os detalhes sobre a VLAN 30.
16	show platform software fed [switch] active acl cam asic 0	Esse comando imprime a ACL cam completa no ASIC 0 que está sendo usado.
17	show platform software fed [switch] active acl counters hardware	Esse comando imprime todos os contadores de ACL do hardware.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	Imprimindo as entradas para a seção PBR, você pode fornecer seções diferentes como ACL e CPP em vez de PBR.
19	show platform software fed [switch] active punt cpuq [1|2|3 â€¦]	Para verificar a atividade em uma das filas da CPU, você também tem opções para limpar o status da fila para depuração.
20	show platform software fed [switch] active ifm mappings gpn	Imprimir o mapeamento de interface com o IIF-ID e os GPNs
21	show platform software fed [switch active ifm if-id	Imprima as informações sobre a configuração da interface e a afinidade com o ASIC. Esse comando é útil para verificar em que interface o ASIC e o CORE estão.
22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error â€¦]	Definindo o rastreamento de um recurso específico no FED.
23	request platform software trace rotate all	Limpando o buffer de rastreamento.
24	show platform software trace message fed [switch] active	Imprimindo o buffer de rastreamento para FED.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error â€¦]	Habilitando os rastreamentos para FMAN.
26	show platform software trace message forwarding-manager [switch] [active] f0	Imprimindo o buffer de rastreamento para FMAN.
27	debug platform software infrastructure punt detail	Defina a depuração no PUNT.
28	debug ip cef packet all input rate 100	A depuração de pacote CEF está ativada.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.