Catalyst 9000 스위치의 보안 ACL 검증

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

- 용어

ACL 리소스 사용률 예

- 예 1. IPv4 TCAM
- 예 2. IPv4 TCAM/L4OP/VCU
- 예 3. IPv6TCAM/L4OP/VCU

토폴로지

구성 및 확인

- 시나리오 1. PACL(IP ACL)
  - IP ACL로 PACL 구성
  - PACL 확인
- 시나리오 2. PACL(MAC ACL)
  - MAC ACL로 PACL 구성
  - PACL 확인
- 시나리오 3. 라클
  - RACL 구성
  - RACL 확인
- 시나리오 4. 바클
  - VACL 구성
  - VACL 확인
- 시나리오 5. 그룹/클라이언트 ACL(DACL)
  - GACL 구성
  - GACL 확인
- 시나리오 6. ACL 로깅

문제 해결

- ACL 통계
  - ACL 통계 지우기
- ACL TCAM이 소진되면 어떻게 됩니까?
  - ACL TCAM 소모
  - VCU 소모
- ACL Syslog 오류
- 리소스 부족 시나리오 및 복구 작업
- ACL 규모 확인
  - 사용자 지정 SDM 템플릿(TCAM 재할당)

관련 정보

- Debug 및 Trace 명령

소개

이 문서에서는 Catalyst 9000 Series 스위치에서 ACL(Access Control List)을 확인하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 내용은 다음 하드웨어 버전을 기반으로 합니다.

- C9200
- C9300
- C9400
- C9500
- C9600

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

참고: 다른 Cisco 플랫폼에서 이러한 기능을 활성화하는 데 사용되는 명령에 대해서는 해당 컨피그레이션 가이드를 참조하십시오.

배경 정보

ACL은 라우터 또는 스위치를 통과할 때 트래픽을 필터링하고 지정된 인터페이스를 통과하는 패킷을 허용하거나 거부합니다. ACL은 패킷에 적용되는 허용 및 거부 조건을 순차적으로 모아 놓은 것입니다. 인터페이스에서 패킷이 수신되면 스위치는 액세스 목록에 지정된 기준에 따라 패킷이 전달할 필수 권한을 갖는지 확인하기 위해 패킷의 필드를 적용된 ACL과 비교합니다. 액세스 목록의 조건에 대해 하나씩 패킷을 테스트합니다. 첫 번째 일치는 스위치에서 패킷을 허용할지 아니면 거부할지를 결정합니다. 스위치가 첫 번째 일치 이후 테스트를 중지하므로 목록의 조건 순서가 중요합니다. 일치하는 조건이 없으면 스위치에서 패킷을 거부합니다. 제한이 없는 경우 스위치는 패킷을 전달합니다. 그렇지 않으면 스위치는 패킷을 삭제합니다. 스위치는 전달하는 모든 패킷에 ACL을 사용할 수 있습니다.

네트워크에 대한 기본 보안을 제공하기 위해 액세스 목록을 구성할 수 있습니다. ACL을 구성하지 않으면 스위치를 통과하는 모든 패킷이 모든 네트워크 부품에 허용될 수 있습니다. ACL을 사용하여 네트워크의 다른 부분에 액세스할 수 있는 호스트를 제어하거나 라우터 인터페이스에서 전달 또는 차단되는 트래픽 유형을 결정할 수 있습니다. 예를 들어, 이메일 트래픽은 전달할 수 있지만 텔넷 트래픽은 전달할 수 없습니다.

용어

에이스	ACE(Access Control Entry) - ACL 내의 단일 규칙/라인
ACL	ACL(Access Control List) - 포트에 적용되는 ACE 그룹
DACL	DACL(Downloadable ACL) - ISE 보안 정책을 통해 동적으로 푸시되는 ACL
PACL	포트 ACL(PACL) - 레이어 2 인터페이스에 적용되는 ACL
라클	RACL(Routed ACL) - 레이어 3 인터페이스에 적용되는 ACL
바클	VACL(VLAN ACL) - VLAN에 적용되는 ACL
GACL	그룹 ACL(GACL) - ID에 따라 사용자 그룹 또는 클라이언트에 동적으로 할당되는 ACL
IP ACL	IPv4/IPv6 패킷을 분류하는 데 사용됩니다. 이러한 규칙에는 소스 및 목적지 IPv4 주소, TCP/UDP 소스 및 목적지 포트, TCP 플래그 및 DSCP 등을 비롯한(이에 제한되지 않음) 다양한 레이어-3 및 레이어-4 패킷 필드와 특성이 포함됩니다.
MACL	MAC Address ACL(MACL) - 비 IP 패킷을 분류하는 데 사용됩니다. 규칙에는 소스/대상 MAC 주소, 이더 유형 등을 비롯한 다양한 레이어 2 필드 및 특성이 포함되어 있습니다.
L4OP	L4OP(Layer 4 Operator Port) - EQ(Equal To)가 아닌 논리와 일치합니다. GT(보다 큼), LT(보다 작음), NE(같지 않음) 및 RANGE(시작-종료)
VCU	VCU(Value Comparison Unit) - L4OP는 레이어 4 헤더에 대해 분류를 수행하기 위해 VCU로 변환됩니다.
VMR	VMR(Value Mask Result) - ACE 항목이 TCAM에 VMR로 내부적으로 프로그래밍됩니다.
CGD	CGD(Class Group Database) - 여기서 FMAN-FP는 ACL 콘텐츠를 저장합니다.
클래스	CGD에서 ACE를 식별하는 방법
CG	CG(클래스 그룹) - CGD에서 ACL을 식별하는 방법에 대한 클래스 그룹입니다.

CGE	CGE(Class Group Entry) - 클래스 그룹에 저장된 ACE 항목입니다.
FMAN	FMAN(Forwarding Manager) - Cisco IOS® XE와 하드웨어 간의 프로그래밍 레이어
연방	FED(Forwarding Engine Driver) - 디바이스의 하드웨어를 프로그래밍하는 구성 요소

ACL 리소스 사용률 예

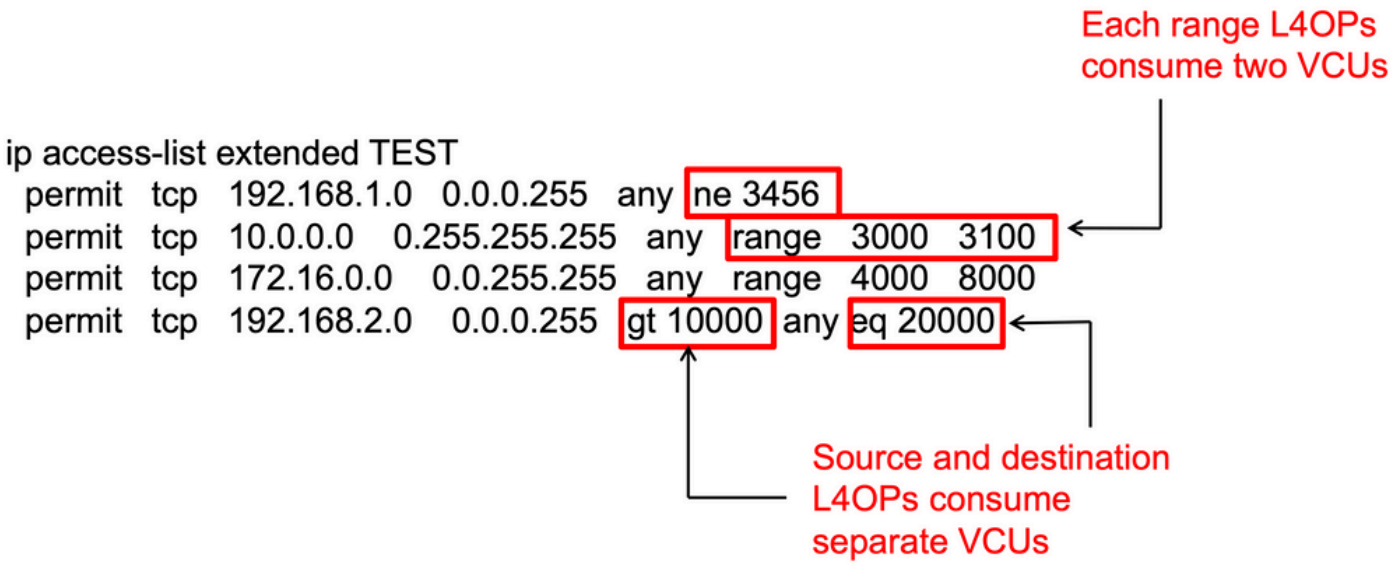
ACL이 TCAM, L4OP 및 VCU를 사용하는 방법을 보여 주기 위해 다음 세 가지 예를 제공합니다.

예 1. IPv4 TCAM

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

	TCAM 항목	L4OP	VCU
소비	5	0	0

예 2. IPv4 TCAM/L4OP/VCU



```
ip access-list extended TEST
10 permit tcp 192.168.1.0 0.0.0.255 any
neq 3456


<-- 1 L4OP, 1 VCU


20 permit tcp 10.0.0.0 0.255.255.255 any
range 3000 3100  <-- 1 L4OP, 2 VCU


30 permit tcp 172.16.0.0 0.0.255.255 any
range 4000 8000  <-- 1 L4OP, 2 VCU


40 permit tcp 192.168.2.0 0.0.0.255
gt 10000
 any
eq 20000 <-- 2 L4OP, 2 VCU
```

	TCAM 항목	L4OP	VCU
소비	4	5	7

예 3. IPv6 TCAM/L4OP/VCU

IPv6 ACE는 TCAM 엔트리 2개를 사용하는 반면, IPv4는 TCAM 엔트리 1개를 사용합니다. 이 예에서 4개의 ACE는 4개가 아닌 8개의 TCAM을 사용합니다.

<#root>

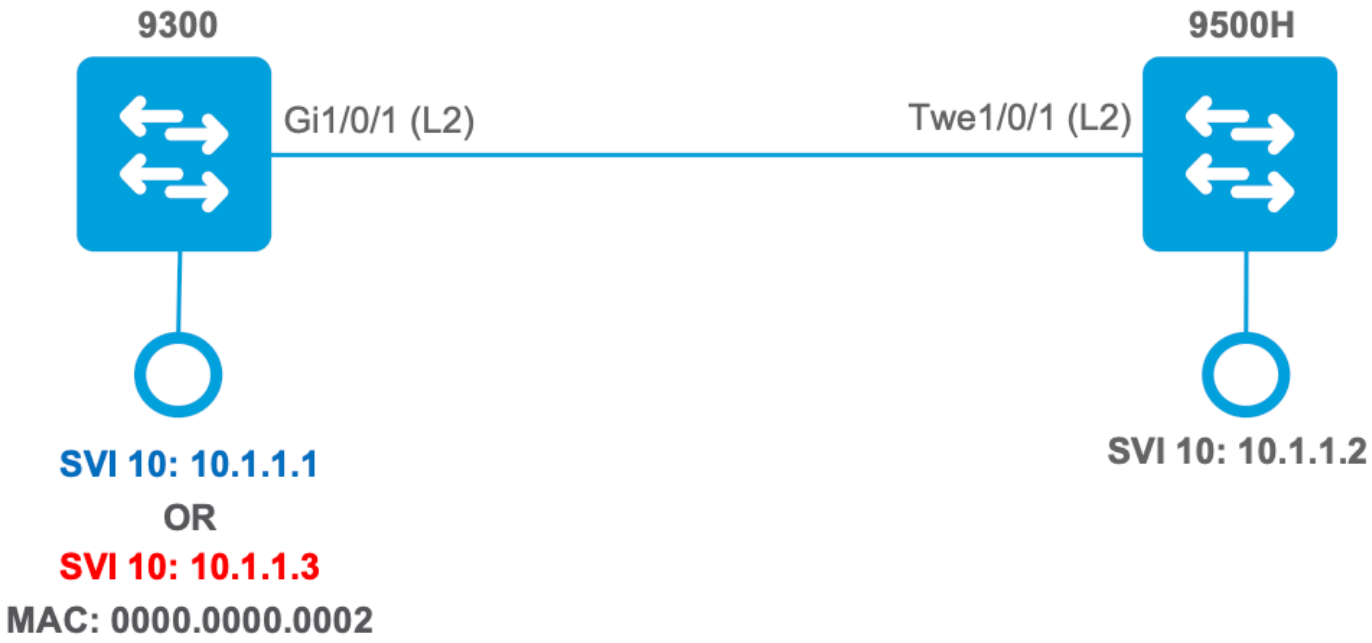
```
ipv6 access-list v6TEST
sequence 10 deny ipv6 any 2001:DB8:C18::/48 fragments
sequence 20 deny ipv6 2001:DB8::/32 any
sequence 30 permit tcp host 2001:DB8:C19:2:1::F host 2001:DB8:C18:2:1::1
eq bgp  <-- One L4OP & VCU


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

	TCAM 항목	L4OP	VCU
소비	8	2	2

토폴로지

9300 VLAN 10 SVI는 이 이미지에 표시된 두 개의 IP 주소 중 하나를 사용합니다. 이 예는 전달 또는 삭제 결과를 보여줍니다.



구성 및 확인

이 섹션에서는 소프트웨어 및 하드웨어에서 ACL 프로그래밍을 확인하고 문제를 해결하는 방법을 다룹니다.

시나리오 1. PACL(IP ACL)

PACL은 레이어 2 인터페이스에 할당됩니다.

- 보안 경계: 포트 또는 VLAN
- 첨부 파일: 레이어 2 인터페이스
- 방향: 인그레스 또는 이그레스(한 번에 하나씩)
- 지원되는 ACL 유형: MAC ACL 및 IP ACL(표준 또는 확장)

IP ACL로 PACL 구성

```
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
```

PACL 확인

인터페이스와 연결된 IF_ID를 검색합니다.

```
<#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
```

IF_ID에 바인딩된 클래스 그룹 ID(CG ID)를 확인합니다.

<#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

CG ID와 연결된 ACL 정보.

<#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)

CG ID 및 CG ID를 사용하는 인터페이스에 대한 정책 정보.

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

PACL이 작동하는지 확인합니다.

참고: 를 입력하면 show ip access-lists privileged EXEC 명령을 사용하면 표시된 일치 수는 하드웨어에서 액세스 제어되는 패킷을 고려하지 않습니다. 스위치드 및 라우티드 패킷에 대한 몇 가지 기본 하드웨어 ACL 통계를 얻으려면 show platform software fed switch{switch_num|active|standby}acl counters hardware privileged EXEC 명령을 사용합니다.

<#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...>
```

시나리오 2. PACL(MAC ACL)

PACL은 레이어 2 인터페이스에 할당됩니다.

- 보안 경계: 포트 또는 VLAN
- 첨부 파일: 레이어 2 인터페이스
- 방향: 인그레스 또는 이그레스(한 번에 하나씩)
- 지원되는 ACL 유형: MAC ACL 및 IP ACL(표준 또는 확장)

MAC ACL로 PACL 구성

```
<#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
```

PACL 확인

인터페이스와 연결된 IF_ID를 검색합니다.

<#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
```

IF_ID에 바인딩된 클래스 그룹 ID(CG ID)를 확인합니다.

<#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
```

CG ID와 연결된 ACL 정보.

```
<#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
```

CG ID 및 CG ID를 사용하는 인터페이스에 대한 정책 정보.

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

PACL이 작동하는지 확인합니다.

- MACL은 소스 주소 0001.aaaa.aaaa만 허용합니다.
- 이는 MAC ACL이므로 비 IP ARP 패킷이 삭제되어 ping이 실패합니다.

<#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...>
```

시나리오 3. 라클

RACL은 SVI 또는 라우티드 인터페이스와 같은 레이어 3 인터페이스에 할당됩니다.

- 보안 경계: 다른 서브넷
- 첨부 파일: 레이어 3 인터페이스
- 방향: 인그레스 또는 이그레스
- 지원되는 ACL 유형: IP ACL(표준 또는 확장)

RACL 구성

```
<#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
```

RACL 확인

인터페이스와 연결된 IF_ID를 검색합니다.

<#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
```

IF_ID에 바인딩된 클래스 그룹 ID(CG ID)를 확인합니다.

<#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
```

CG ID와 연결된 ACL 정보.

<#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)
```

CG ID 및 CG ID를 사용하는 인터페이스에 대한 정책 정보.

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

RACL이 작동하는지 확인합니다.

참고: 를 입력하면 show ip access-lists privileged EXEC 명령을 사용하면 표시된 일치 수는 하드웨어에서 액세스 제어되는 패킷을 고려하지 않습니다. show platform software fed switch{switch_num|active|standby}ACL 카운터 하드웨어 사용스위치드 및 라우티드 패킷에 대한 몇 가지 기본 하드웨어 ACL 통계를 얻기 위한 특별 권한 EXEC 명령

<#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...>
```

시나리오 4. 바클

VACL은 레이어 2 VLAN에 할당됩니다.

- 보안 경계: VLAN 내부 또는 VLAN 간
- 첨부 파일: VLAN/VLAN 맵
- 방향: 인그레스(Ingress) 및 이그레스(Egress) 모두 동시에
- 지원되는 ACL 유형: MAC ACL 및 IP ACL(표준 또는 확장)

VACL 구성

<#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
```

VACL 확인

인터페이스와 연결된 IF_ID를 검색합니다.

<#root>

```
9500H#
show platform software fed active ifm interfaces vlan

Interface
IF_ID
               State
--------------------------------------------------------------------------
Vlan10                              0x00420010
        READY
```

IF_ID에 바인딩된 클래스 그룹 ID(CG ID)를 확인합니다.

<#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
```

CG 그룹 ID와 연결된 ACL 정보.

동일한 명명된 VACL 정책에서 사용되는 두 개의 ACL이 있으며 이 acl-group으로 그룹화됩니다

```
<#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
```

CG ID 및 CG ID를 사용하는 인터페이스에 대한 정책 정보.

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

VACL이 작동하는지 확인합니다.

- 문제 해결은 PACL 및 RACl 섹션과 동일한 시나리오입니다. Ping 테스트에 대한 자세한 내용은 이 섹션을 참조하십시오.
- 적용된 ACL 정책에 의해 거부된 10.1.1.3에서 10.1.1.2로의 Ping입니다.
- platform drop 명령을 확인합니다.

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

시나리오 5. 그룹/클라이언트 ACL(DACL)

그룹/클라이언트 ACL은 ID에 따라 사용자 그룹 또는 클라이언트에 동적으로 적용됩니다. DACL이라고도 합니다.

- 보안 경계: 클라이언트(클라이언트 인터페이스 레벨)
- 첨부 파일: 클라이언트 인터페이스당
- 방향: 인그레스 전용
- 지원되는 ACL 유형: MAC ACL 및 IP ACL(표준 또는 확장)

GACL 구성

```
<#root>

Cat9400#
```

show run interface gigabitEthernet 2/0/1

```
Building configuration...

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

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

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

service-policy type control subscriber ISE_Gi2/0/1

```
end

Cat9400#
```

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

```
            Interface:  GigabitEthernet2/0/1
```

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

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

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

Status: Authorized **<-- Authorized client**

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

Server Policies:

```
              ACS ACL:
```

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

<-- The ACL pushed from ISE server

```
Method status list:
       Method           State
        dot1x           Stopped

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

Cat9400#
show ip access-lists xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

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

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

GACL 확인

iif-id에 바인딩된 그룹 CG ID입니다.

<#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

그룹 GC ID와 연결된 ACL 정보.

<#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
```

시나리오 6. ACL 로깅

디바이스 소프트웨어는 표준 IP 액세스 목록에 의해 허용되거나 거부된 패킷에 대한 syslog 메시지를 제공할 수 있습니다. ACL과 일치하는 패킷은 패킷에 대한 정보 로그 메시지가 콘솔로 전송됩니다. 콘솔에 로깅되는 메시지의 레벨은로깅 콘솔명령을 사용하여 Syslog 메시지를 제어합니다.

- ACL 로그 메시지는 uRPF(Unicast Reverse Path Forwarding)와 함께 사용되는 ACL에 대해 지원되지 않습니다. RACL에 대해서만 지원됩니다.
- 이그레스 방향의 ACL 로그는 디바이스의 제어 평면에서 생성된 패킷에 대해 지원되지 않습니다.
- 라우팅은 하드웨어에서 수행하고 소프트웨어에서 로깅하므로, 많은 수의 패킷이 logkeyword를 포함하는 permit 또는 deny ACE와 일치하는 경우 소프트웨어가 하드웨어 처리 속도와 일치하지 않으며 모든 패킷을 로깅할 수 없습니다.
- ACL을 트리거하는 첫 번째 패킷은 바로 로그 메시지를 발생시키고 이후 패킷은 나타나거나 기록되기 전에 5분 간격으로 수집됩니다. 로그 메시지에는 액세스 목록 번호, 패킷의 허용 또는 거부 여부, 패킷의 소스 IP 주소, 이전 5분 간격 동안 해당 소스의 허용 또는 거부된 패킷 수가 포함됩니다.
- ACL 로그 동작 및 제한에 대한 자세한 내용은 관련 정보 섹션에 나와 있는 해당 보안 컨피그레이션 가이드 Cisco IOS XE를 참조하십시오.

로그 예 PACL:

이 예에서는 ACL 유형과 log 키워드가 함께 작동하지 않는 음수 사례를 보여 줍니다.

```
<#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
```

로그 예 RACL(거부):

<#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
```

로그 예 RACL(허용):
log 명령문이 permit 명령문에 사용되는 경우 소프트웨어 카운터 hit는 전송된 패킷 수의 2배를 표시합니다.

```
<#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)
```

문제 해결

ACL 통계

ACL 문제를 해결할 때 디바이스에서 ACL 통계를 측정하는 방법과 위치를 이해하는 것이 중요합니다.

- ACL 통계는 ACE 레벨이 아닌 집계 레벨에서 수집됩니다.
- 하드웨어에는 ACE 또는 ACL 상태별로 허용할 수 있는 기능이 없습니다.
- 거부, 로그 및 CPU 전달 패킷과 같은 통계가 수집됩니다.
- MAC, IPv4 및 IPv6 패킷에 대한 통계는 별도로 수집됩니다.
- show platform software fed switch active acl counters hardware 집계 통계를 표시하는 데 사용할 수 있습니다.

ACL 통계 지우기

ACL 문제를 트러블슈팅할 때 다양한 ACL 카운터를 지워 새로운 베이스라인 카운트를 확보하는 것이 도움이 될 수 있습니다.

- 이 명령을 사용하면 소프트웨어 및 하드웨어 ACL 카운터 통계를 지울 수 있습니다.
- ACL 일치/적중 이벤트 문제를 해결할 때 최신 일치 또는 관련 일치의 기준을 설정하려면 관련 ACL을 지우는 것이 좋습니다.

<#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)

ACL TCAM이 소진되면 어떻게 됩니까?

- ACL은 항상 하드웨어 TCAM에 적용됩니다. TCAM이 이전에 구성된 ACL에서 이미 사용되고 있는 경우 새 ACL은 프로그래밍에 필요한 ACL 리소스를 얻지 못합니다.
- TCAM이 소진된 후 ACL이 추가되면 TCAM이 연결된 인터페이스에 대한 모든 패킷이 삭제됩니다.
- 소프트웨어에서 ACL을 보유하는 작업을 언로드라고 합니다.
- 리소스를 사용할 수 있게 되면 스위치에서 자동으로 하드웨어에 ACL을 프로그래밍하려고 시도합니다. 성공하면 ACL이 하드웨어로 푸시되고 패킷이 포워딩되기 시작합니다.
- 소프트웨어가 보유한 ACL을 TCAM에 프로그래밍하는 작업을 Reloading이라고 합니다.
- PACL, VACL, RACL 및 GACL은 서로 독립적으로 언로딩/재로딩될 수 있다.

ACL TCAM 소모

- 새로 추가된 ACL이 적용되는 인터페이스는 하드웨어 리소스를 사용할 수 있을 때까지 패킷 삭제를 시작합니다.
- GACL 클라이언트는 UnAuth 상태가 됩니다.

VCU 소모

- L4OP가 제한되거나 VCU에서 벗어나면 소프트웨어가 ACL 확장을 수행하고 VCU를 사용하지 않고 동일한 작업을 수행하기 위해 새 ACE 항목을 생성합니다.
- 이렇게 되면 추가된 항목에서 TCAM이 모두 소진될 수 있습니다.

ACL Syslog 오류

특정 보안 ACL 리소스가 부족하면 시스템에서 SYSLOG 메시지가 생성됩니다(인터페이스, VLAN, 레이블 등, 값이 다를 수 있음).

ACL 로그 메시지	정의	복구 작업
%ACL_ERRMSG-4-UNLOADED: 스위치 1 fed: 인터페이스 <interface>의 입력 <ACL>이(가) 하드웨어에서 프로그래밍되지 않고 트래픽이 삭제됩니다.	ACL이 언로드됨(소프트웨어에서 유지)	TCAM 배율을 조사합니다. 확장 범위를 벗어나면 ACL을 재설계합니다.
%ACL_ERRMSG-6-REMOVED: 1fed: <label>asic<number> 레이블에 대해 <interface> 인터페이스의 <ACL> 입력에 대한 언로드된 구성이 제거되었습니다.	언로드된 ACL 컨피그레이션이 인터페이스에서 제거되었습니다.	ACL이 이미 제거되었습니다. 수행할 작업이 없습니다.
%ACL_ERRMSG-6-RELOADED: 1 fed: 인터페이스 <interface>의 입력 <ACL>이(가) asic<number>의 <label>에 대한 하드웨어로 로드되었습니다.	이제 ACL이 하드웨어에 설치됨	ACL의 문제가 이제 하드웨어로 해결되었습니다. 수행할 작업이 없습니다.
%ACL_ERRMSG-3-ERROR: 1 fed: 입력 <ACL> IP ACL <NAME> 구성이 <interface>의 바인드 순서 <number>에 적용되지 않았습니다.	기타 유형의 ACL 오류(예: dot1x ACL 설치 실패)	ACL 컨피그레이션이 지원되는지, TCAM이 확장 불가한지 확인합니다.
%ACL_ERRMSG-6-GACL_INFO: 스위치 1 R0/0: fed: GACL에 대해 로깅이 지원되지 않습니다.	GACL에 구성된 로그 옵션이 있습니다.	GACL은 로그를 지원하지 않습니다. GACL에서 로그 명령문을 제거합니다.
%ACL_ERRMSG-6-PACL_INFO: 스위치 1 R0/0: fed: PACL에 대해 로깅이 지원되지 않습니다.	PACL에 구성된 로그 옵션이 있습니다.	PACL은 로그를 지원하지 않습니다. PACL에서 로그 명령문을 제거합니다.
%ACL_ERRMSG-3-ERROR: 스위치 1 R0/0:	(dot1x) ACL이 대	ACL 컨피그레이션이 지원되는

fed: 입력 IPv4 그룹 ACL implicit_deny:<name>: 컨피그레이션이 클라이언트 MAC 0000.0000.0000에 적용되지 않습니다.	상 포트에 적용되지 않음	지, TCAM이 확장 불가한지 확인합니다.

리소스 부족 시나리오 및 복구 작업

시나리오 1. ACL 바인딩	복구 작업
• ACL이 생성되어 인터페이스 또는 VLAN에 적용됩니다. • TCAM 소진과 같은 '리소스 부족' 조건으로 인해 바인딩이 실패합니다. • ACL 내의 어떤 ACE도 TCAM에 프로그래밍할 수 없습니다. ACL은 언로드됨 상태로 유지됩니다. • UNLOADED 상태에서 문제가 해결될 때까지 모든 트래픽(제어 패킷 포함)이 인터페이스에 드롭됩니다.	TCAM 사용률을 낮추기 위해 ACL을 다시 설계합니다.
시나리오 2. ACL 수정	복구 작업
• ACL이 생성되어 인터페이스에 적용되고, 인터페이스에 적용되는 동안 더 많은 ACE 항목이 이 ACL에 추가됩니다. • TCAM에 리소스가 없으면 수정 작업이 실패합니다. • ACL 내의 어떤 ACE도 TCAM에 프로그래밍할 수 없습니다. ACL은 언로드됨 상태로 유지됩니다. • Unloaded 상태에서는 문제가 해결될 때까지 모든 트래픽(제어 패킷 포함)이 인터페이스에 드롭됩니다. • 기존 ACL 항목도 수정될 때까지 UNLOADED 상태에서 실패합니다.	TCAM 사용률을 낮추기 위해 ACL을 다시 설계합니다.
시나리오 3. ACL 다시 바인딩	복구 작업
• ACL Re-bind는 ACL을 인터페이스에 연결한 다음 첫 번째 ACL을 분리하지 않고 다른 ACL을 동일한 인터페이스에 연결하는 작업입니다.	TCAM 사용률을 낮추기 위해 ACL을 다시 설계합니다.

• 첫 번째 ACL이 생성되어 성공적으로 연결됩니다. • 다른 이름과 동일한 프로토콜(IPv4/IPv6)을 가진 더 큰 ACL이 생성되어 동일한 인터페이스에 연결됩니다. • 디바이스에서 첫 번째 ACL을 성공적으로 분리하고 새 ACL을 이 인터페이스에 연결하려고 시도합니다. • TCAM에 리소스가 없으면 다시 바인딩 작업이 실패합니다. • ACL 내의 어떤 ACE도 TCAM에 프로그래밍할 수 없습니다. ACL은 언로드됨 상태로 유지됩니다. • UNLOADED 상태에서 문제가 해결될 때까지 모든 트래픽(제어 패킷 포함)이 인터페이스에 드롭됩니다.	
시나리오 4. 빈(Null) ACL 바인딩	복구 작업
• ACE 항목이 없는 ACL이 생성되어 인터페이스에 연결됩니다. • 시스템은 허용 'any ACE'를 사용하여 내부적으로 이 ACL을 생성하고 이를 하드웨어의 인터페이스에 연결합니다(이 상태에서는 모든 트래픽이 허용됨). • 그러면 ACE 항목이 동일한 이름 또는 번호로 ACL에 추가됩니다. 시스템은 각 ACE가 추가될 때마다 TCAM을 프로그래밍합니다. • ACE 항목을 추가할 때 TCAM에 리소스가 부족하면 ACL이 언로드됨 상태로 이동됩니다. • UNLOADED 상태에서 문제가 해결될 때까지 모든 트래픽(제어 패킷 포함)이 인터페이스에 드롭됩니다. • 기존 ACL 항목도 수정될 때까지 UNLOADED 상태에서 실패합니다.	TCAM 사용률을 낮추기 위해 ACL을 다시 설계합니다.

ACL 규모 확인

이 섹션에서는 ACL 확장 및 TCAM 사용률을 확인하기 위한 명령에 대해 설명합니다.

FMAN 액세스 목록 요약:

구성된 ACL 및 ACL당 총 ACE 수를 식별합니다.

<#root>

9500H#

show platform software access-list f0 summary

Access-list

Index Num Ref

Num ACEs

TEST

1 1 2

<-- ACL TEST contains 2 ACE entries

ELSE 2 1 1
DENY 3 0 1

ACL 사용:

<#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
```

TCAM 사용(17.x):

TCAM usage 명령은 16.x와 17.x 열차 간에 상당한 차이가 있습니다.

<#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)
```

TCAM 사용(16.x):

TCAM usage 명령은 16.x와 17.x 열차 간에 상당한 차이가 있습니다.

<#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...>
```

사용자 지정 SDM 템플릿(TCAM 재할당)

Cisco IOS XE Bengaluru 17.4.1 사용 시 를 사용하여 ACL 기능에 대한 사용자 지정 SDM 템플릿을 구성할 수 있습니다. sdm prefer custom acl명령을 실행합니다.

이 기능을 구성하고 확인하는 방법에 대한 자세한 내용은 System Management Configuration Guide, Cisco IOS XE Bengaluru 17.4.x (Catalyst 9500 Switches)를 참조하십시오.

이 섹션에는 몇 가지 기본 컨피그레이션 및 검증이 나와 있습니다.

현재 SDM 템플릿을 확인합니다.

<#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
```

현재 SDM 템플릿을 수정합니다.

- 9500H(config)#sdm에서 사용자 지정 acl 선호
  9500H(config-sdm-acl)#acl-ingress 26 priority 1 <— 새 26K 값을 적용합니다. (컨피그레이션 가이드에서 설명하는 우선순위)
  9500H(config-sdm-acl)#acl-egress 20 우선순위 2
  9500H(config-sdm-acl)#종료
  Use show sdm prefer custom 제안 값 및 sdm prefer custom commit 이 CLI를 통해 'view the changes(변경 사항 보기)'를 적용하려면 다음을 수행합니다.
- SDM 프로필의 변경 사항을 확인합니다.
- 9500H#show sdm prefer custom

SDM 템플릿 정보 표시:

세부 정보가 포함된 사용자 지정 템플릿입니다.
Ingress Security Access Control Entries*: 12288(현재) - 26624(제안) <— 현재 및 제안된 사용량 (26K 제안)
이그레스 보안 액세스 제어 항목*: 15360(현재) - 20480(제안)

9500H#show sdm prefer custom user-input

ACL 기능 사용자 입력
사용자 입력 값
==========

기능 이름 우선 순위 규모

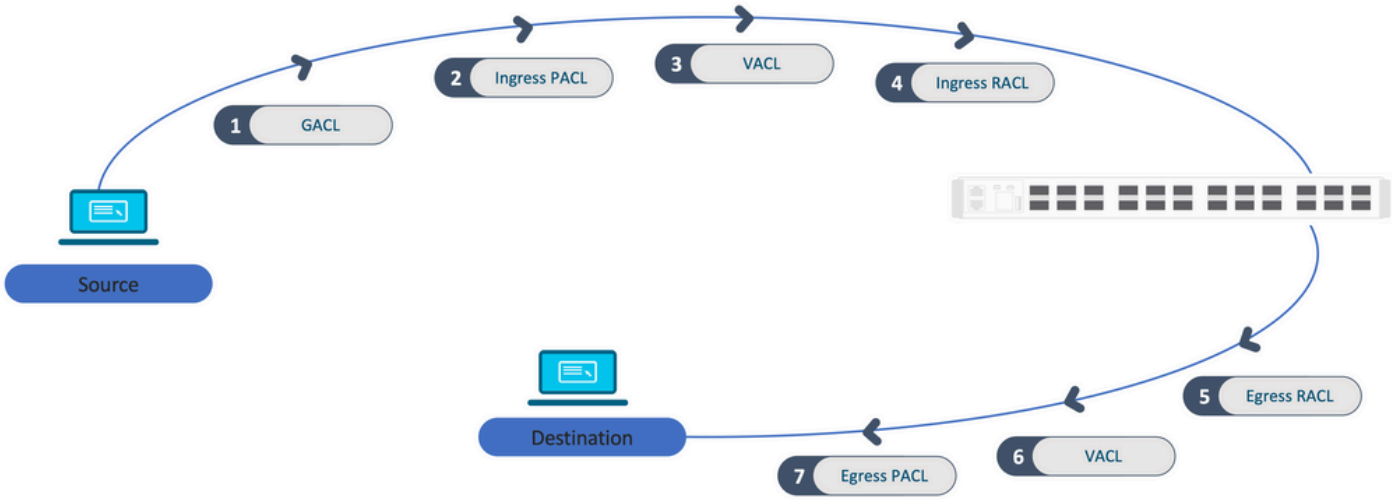
인그레스 보안 액세스 제어 항목: 1 26*1024 <— 사용자 입력으로 26 x 1024(26K)로 수정됨
이그레스 보안 액세스 제어 항목: 2 20*1024 <— 사용자 입력으로 20 x 1024(20K)로 수정됨

- SDM 프로필에 변경 사항을 적용합니다.
- 9500H(config)#sdm은 사용자 지정 커밋 선호
  실행 중인 SDM 기본 설정에 대한 변경 사항이 저장되며 다음 다시 로드할 때 적용됩니다. <—
  다시 로드되면 ACL TCAM이 사용자 지정 값에 할당됩니다.

추가 자료:

ACL 처리 순서:

ACL은 소스에서 대상까지 이 순서로 처리됩니다.



스택에서 프로그래밍된 ACL:

- 포트 기반 ACL(예: VACL, RACL)이 아닌 ACL은 모든 스위치의 트래픽에 적용되며 스택의 모든 스위치에 프로그래밍됩니다.
- 포트 기반 ACL은 포트의 트래픽에만 적용되며 인터페이스를 소유한 스위치에서만 프로그래밍됩니다.
- ACL은 액티브 스위치에 의해 프로그래밍되고 그 후에 멤버 스위치에 적용됩니다.
- ISSU/SVL과 같은 다른 이중화 옵션에도 동일한 규칙이 적용됩니다.

ACL 확장:

- ACL 확장은 디바이스에서 L4OP, Labels 또는 VCU가 부족할 때 발생합니다. 동일한 논리를 달성하고 TCAM을 신속하게 배출하려면 디바이스에서 동등한 ACE를 여러 개 생성해야 합니다.
- ### L4OP는 확장 중이며 이 ACL은 ## 생성됩니다.

9500H(config)#ip access-list extended 테스트
9500H(config-ext-nacl)#permit tcp 10.0.0.0 0.255.255.255 any gt 150 <— 포트 151 이상과 일치

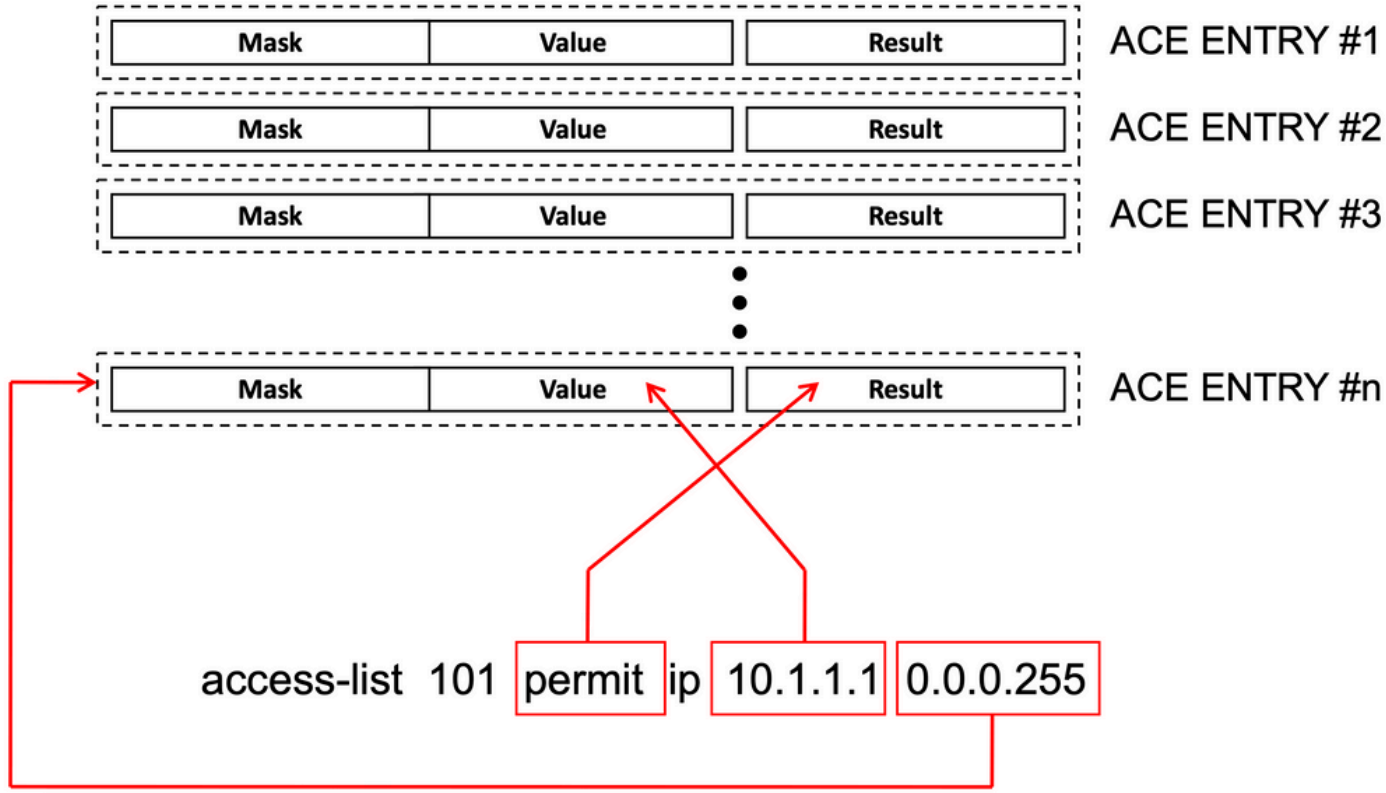
L4OP ###을 사용하지 않는 여러 ACE로 확장해야 합니다.
9500H(config-ext-nacl)#허용 tcp 10.0.0.0 0.255.255.255 모든 eq 151
9500H(config-ext-nacl)#허용 tcp 10.0.0.0 0.255.255.255 모든 eq 152
9500H(config-ext-nacl)#허용 tcp 10.0.0.0 0.255.255.255 모든 eq 153
9500H(config-ext-nacl)#허용 tcp 10.0.0.0 0.255.255.255 모든 eq 154
... .

TCAM 소비 및 레이블 공유:

- 각 ACL 정책은 레이블에 의해 내부적으로 참조됩니다.
- ACL 정책(GACL, PACL, VACL, RACL과 같은 보안 ACL)을 여러 인터페이스 또는 VLAN에 적용할 경우 동일한 레이블을 사용합니다.
- 인그레스/이그레스 ACL은 서로 다른 레이블 공간을 사용합니다.
- IPv4, IPv6 및 MAC ACL은 다른 레이블 공간을 사용합니다.
- 동일한 PACL은 interface-A의 인그레스 및 interface-A의 이그레스에 적용됩니다. TCAM에는 두 개의 PACL 인스턴스가 있으며, 각 인스턴스에는 인그레스 및 이그레스(Ingress and Egress)에 대한 고유한 레이블이 있습니다.
- L4OP가 포함된 동일한 PACL을 각 코어에 있는 여러 인그레스 인터페이스에 적용할 경우 TCAM에 프로그래밍된 동일한 PACL의 인스턴스가 각 코어당 하나씩 두 개 있습니다.

VMR 설명:

ACE는 내부적으로 TCAM에 'VMR'로 프로그래밍됩니다(값, 마스크, 결과라고도 함). 각 ACE 항목은 VMR을 사용하고 VCU를 사용할 수 있습니다.



ACL 확장성:

보안 ACL 리소스는 보안 ACL 전용입니다. 다른 기능과 공유되지 않습니다.

ACL TCAM 리소스	Cisco Catalyst 9600	Cisco Catalyst 9500	Cisco Catalyst 9400	Cisco Catalyst 9300	Cisco Catalyst 9200				
IPv4 항목	인그레스: 12000*	이그레스: 15000*	C9500: 18000*	C9500 고성능 인그레스: 12000* 이그레스: 15000*	18000*	C9300: 5000	C9300B 18000	C9300X:8000	1000
IPv6 항목	IPv4 항목의 절반		IPv4 항목의 절반		IPv4 항목의 절반	IPv4 항목의 절반			IPv4 항목의 절반

한 가지 유형의 IPv4 ACL 항목은 다음을 초과할 수 없습니다	12000	C9500: 18000	C9500 고성능: 15000	18000	C9300: 5000	C9300B: 18000	C9300X: 8000	1000
한 가지 유형의 IPv6 ACL 항목은 다음을 초과할 수 없습니다	6000	C9500: 9000	C9500 고성능: 7500	9000	2500/9000/4000			500
L4OPs/레이블	8	8		8	8			8
인그레스 VCU	192	192		192	192			192
이그레스(egress) VCU	96	96		96	96			96

관련 정보

- 보안 컨피그레이션 가이드, Cisco IOS XE Amsterdam 17.3.x(Catalyst 9200 스위치)
- 보안 컨피그레이션 가이드, Cisco IOS XE Amsterdam 17.3.x(Catalyst 9300 스위치)
- 보안 컨피그레이션 가이드, Cisco IOS XE Amsterdam 17.3.x(Catalyst 9400 스위치)
- 보안 컨피그레이션 가이드, Cisco IOS XE Amsterdam 17.3.x(Catalyst 9500 스위치)
- 보안 컨피그레이션 가이드, Cisco IOS XE Amsterdam 17.3.x(Catalyst 9600 스위치)
- 시스템 관리 컨피그레이션 가이드, Cisco IOS XE Bengaluru 17.4.x(Catalyst 9500 스위치)
- Cisco 기술 지원 및 다운로드

Debug 및 Trace 명령

번호	명령을 사용합니다	설명

1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	ASIC 서버에서 예외 카운터를 #N.
2	show platform software fed [switch] active acl	이 명령은 구성된 모든 ACL에 대한 정보를 인터페이스 및 정책 정보와 함께 상자에 인쇄합니다.
3	show platform software fed [switch] active acl policy 18	이 명령은 정책 18에 대한 정보만 인쇄합니다. 명령 2에서 이 정책 ID를 가져올 수 있습니다.
4	show platform software fed [switch] active acl interface intftype pacl	이 명령은 인터페이스 유형(pacl/vacl/racl/gacl/sgacl 등)에 따라 ACL에 대한 정보를 인쇄합니다.
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	이 명령은 인터페이스 유형(pacl/vacl/racl/gacl/sgacl 등)에 따라 ACL에 대한 정보를 인쇄하고, 프로토콜 단위(ipv4/ipv6/mac 등)로 필터링합니다.
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	이 명령은 인터페이스에 대한 정보를 인쇄합니다.
7	show platform software fed [switch] active acl interface 0x9	이 명령은 IIF-ID를 기반으로 인터페이스에 적용된 ACL의 짧은 정보를 인쇄합니다(6부터 명령).
8	show platform software fed [switch] active acl definition	이 명령은 상자에 구성되어 있고 CGD에 해당 항목이 있는 ACL에 대한 정보를 인쇄합니다.
9	show platform software fed [switch] active acl iifid 0x9	이 명령은 IIF-ID를 기반으로 인터페이스에 적용된 ACL의 Detailed 정보를 인쇄합니다.
10	show platform software fed [switch] active acl usage	이 명령은 각 ACL에서 Feature Type(기능 유형)에 따라 사용하는 VMR 수를 인쇄합니다.
11	show platform software fed [switch] active acl policy intftype pacl vcu	이 명령은 인터페이스 유형(pacl/vacl/racl/gacl/sgacl 등)에 따라 정책 정보 및 VCU 정보를 제공합니다.
12	show platform software fed [switch] active acl policy intftype pacl cam	이 명령은 인터페이스 유형(pacl/valc/racl/gacl/sgacl 등)에 따라 CAM의 VMR에 대한 정책 정보 및 세부사항을 제공합니다.

13	show platform software interface [switch] [active] R0 brief	이 명령은 상자의 인터페이스에 대한 세부 정보를 제공합니다.
14	show platform software fed [switch] active port if_id 9	이 명령은 IIF-ID를 기반으로 포트에 대한 세부사항을 인쇄합니다.
15	show platform software fed [switch] active vlan 30	이 명령은 VLAN 30에 대한 세부사항을 인쇄합니다.
16	show platform software fed [switch] active acl cam asic 0	이 명령은 사용 중인 ASIC 0에 전체 ACL 캠을 인쇄합니다.
17	show platform software fed [switch] active acl counters hardware	이 명령은 하드웨어의 모든 ACL 카운터를 인쇄합니다.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	PBR 섹션에 대한 항목을 인쇄하면 PBR 대신 ACL 및 CPP와 같은 다른 섹션을 제공할 수 있습니다.
19	show platform software fed [switch] active punt cpuq [1|2|3 …]	CPU 대기열 중 하나에서 작업을 확인하려면 디버깅을 위해 대기열 통계를 지우는 옵션도 있습니다.
20	show platform software fed [switch] active ifm mappings gpn	IIF-ID 및 GPN으로 인터페이스 매핑 인쇄
21	show platform software fed [switch active ifm if-id	인터페이스 컨피그레이션 및 ASIC와의 선호도에 대한 정보를 인쇄합니다. 이 명령은 ASIC 및 CORE가 어떤 인터페이스인지 확인하는 데 유용합니다.
22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error …]	FED에서 특정 기능에 대한 추적을 설정합니다.
23	request platform software trace rotate all	추적 버퍼를 지웁니다.
24	show platform software trace message fed [switch] active	FED에 대한 추적 버퍼를 인쇄하는 중입니다.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error …]	FMAN에 대한 추적을 활성화합니다.

26	show platform software trace message forwarding-manager [switch] [active] f0	FMAN에 대한 추적 버퍼를 인쇄하는 중입니다.
27	debug platform software infrastructure punt detail	PUNT에서 디버깅을 설정합니다.
28	debug ip cef packet all input rate 100	CEF 패킷 디버깅이 켜져 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.