Validierung von Sicherheits-ACLs auf Catalyst Switches der Serie 9000

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Terminologie
Beispiele für die Nutzung von ACL-Ressourcen
Beispiel 1. IPv4-TCAM
Beispiel 2. IPv4 TCAM/L4OP/VCU
Beispiel 3. IPv6TCAM/L4OP/VCU
Topologie
Konfiguration und Überprüfung
Szenario 1. PACL (IP ACL)
Konfigurieren von PACL mit IP ACL
PACL überprüfen
Szenario 2. PACL (MAC-ACL)
Konfigurieren der PACL mit MAC ACL
PACL überprüfen
Szenario 3. RACL
RACL konfigurieren
RACL überprüfen
Szenario 4. VACL
Konfigurieren von VACL
VACL überprüfen
Szenario 5. Gruppen-/Client-ACL (DACL)
Konfigurieren von GACL
GACL überprüfen
Szenario 6. ACL-Protokollierung
Fehlerbehebung
ACL-Statistik
Löschen von ACL-Statistiken
Was passiert, wenn der ACL-TCAM erschöpft ist?
ACL TCAM-Erschöpfung
Erschöpfung der VCU
ACL-Syslog-Fehler
Szenarien außerhalb der Ressourcen und Wiederherstellungsaktionen
Überprüfung der ACL-Skalierung
Benutzerdefinierte SDM-Vorlage (TCAM-Neuzuweisung)
Zugehörige Informationen
Debug- und Trace-Befehle

Einleitung

In diesem Dokument wird beschrieben, wie Sie ACLs (Zugriffskontrolllisten) auf Catalyst Switches der Serie 9000 überprüfen und entsprechende Fehler beheben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software- und Hardware-Versionen:

- C9200
- C9300
- C9400
- C9500
- C9600

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

> **Hinweis**: Informationen zu den zur Aktivierung dieser Funktionen auf anderen Cisco Plattformen verwendeten Befehlen finden Sie im entsprechenden Konfigurationsleitfaden.

Hintergrundinformationen

ACLs filtern den Datenverkehr, der einen Router oder Switch passiert, und lassen Pakete zu bzw. verweigern diese, die bestimmte Schnittstellen überschreiten. Eine ACL ist eine sequenzielle Sammlung von Zulassen- und Ablehnungsbedingungen, die für Pakete gelten. Wenn ein Paket über eine Schnittstelle empfangen wird, vergleicht der Switch die Felder im Paket mit allen angewendeten ACLs, um zu überprüfen, ob das Paket über die erforderlichen Berechtigungen für die Weiterleitung verfügt. Hierbei werden die in den Zugriffslisten angegebenen Kriterien zugrunde gelegt. Die einzelnen Pakete werden anhand der Bedingungen in einer Zugriffsliste getestet. Die erste Übereinstimmung entscheidet, ob der Switch die Pakete akzeptiert oder ablehnt. Da der Switch die Tests nach der ersten Übereinstimmung beendet, ist die Reihenfolge der Bedingungen in der Liste kritisch. Wenn keine Bedingungen übereinstimmen, lehnt der Switch das Paket ab. Wenn keine Einschränkungen bestehen, leitet der Switch das Paket weiter. Andernfalls bricht er das Paket ab. Der Switch kann ACLs für alle weitergeleiteten Pakete verwenden.

Sie können Zugriffslisten konfigurieren, um grundlegende Sicherheitsfunktionen für Ihr Netzwerk bereitzustellen. Wenn Sie keine ACLs konfigurieren, können alle Pakete, die über den Switch geleitet werden, auf alle Netzwerkkomponenten angewendet werden. Sie können ACLs verwenden, um zu steuern, welche Hosts auf verschiedene Teile eines Netzwerks zugreifen können, oder um zu entscheiden, welche Arten von Datenverkehr an Routerschnittstellen weitergeleitet oder blockiert werden. Sie können beispielsweise E-Mail-Verkehr weiterleiten, jedoch keinen Telnet-Verkehr.

Terminologie

RAUM	Zugriffskontrolleintrag (Access Control Entry, ACE) - eine einzelne Regel/Leitung in einer ACL

ACL	Zugriffskontrollliste (ACL) - Eine Gruppe von ACEs, die auf einen Port angewendet werden
DACL	Herunterladbare ACL (DACL) - Eine ACL wird dynamisch über die ISE-Sicherheitsrichtlinie übertragen
PACL	Port-ACL (PACL) - Eine ACL, die auf eine Layer-2-Schnittstelle angewendet wird
RACL	Routed ACL (RACL) - Eine ACL, die auf eine Layer 3-Schnittstelle angewendet wird
VACL	VLAN ACL (VACL) - Eine auf ein VLAN angewendete ACL
GACL	Gruppen-ACL (Group ACL, GACL) - Eine ACL, die einer Benutzergruppe oder einem Client basierend auf deren Identität dynamisch zugewiesen wird
IP-Zugriffskontrolllisten	Dient zur Klassifizierung von IPv4-/IPv6-Paketen. Diese Regeln enthalten verschiedene Layer-3- und Layer-4-Paketfelder und -attribute, darunter Quell- und Ziel-IPv4-Adressen, TCP/UDP-Quell- und Ziel-Ports, TCP-Flags und DSCP usw.
MACL	MAC Address ACL (MACL) - Dient der Klassifizierung von Nicht-IP-Paketen. Regeln enthalten verschiedene Layer-2-Felder und -Attribute, z. B. Quell-/Ziel-MAC-Adresse, Ethertyp usw.
L4OP	Layer-4-Operator-Port (L4OP) - Entspricht anderer Logik als EQ (Equal To). GT (größer als), LT (kleiner als), NE (ungleich) und RANGE (von-zu)
VCU	Value Comparison Unit (VCU) - L4OPs werden in VCU übersetzt, um die Klassifizierung für Layer-4-Header durchzuführen.
VMR	Value Mask Result (VMR) - Ein ACE-Eintrag wird im TCAM intern als VMR programmiert.
CGD	Class Group Database (CGD) - Wo FMAN-FP ACL-Inhalte speichert
Klassen	Wie werden ACEs in der CGD identifiziert?
CG	Class Group (CG) - Eine Gruppe von Klassen, in denen die Identifizierung von ACLs in der CGD beschrieben wird.
CGE	Class Group Entry (CGE) - Ein ACE-Eintrag, der in einer Klassengruppe gespeichert

	ist
FMAN	Forwarding Manager (FMAN) - Die Programmierungsebene zwischen Cisco IOS® XE und Hardware
FED	Forwarding Engine Driver (FED) - Die Komponente, die die Hardware des Geräts programmiert

Beispiele für die Nutzung von ACL-Ressourcen

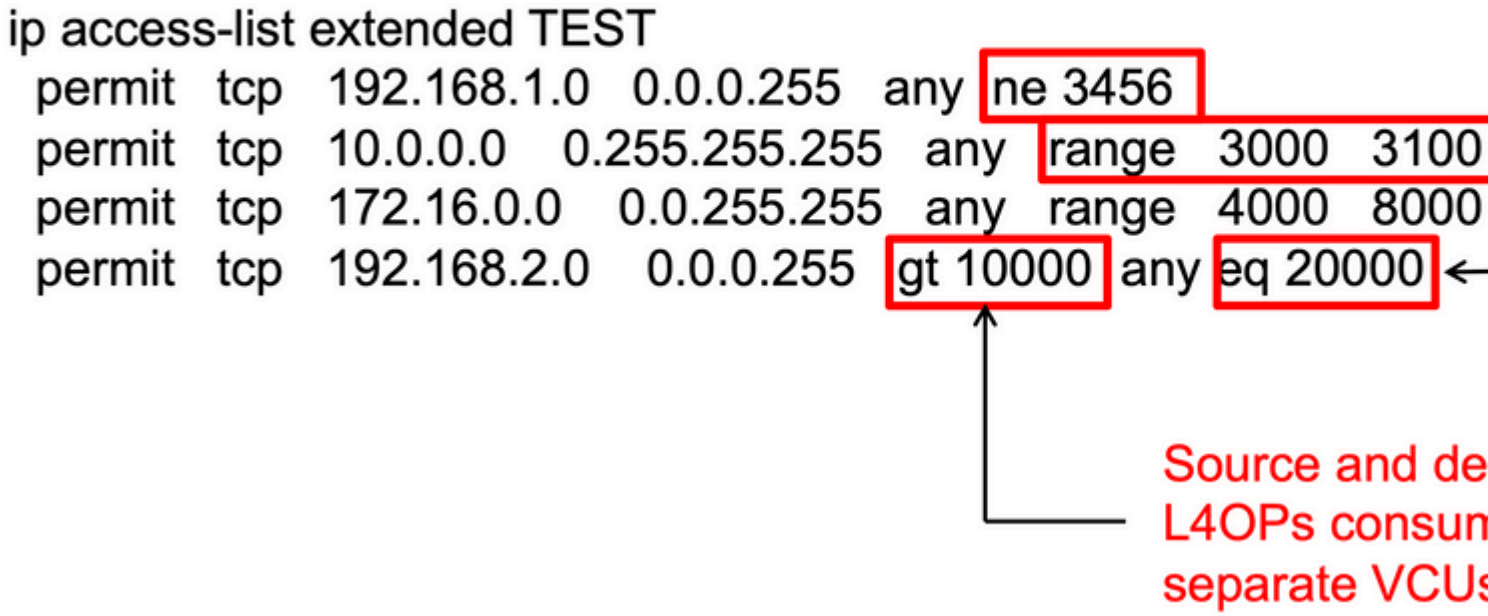
Es werden drei Beispiele angeführt, um zu veranschaulichen, wie ACLs TCAM, L4OPs und VCUs nutzen.

Beispiel 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-Einträge	**L4OPs**	**VCUs**
Verbrauch	5	0	0

Beispiel 2. IPv4 TCAM/L4OP/VCU



<#root>

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


<-- 1 L4OP, 1 VCU


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


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


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

	TCAM-Einträge	L4OPs	VCUs
Verbrauch	4	5	7

Beispiel 3. IPv6 TCAM/L4OP/VCU

IPv6-ACEs verwenden zwei TCAM-Einträge im Vergleich zu einem für IPv4. In diesem Beispiel benötigen vier ACEs statt vier acht TCAMs.

<#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

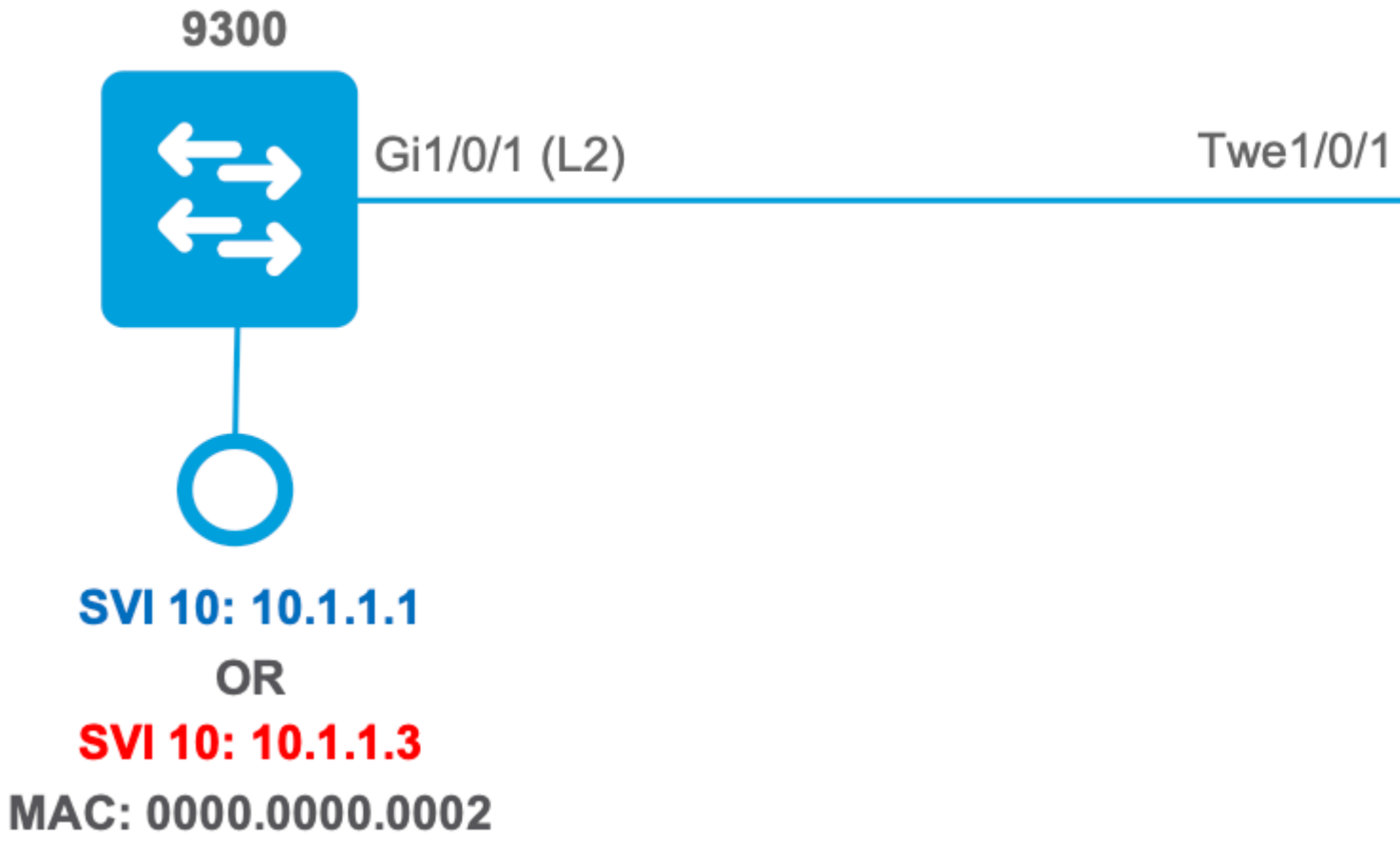
```
 host 2001:DB8:C18:2:1::1
```

<-- One L4OP & VCU

	TCAM-Einträge	L4OPs	VCUs
Verbrauch	8	2	2

Topologie

Die 9300 VLAN 10 SVI verwendet eine der beiden in diesem Bild gezeigten IP-Adressen, je nachdem, ob in den Beispielen ein Weiterleitungs- oder ein Ableitungsergebnis angezeigt wird.



Konfiguration und Überprüfung

In diesem Abschnitt wird beschrieben, wie Sie die ACL-Programmierung in Software und Hardware überprüfen und Fehler in dieser beheben.

Szenario 1. PACL (IP ACL)

PACLs werden einer Layer-2-Schnittstelle zugewiesen.

- Sicherheitsgrenze: Ports oder VLANs
- Anhang: Layer-2-Schnittstelle
- Richtung: Eingang oder Ausgang (einzeln)
- Unterstützte ACL-Typen: MAC ACL und IP ACLs (Standard oder erweitert)

Konfigurieren von PACL mit IP ACL

<#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
```

PACL überprüfen

Rufen Sie die der Schnittstelle zugeordnete IF_ID ab.

```
<#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
```

Überprüfen Sie die Klassengruppen-ID (CG-ID), die an IF_ID gebunden ist.

```
<#root>

9500H#
show platform software fed active acl interface 0x8       <-- IF_ID with leading zeros omitted


############################################################
########                                  ##################
#######   Printing Interface Infos     ###################
########                                  ##################
############################################################

INTERFACE:
TwentyFiveGigE1/0/1                                  <-- Confirms the interface matches the IF_ID


MAC 0000.0000.0000
############################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028

Interface Type: Port                                    <-- Type: Port indicates Layer 2 interface



if-id: 0x0000000000000008                               <-- IF_ID 0x8 is correct

    Input IPv4: Policy Handle: 0x5b000093

Policy Name: TEST                                     <-- The named ACL bound to this interface



    CG ID: 9                                         <-- Class Group ID for this entry



CGM Feature: [0] acl                                    <-- Feature is ACL

        Bind Order: 0
```

ACL-Informationen, die der CG-ID zugeordnet sind.

```
<#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)
```

Richtlinieninformationen zur CG-ID sowie zu den Schnittstellen, die die CG-ID verwenden.

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

Bestätigen Sie, dass die PACL funktioniert.

> **Anmerkung:** Wenn Sie das show ip access-lists privileged EXEC -Befehl wird die angezeigte Übereinstimmungsanzahl nicht für Pakete berücksichtigt, die in der Hardware zugriffsgesteuert werden. Verwenden Sie den Befehl show platform software fed switch {*switch_num*|active|standby}acl counters hardware-privileged EXEC, um einige grundlegende Hardware-ACL-Statistiken für geswitchte und geroutete Pakete zu erhalten.

<#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...>
```

Szenario 2. PACL (MAC-ACL)

PACLs werden einer Layer-2-Schnittstelle zugewiesen.

- Sicherheitsgrenze: Ports oder VLANs
- Anhang: Layer-2-Schnittstelle
- Richtung: Eingang oder Ausgang (einzeln)
- Unterstützte ACL-Typen: MAC ACL und IP ACLs (Standard oder erweitert)

Konfigurieren der PACL mit MAC ACL

<#root>

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


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



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



9500H#
show access-lists MAC-TEST


Extended MAC access list MAC-TEST
    permit host 0001.aaaa.aaaa any

9500H#
show running-config interface twentyFiveGigE 1/0/1


Building configuration...
```

```
interface TwentyFiveGigE1/0/1
switchport access vlan 10
switchport mode access
```

mac access-group MAC-TEST in <-- Applied MACL to layer 2 interface

PACL überprüfen

Rufen Sie die der Schnittstelle zugeordnete IF_ID ab.

<#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

Überprüfen Sie die Klassengruppen-ID (CG-ID), die an IF_ID gebunden ist.

<#root>

9500H#

show platform software fed active acl interface 0x8 <-- IF_ID with leading zeros omitted

```
############################################################
########                                ##################
#######   Printing Interface Infos     #################
########                                ##################
############################################################
```

INTERFACE: TwentyFiveGigE1/0/1 <-- Confirms the interface matches the IF

```
MAC 0000.0000.0000
############################################################
    intfinfo: 0x7f489404e408
    Interface handle: 0x7e000028
```

Interface Type: Port **<-- Type: Port indicates Layer 2 interface**

if-id: 0x0000000000000008 **<-- IF_ID 0x8 is correct**

Input MAC: Policy Handle: 0xde000098

Policy Name: MAC-TEST **<-- The named ACL bound to this interface**

CG ID: 20 **<-- Class Group ID for this entry**

CGM Feature: [0] acl **<-- Feature is ACL**

Bind Order: 0

ACL-Informationen, die der CG-ID zugeordnet sind.

<#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

Richtlinieninformationen zur CG-ID sowie zu den Schnittstellen, die die CG-ID verwenden.

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

PACL funktioniert:

- Die MACL lässt nur die Quelladresse 0001.aaaa.aaaa zu.
- Da es sich um eine MAC-Zugriffskontrollliste handelt, wird ein Nicht-IP-ARP-Paket verworfen, wodurch der Ping fehlschlägt.

<#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...>

Szenario 3. RACL

RACL wird einer Layer-3-Schnittstelle wie einer SVI oder einer gerouteten Schnittstelle zugewiesen.

- Sicherheitsgrenze: Unterschiedliche Subnetze
- Anhang: Layer-3-Schnittstelle
- Richtung: Eingang oder Ausgang
- Unterstützte ACL-Typen: IP ACLs (Standard oder erweitert)

RACL konfigurieren

```
<#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 überprüfen

Rufen Sie die der Schnittstelle zugeordnete IF_ID ab.

```
<#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
```

Überprüfen Sie die Klassengruppen-ID (CG-ID), die an IF_ID gebunden ist.

```
<#root>

9500H#

show platform software fed active acl interface 0x26  <-- IF_ID for SVI Vlan 10 with leading zeros omitt

############################################################
########                                ##################
#######     Printing Interface Infos   #################
########                                ##################
############################################################


INTERFACE: Vlan10                                          <-- Confirms the interface matches the IF_ID


MAC 0000.0000.0000
############################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x6e000047


Interface Type: L3                                         <-- Type: L3 indicates Layer 3 type interface



if-id: 0x0000000000000026                                  <-- IF_ID 0x26 is correct


    Input IPv4: Policy Handle: 0x2e000095
```

Policy Name: TEST **<-- The named ACL bound to this interface**

CG ID: 9 **<-- Class Group ID for this entry**

CGM Feature: [0] acl **<-- Feature is ACL**

Bind Order: 0

ACL-Informationen, die der CG-ID zugeordnet sind.

<#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)
```

Richtlinieninformationen zur CG-ID sowie zu den Schnittstellen, die die CG-ID verwenden.

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

Bestätigen Sie, dass die RACL funktioniert.

Anmerkung: Wenn Sie das show ip access-lists privileged EXEC -Befehl wird die angezeigte Übereinstimmungsanzahl nicht für Pakete berücksichtigt, die in der Hardware zugriffsgesteuert werden. Verwenden Sie die Hardware des über die Plattformsoftware gespeisten Switch{*switch_num*|active|standby}acl-Zählers.privilegierten EXEC-Befehl, um einige grundlegende ACL-Statistiken für Switch- und Routing-Pakete zu erhalten.

<#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...>
```

Szenario 4. VACL

VACLs werden einem Layer-2-VLAN zugewiesen.

- Sicherheitsgrenze: innerhalb oder über ein VLAN
- Anhang: VLAN-/VLAN-Zuordnung
- Richtung: Eingang und Ausgang gleichzeitig
- Unterstützte ACL-Typen: MAC ACL und IP ACLs (Standard oder erweitert)

Konfigurieren von 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
```

VACL überprüfen

Rufen Sie die der Schnittstelle zugeordnete IF_ID ab.

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

show platform software fed active ifm interfaces vlan

Interface

IF_ID

State

Vlan10 0x00420010

READY

Überprüfen Sie die Klassengruppen-ID (CG-ID), die an IF_ID gebunden ist.

<#root>

9500H#

show platform software fed active acl interface 0x420010 <-- IF_ID for the Vlan

```
##########################################################
########                                ##################
#######   Printing Interface Infos     #################
########                                ##################
##########################################################
```

INTERFACE: Vlan10 <-- Can be L2 only, with no vlan interfa

MAC 0000.0000.0000

```
##########################################################
    intfinfo: 0x7fc8cc7c7f48
    Interface handle: 0xf1000024
    Interface Type: Vlan
    if-id: 0x0000000000420010
```

Input IPv4:

Policy Handle: 0xd10000a3

<-- VACL has both Ingress and Egress actions

Policy Name: VACL <-- Name of the VACL used

CG ID: 530 <-- Class Group ID for entry

CGM Feature: [35] acl-grp <-- Feature is ACL group, versus ACl

Bind Order: 0

Output IPv4:

```
 Policy Handle: 0xc80000a4
```

<-- VACL has both Ingress and Egress actions

```
         Policy Name: VACL
              CG ID: 530
         CGM Feature: [35] acl-grp
    Bind Order: 0
```

ACL-Informationen, die der CG-Gruppen-ID zugeordnet sind.

In derselben benannten VACL-Richtlinie werden zwei ACLs verwendet, die in diese ACL-Gruppe gruppiert sind.

<#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

Richtlinieninformationen zur CG-ID sowie zu den Schnittstellen, die die CG-ID verwenden.

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

Bestätigen Sie, dass die VACL funktioniert.

- Die Fehlerbehebung entspricht dem Szenario in den Abschnitten zu PACL und RACl. Weitere Informationen zum Ping-Test finden Sie in den folgenden Abschnitten.
- Ping von 10.1.1.3 an 10.1.1.2 verweigert von der angewendeten ACL-Richtlinie.
- Überprüfen Sie den Befehl 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...>
```

Szenario 5. Gruppen-/Client-ACL (DACL)

Gruppen-/Client-ACLs werden auf Grundlage ihrer Identität dynamisch auf eine Benutzergruppe oder einen Client angewendet. Diese werden manchmal auch als DACL bezeichnet.

- Sicherheitsgrenze: Client (Client-Schnittstellenebene)
- Anhang: Pro Client-Schnittstelle
- Richtung: nur Eingang
- Unterstützte ACL-Typen: MAC ACL und IP ACLs (Standard oder erweitert)

Konfigurieren von 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
```

GACL überprüfen

Die Gruppen-CG-ID ist an die if-id gebunden.

<#root>

```
Cat9400#
```

```
show platform software fed active acl interface 0x1765EB2C                <-- The IF_ID from the access

############################################################
########                                  ##################
#######    Printing Interface Infos    ###################
########                                 ##################
############################################################

INTERFACE: Client MAC

000a.aaaa.aaaa

                                                <-- Client MAC matches the access-session output

MAC

000a.aaaa.aaaa

############################################################
    intfinfo: 0x7f104820cae8
    Interface handle: 0x5a000110


Interface Type: Group                                                      <-- This is a group ident


IIF ID: 0x1765eb2c

    Input IPv4: Policy Handle: 0x9d00011e


  Policy Name: ACL-ALLOW:xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

:

<-- DACL name matches



CG ID: 127760                                                    <-- The ACL group ID

       CGM Feature: [35]

acl-grp

        Bind Order: 0
```

ACL-Informationen, die der GC-ID der Gruppe zugeordnet sind.

```
<#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
```

Szenario 6. ACL-Protokollierung

Die Gerätesoftware kann Syslog-Meldungen über Pakete bereitstellen, die von einer Standard-IP-Zugriffsliste zugelassen oder abgelehnt wurden. Jedes Paket, das mit der ACL übereinstimmt, bewirkt, dass eine informative Protokollmeldung über das Paket an die Konsole gesendet wird. Die Ebene der an der Konsole protokollierten Meldungen wird vomProtokollierungskonsoleBefehle, die die Syslog-Meldungen steuern.

- ACL-Protokollmeldungen werden für ACLs, die mit Unicast Reverse Path Forwarding (uRPF) verwendet werden, nicht unterstützt. Es wird nur für RACL unterstützt.

- ACL-Protokolle in Ausgangsrichtung werden für Pakete, die von der Kontrollebene des Geräts generiert werden, nicht unterstützt.

- Das Routing erfolgt in der Hardware und in der Protokollierungssoftware. Wenn also eine große Anzahl von Paketen mit einem Zulassen- oder Verweigern-ACE übereinstimmt, der ein Logschlüsselwort enthält, kann die Software nicht mit der Hardwareverarbeitungsrate übereinstimmen, und nicht alle Pakete können protokolliert werden.
- Das erste Paket, das die ACL auslöst, löst sofort eine Protokollmeldung aus, und die nachfolgenden Pakete werden in Intervallen von fünf Minuten erfasst, bevor sie angezeigt werden oder protokolliert werden. Die Protokollmeldung enthält die Zugriffslistennummer, ob das Paket zugelassen oder abgelehnt wurde, die Quell-IP-Adresse des Pakets und die Anzahl der Pakete von dieser Quelle, die im Intervall von fünf Minuten zuvor zugelassen oder abgelehnt wurden.
- Vollständige Details zum Verhalten und den Einschränkungen im ACL-Protokoll finden Sie im entsprechenden Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE, wie im Abschnitt "Related Information" (Verwandte Informationen) angegeben.

Protokollbeispiel für PACL:

Dieses Beispiel zeigt einen negativen Fall, bei dem der ACL-Typ und das log-Schlüsselwort nicht zusammenarbeiten.

```
<#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
```

RACL-Protokollbeispiel (Verweigern):

```
<#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
```

RACL-Beispiel (Permit) für Protokoll:
Wenn eine Protokollanweisung für eine permit-Anweisung verwendet wird, zeigt der Softwarezähler bei Treffern die doppelte Anzahl von gesendeten Paketen an.

<#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)
```

Fehlerbehebung

ACL-Statistik

Wenn Sie ein Problem mit einer Zugriffskontrollliste beheben, ist es wichtig zu wissen, wie und wo die Statistiken der Zugriffskontrollliste vom Gerät gemessen werden.

- ACL-Statistiken werden auf aggregierter Ebene und nicht auf ACE-Ebene gesammelt.
- Die Hardware kann keine ACE- oder ACL-Statistiken zulassen.
- Es werden Statistiken wie Deny-, Log- und CPU-weitergeleitete Pakete erfasst.
- Statistiken für MAC-, IPv4- und IPv6-Pakete werden separat erfasst.
- show platform software fed switch active acl counters hardware kann verwendet werden, um aggregierte Statistiken anzuzeigen.

Löschen von ACL-Statistiken

Bei der Behebung eines ACL-Problems kann es hilfreich sein, die verschiedenen ACL-Zähler zu löschen, um neue Baseline-Zähler zu erhalten.

- Mit diesen Befehlen können Sie die Software- und Hardware-ACL-Zählerstatistiken löschen.
- Wenn Sie Fehler bei Übereinstimmungen/Treffereignissen von ACLs beheben, wird empfohlen, die relevante ACL für Baseline-Übereinstimmungen zu löschen, die neu sind oder relevant sind.

<#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)
```

Was passiert, wenn der ACL-TCAM erschöpft ist?

- ACLs werden immer im Hardware-TCAM angewendet. Wenn TCAM bereits von zuvor konfigurierten ACLs verwendet wird, erhalten die neuen ACLs nicht die erforderlichen ACL-Ressourcen für die Programmierung.

- Wenn eine ACL hinzugefügt wird, nachdem der TCAM erschöpft ist, werden alle Pakete für die angeschlossene Schnittstelle verworfen.

- Die Aktion zum Halten einer ACL in der Software heißt **Entladen**.
- Sobald Ressourcen verfügbar sind, versucht der Switch automatisch, die ACLs in die Hardware zu programmieren. Bei einem erfolgreichen Vorgang werden die ACLs an die Hardware weitergeleitet, und die Pakete werden weitergeleitet.
- Das Programmieren einer softwarebasierten Zugriffskontrollliste in TCAM wird als **Neuladen** bezeichnet.

- PACL, VACL, RACL und GACL können unabhängig voneinander entladen/neu geladen werden.

ACL TCAM-Erschöpfung

- Die Schnittstelle, auf die die neu hinzugefügte ACL angewendet wird, verwirft Pakete, bis Hardwareressourcen verfügbar sind.
- GACL-Clients werden in den UnAuth-Status versetzt.

Erschöpfung der VCU

- Sobald die Anzahl der L4OPs überschritten ist oder die Anzahl der VCUs überschritten ist, führt die Software eine ACL-Erweiterung durch und erstellt neue ACE-Einträge, um eine gleichwertige Aktion ohne Verwendung von VCUs auszuführen.
- Sobald dies geschieht, kann der TCAM von diesen hinzugefügten Einträgen erschöpft werden.

ACL-Syslog-Fehler

Wenn eine bestimmte Security ACL-Ressource ausgeht, werden vom System SYSLOG-Meldungen generiert (Schnittstelle, VLAN, Label usw., die Werte können sich unterscheiden).

ACL-Protokollmeldung	Definition	Wiederherstellungsaktion
%ACL_ERRMSG-4-UNLOADED: Switch 1 wird gespeist: Eingang <ACL> an Schnittstelle <Schnittstelle> ist nicht in Hardware programmiert, und der Datenverkehr wird verworfen.	ACL ist entladen (wird in der Software gespeichert)	Prüfen der TCAM-Skalierung Wenn ACLs nicht ausreichend skalierbar sind, überarbeiten Sie sie.
%ACL_ERRMSG-6-REMOVED: 1 fed: Die entladene Konfiguration für Input <ACL> auf Schnittstelle <interface> wurde für Label <label>asic<number> entfernt.	Die entladene ACL-Konfiguration wird von der Schnittstelle entfernt.	ACL wurde bereits entfernt, keine Aktion erforderlich

%ACL_ERRMSG-6-RELOADED: 1 Einspeisung: Eingabe <ACL> an Schnittstelle <Schnittstelle> wurde jetzt in die Hardware für Label <Label> auf Basis<Nummer> geladen.	ACL ist jetzt in der Hardware installiert.	Das Problem mit der ACL ist nun in der Hardware behoben, es müssen keine Maßnahmen ergriffen werden.
%ACL_ERRMSG-3-ERROR: 1 eingegeben: Die Konfiguration der Eingabe <ACL>-IP-ACL <NAME> wird auf <Schnittstelle> bei der Bindungsreihenfolge <Nummer> nicht angewendet.	Andere Arten von ACL-Fehlern (z. B. Fehler bei der 802.1x ACL-Installation)	Bestätigung, dass die ACL-Konfiguration unterstützt wird und sich der TCAM nicht über die Skalierbarkeit hinaus erstreckt
%ACL_ERRMSG-6-GACL_INFO: Switch 1 R0/0: feed: Die Protokollierung wird für GACL nicht unterstützt.	Für GACL ist eine Protokolloption konfiguriert.	GACL unterstützt keine Protokolle. Protokollanweisungen aus GACL entfernen
%ACL_ERRMSG-6-PACL_INFO: Switch 1 R0/0: feed: Protokollierung wird für PACL nicht unterstützt.	Für PACL ist eine Protokolloption konfiguriert.	PACL unterstützt keine Protokolle. Protokollanweisungen aus PACL entfernen
%ACL_ERRMSG-3-ERROR: Switch 1 R0/0: fed: Input IPv4 Group ACL implicit_deny:<name>: Konfiguration wird nicht auf Client MAC 0000.0000.0000 angewendet.	(dot1x) ACL kann auf den Zielport nicht angewendet werden	Bestätigung, dass die ACL-Konfiguration unterstützt wird und sich der TCAM nicht über die Skalierbarkeit hinaus erstreckt

Szenarien außerhalb der Ressourcen und Wiederherstellungsaktionen

Szenario 1. ACL-Bindung	**Wiederherstellungsaktion**
• ACL wird erstellt und auf eine Schnittstelle oder ein VLAN angewendet. • Die Bindung schlägt aufgrund von Bedingungen fehl, bei denen keine Ressourcen verfügbar sind, z. B. TCAM-Erschöpfung. • Innerhalb der ACL können keine ACEs in TCAM programmiert werden. ACL bleibt im Zustand **UNLOADED**. • Im Status **UNLOADED** wird der gesamte Datenverkehr (einschließlich der Steuerungspakete) an der Schnittstelle verworfen, bis das Problem behoben ist.	Entwerfen Sie die ACL neu, um die Auslastung von TCAM zu reduzieren.
Szenario 2. ACL-Bearbeitung	**Wiederherstellungsaktion**
• Eine ACL wird erstellt und auf eine Schnittstelle angewendet, und weitere ACE-Einträge werden	Entwerfen Sie die ACL neu, um die Auslastung von TCAM zu reduzieren.

zu dieser ACL hinzugefügt, während sie auf die Schnittstelle(n) angewendet werden. • Wenn der TCAM nicht über Ressourcen verfügt, schlägt der Bearbeitungsvorgang fehl. • Innerhalb der ACL können keine ACEs in TCAM programmiert werden. ACL bleibt im Zustand **UNLOADED**. • Im Status **UNLOADED** wird der gesamte Datenverkehr (einschließlich Steuerungspakete) an der Schnittstelle verworfen, bis das Problem behoben ist. • Die vorhandenen ACL-Einträge schlagen ebenfalls im Zustand **UNLOADED fehl**, bis dies behoben ist.	
Szenario 3. ACL neu binden	**Wiederherstellungsaktion**
• ACL Re-bind (ACL-Neubindung) ist der Vorgang, bei dem eine ACL an eine Schnittstelle und dann eine weitere ACL an die gleiche Schnittstelle angefügt wird, ohne die erste ACL zu trennen. • Die erste ACL wurde erstellt und erfolgreich angehängt. • Eine größere ACL mit einem anderen Namen und demselben Protokoll (IPv4/IPv6) wird erstellt und an dieselbe Schnittstelle angeschlossen. • Das Gerät trennt die erste ACL erfolgreich ab und versucht, die neue ACL an diese Schnittstelle anzuschließen. • Wenn der TCAM nicht über Ressourcen verfügt, schlägt die erneute Bindung fehl. • Innerhalb der ACL können keine ACEs in TCAM programmiert werden. ACL bleibt im Zustand **UNLOADED**. • Im Status **UNLOADED** wird der gesamte Datenverkehr (einschließlich der Steuerungspakete) an der Schnittstelle verworfen, bis das Problem behoben ist.	Entwerfen Sie die ACL neu, um die Auslastung von TCAM zu reduzieren.
Szenario 4. Leere Bindungs-ACL (Null)	**Wiederherstellungsaktion**
• Eine ACL ohne ACE-Einträge wird erstellt und an eine Schnittstelle angeschlossen. • Das System erstellt diese ACL intern mit einer Berechtigung "any ACE" und fügt sie der Schnittstelle in der Hardware an (der gesamte Datenverkehr ist in diesem Zustand zulässig). • ACE-Einträge werden dann der ACL mit demselben Namen oder derselben Nummer	Entwerfen Sie die ACL neu, um die Auslastung von TCAM zu reduzieren.

hinzugefügt. Das System programmiert TCAM, wenn jeder ACE hinzugefügt wird. • Wenn dem TCAM beim Hinzufügen von ACE-Einträgen die Ressourcen ausgehen, wird die ACL in den Status **UNLOADED** verschoben. • Im Status **UNLOADED** wird der gesamte Datenverkehr (einschließlich der Steuerungspakete) an der Schnittstelle verworfen, bis das Problem behoben ist. • Die vorhandenen ACL-Einträge schlagen ebenfalls im Zustand **UNLOADED fehl**, bis dies behoben ist.	

Überprüfung der ACL-Skalierung

In diesem Abschnitt werden Befehle zur Bestimmung der ACL-Skalierung und der TCAM-Nutzung beschrieben.

FMAN-Zugriffslistenübersicht:

Identifizieren der konfigurierten ACLs und der gesamten ACE-Anzahl pro ACL

<#root>

9500H#

show platform software access-list f0 summary

Access-list

Index Num Ref

Num ACEs

TEST

1 1 2

<-- ACL TEST contains 2 ACE entries

ELSE 2 1 1
DENY 3 0 1

ACL-Verwendung:

<#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-Nutzung (17.x):

Der TCAM-Verwendungsbefehl weist erhebliche Unterschiede zwischen 16.x- und 17.x-Zügen auf.

<#root>

9500H#

show platform hardware fed active fwd-asic resource tcam utilization

Codes: EM - Exact_Match,

I - Input

,

O - Output

, IO - Input & Output, NA - Not Applicable

```
CAM Utilization for ASIC [0]

 Table                    Subtype

Dir


Max

     Used

%Used

       V4       V6    MPLS   Other
 ---------------------------------------------------------------------------------------------------

 Security ACL Ipv4

      TCAM

I


 7168

      16

 0.22%

    16        0       0        0
 Security ACL Non Ipv4   TCAM        I        5120       76    1.48%        0       36       0       40
 Security ACL Ipv4       TCAM

  O

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

<...snip...>

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

TCAM-Nutzung (16.x):

Der TCAM-Verwendungsbefehl weist erhebliche Unterschiede zwischen 16.x- und 17.x-Zügen auf.

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

Benutzerdefinierte SDM-Vorlage (TCAM-Neuzuweisung)

Verwenden von Cisco IOS XE Bengaluru 17.4.1 Sie können eine benutzerdefinierte SDM-Vorlage für ACL-Funktionen konfigurieren, indem Sie sdm prefer custom aclaus.

Details zur Konfiguration und Überprüfung dieser Funktion finden Sie im Konfigurationshandbuch zur Systemverwaltung, Cisco IOS XE Bengaluru 17.4.x (Catalyst 9500-Switches).

Dieser Abschnitt enthält Informationen zur grundlegenden Konfiguration und Verifizierung.

Überprüfen Sie die aktuelle SDM-Vorlage:

<#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
```

Aktuelle SDM-Vorlage ändern:

- 9500H(config)#**SDM bevorzugt benutzerdefinierte Zugriffskontrolllisten**
  9500H(config-sdm-acl)#**acl-ingress 26 priority 1 <â€" Apply new 26K value. (Priorität wird im Konfigurationsleitfaden erläutert)**
  9500H(config-sdm-acl)#**ACL-Ausgang 20 Priorität 2**
  9500H(config-sdm-acl)#**beenden**
  Nutzung show sdm prefer custom um die vorgeschlagenen Werte zu sehen und sdm prefer custom commit um die

Änderungen über diese CLI anzuzeigen.
- Überprüfen Sie die Änderungen am SDM-Profil.
- 9500H#**show sdm prefer benutzerdefiniert**

SDM-Vorlageninformationen werden angezeigt:

Dies ist die benutzerdefinierte Vorlage mit ihren Details.
Einträge für Zugangskontrolle im Sicherheitsbereich*: **12288 (aktuell) - 26624 (vorgeschlagen) <â€" Aktuelle und vorgeschlagene Nutzung (26 KB vorgeschlagen)**
Einträge für die Ausgangssicherheitszugriffskontrolle*: **15360 (aktuell) - 20480 (vorgeschlagen)**

9500H#**show sdm prefer benutzerdefinierte Benutzereingabe**

BENUTZEREINGABE FÜR ACL-FUNKTION
Benutzereingabewerte
==========

PRIORITÄT DES FEATURE-NAMENS **SKALIERUNG**

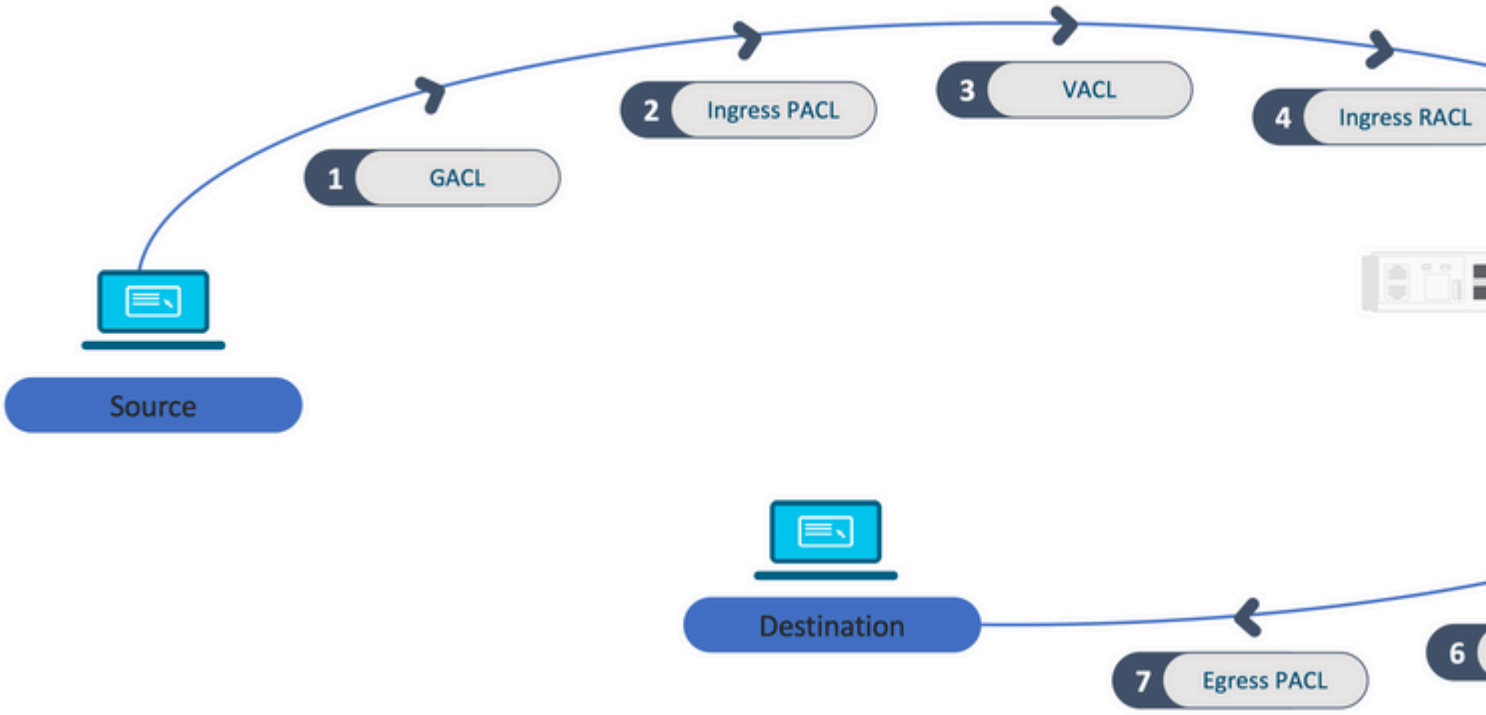
Einträge für die Zugriffskontrolle für Eingangssicherheit: **1 26*1024 <â€" Geändert durch Benutzereingabe auf 26 x 1024 (26 KB)**
Egress Security Access Control Entries: **2 20*1024 <â€" Geändert durch Benutzereingabe zu 20 x 1024 (20 K)**

- Änderungen auf das SDM-Profil anwenden.
- 9500H(config)#**SDM bevorzugt benutzerdefiniertes Commit**
  Änderungen an den aktuellen SDM-Einstellungen werden gespeichert und werden beim nächsten Neuladen wirksam. **<â€" Nach dem erneuten Laden wurde der ACL-TCAM dem benutzerdefinierten Wert zugewiesen.**

Weitere Informationen:

ACL-Verarbeitungsauftrag:

ACLs werden in dieser Reihenfolge von der Quelle bis zum Ziel verarbeitet.



In einem Stack programmierte ACLs:

- ACLs, die nicht auf Ports basieren (z. B. VACL, RACL), werden auf den Datenverkehr aller Switches angewendet und auf allen Switches im Stack programmiert.
- Port-basierte ACLs werden nur auf den Datenverkehr an einem Port angewendet und nur auf dem Switch programmiert, der die Schnittstelle besitzt.
- ACLs werden vom aktiven Switch programmiert und anschließend auf die Member-Switches angewendet.
- Die gleichen Regeln gelten für andere Redundanzoptionen wie ISSU/SVL.

ACL-Erweiterung:

- Die ACL-Erweiterung erfolgt, wenn auf dem Gerät keine L4OPs, Labels oder VCUs mehr vorhanden sind. Das Gerät muss mehrere äquivalente ACEs erstellen, um dieselbe Logik zu erreichen und den TCAM schnell zu erschöpfen.
- **### L4OPs sind skalierbar, und diese ACL wird erstellt ##**
  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€" entspricht Ports 151 und höher**

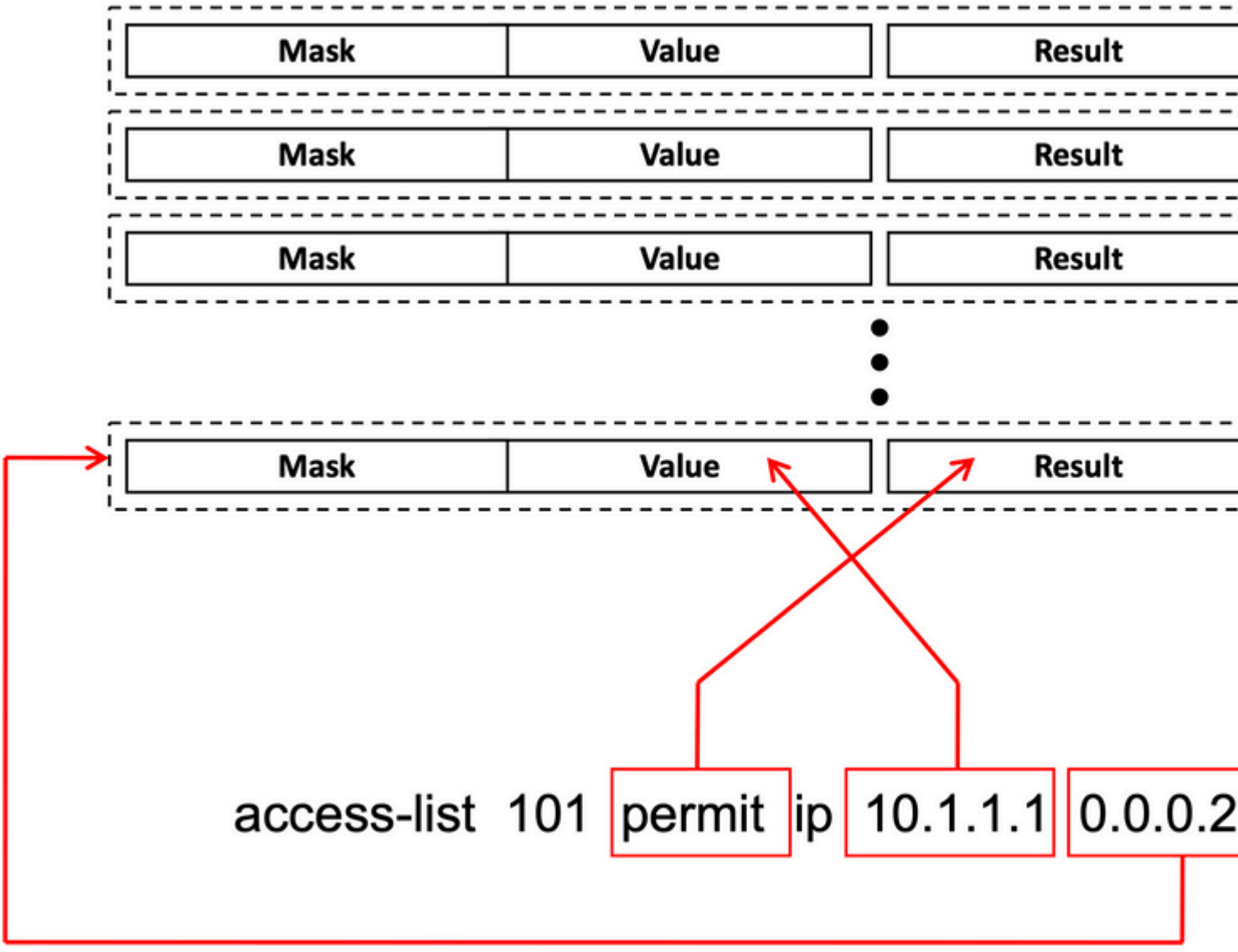
  ### Dies muss auf mehrere ACEs erweitert werden, die kein L4OP verwenden ###
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 151**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 152**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 153**
  9500H(config-ext-nacl)#**permit tcp 10.0.0.0 0.255.255.255 any eq 154**
  ... und so weiter ....

TCAM-Nutzung und gemeinsame Nutzung von Labels:

- Auf jede ACL-Richtlinie wird intern durch ein Label verwiesen.
- Wenn eine ACL-Richtlinie (eine Sicherheits-ACL wie GACL, PACL, VACL, RACL) auf mehrere Schnittstellen oder VLANs angewendet wird, verwendet sie das gleiche Label.
- Bei der Eingangs-/Ausgangs-ACL werden unterschiedliche Labels verwendet.
- IPv4, IPv6 und MAC ACL verwenden andere Labelräume.
- Dieselbe PACL wird auf den Eingang von Schnittstelle A und den Ausgang von Schnittstelle A angewendet. Es gibt zwei Instanzen der PACL im TCAM, von denen jede eine eindeutige Bezeichnung für "Ingress" und "Egress" trägt.
- Wenn dieselbe PACL mit L4OP auf mehrere Eingangsschnittstellen angewendet wird, die auf jedem Core vorhanden sind, gibt es zwei Instanzen derselben PACL, die im TCAM programmiert sind, eine pro Core.

VMR-Beschreibung:

Ein ACE wird im TCAM intern als 'VMR' programmiert - auch als Wert, Maske, Ergebnis bekannt. Jeder ACE-Eintrag kann VMRs und VCUs nutzen.



ACL-Skalierbarkeit:

Security ACL-Ressourcen sind dediziert für Security ACLs. Sie werden nicht mit anderen Funktionen geteilt.

ACL TCAM-Ressourcen	**Cisco Catalyst Serie 9600**	**Cisco Catalyst Serie 9500**	**Cisco Catalyst Serie 9400**	**Cisco Catalyst Serie 9300**	**Cisco Catalyst Serie 9200**				
IPv4-Einträge	Eingang: 12000*	Ausgehend: 15000*	C9500: 18000*	C9500 - Hohe Leistung Eingang: 12000* Ausgehend: 15000*	18000*	C9300: 5000	C9300B: 18000	C9300X: 8000	1000
IPv6-Einträge	Die Hälfte der IPv4-Einträge		Die Hälfte der IPv4-Einträge		Die Hälfte der IPv4-Einträge	Die Hälfte der IPv4-Einträge			Die Hälfte der IPv4-Einträge
Ein Typ von IPv4-ACL-Einträgen darf nicht überschritten werden.	12000		C950: 18000	C9500 - Hohe Leistung: 15000	18000	C9300: 5000	C9300B: 18000	C9300X: 8.000	1000
Ein Typ von IPv6-ACL-Einträgen darf nicht überschritten werden	6000		C9500: 9000	C9500 - Hohe Leistung: 7500	9000	2500/9000/4000			500
L4OPs/Label	8		8		8	8			8
Eingangs-VCU	192		192		192	192			192
Ausgangs-VCUs	96		96		96	96			96

Zugehörige Informationen

- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9200 Switches)
- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches)
- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9400 Switches)
- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9500 Switches)
- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9600 Switches)
- Konfigurationsanleitung zur Systemverwaltung, Cisco IOS XE Bengaluru 17.4.x (Catalyst 9500 Switches)
- Technischer Support und Downloads von Cisco

Debug- und Trace-Befehle

Zahl	Command	Bemerkung
1	show platform hardware fed [switch] active fwd-asic drops exceptions asic <0>	Speichern Sie die Ausnahmenzähler im ASIC #N.
2	show platform software fed [switch] active acl	Mit diesem Befehl werden die Informationen zu allen konfigurierten ACLs zusammen mit Schnittstellen- und Richtlinieninformationen ausgegeben.
3	show platform software fed [switch] active acl policy 18	Dieser Befehl druckt nur die Informationen zur Richtlinie 18. Sie können diese Richtlinien-ID aus Befehl 2 abrufen.
4	show platform software fed [switch] active acl interface intftype pacl	Dieser Befehl druckt die Informationen über die ACL auf Basis des Schnittstellentyps (pacl/vacl/racl/gacl/sgacl usw.).
5	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Dieser Befehl druckt die Informationen über die ACL auf Basis des Schnittstellentyps (pacl/vacl/racl/gacl/sgacl usw.) und filtert auch protokollmäßig (ipv4/ipv6/mac usw.).
6	show platform software fed [switch] active acl interface intftype pacl acltype ipv4	Dieser Befehl druckt die Informationen zu Schnittstellen.
7	show platform software fed [switch] active acl interface 0x9	Dieser Befehl druckt die kurzen Informationen der auf die Schnittstelle angewendeten ACL basierend auf der IIF-ID (Befehl von 6).
8	show platform software fed [switch] active acl definition	Mit diesem Befehl werden die Informationen zu den im Gerät konfigurierten ACLs ausgegeben, die im CGD vorhanden sind.
9	show platform software fed [switch] active acl iifid 0x9	Mit diesem Befehl werden auf Basis der IIF-ID die

		detaillierten Informationen der auf die Schnittstelle angewendeten ACL ausgegeben.
10	show platform software fed [switch] active acl usage	Mit diesem Befehl wird die Anzahl der VMRs ausgegeben, die jede ACL basierend auf dem Funktionstyp verwendet.
11	show platform software fed [switch] active acl policy intftype pacl vcu	Mit diesem Befehl erhalten Sie die Richtlinieninformationen sowie die VCU-Informationen, die auf dem Schnittstellentyp (pacl/vacl/racl/gacl/sgacl usw.) basieren.
12	show platform software fed [switch] active acl policy intftype pacl cam	Mit diesem Befehl erhalten Sie die Richtlinieninformationen und Details zu den VMRs im CAM, basierend auf dem Schnittstellentyp (pacl/valc/racl/gacl/sgacl usw.).
13	show platform software interface [switch] [active] R0 brief	Mit diesem Befehl erhalten Sie Details zur Benutzeroberfläche auf dem Gerät.
14	show platform software fed [switch] active port if_id 9	Dieser Befehl druckt die Details des Ports basierend auf der IIF-ID.
15	show platform software fed [switch] active vlan 30	Mit diesem Befehl werden die Details zum VLAN 30 ausgegeben.
16	show platform software fed [switch] active acl cam asic 0	Mit diesem Befehl wird die vollständige ACL-Cam auf dem verwendeten ASIC 0 gedruckt.
17	show platform software fed [switch] active acl counters hardware	Mit diesem Befehl werden alle ACL-Zähler von der Hardware ausgegeben.
18	show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0	Wenn Sie die Einträge für den PBR-Abschnitt drucken, können Sie andere Abschnitte wie ACL und CPP anstelle von PBR angeben.
19	show platform software fed [switch] active punt cpuq [1|2|3 â€¦]	Um die Aktivität in einer der CPU-Warteschlangen zu überprüfen, haben Sie außerdem die Möglichkeit, die Warteschlangenstatistiken für das Debuggen zu löschen.
20	show platform software fed [switch] active ifm mappings gpn	Ausgabe der Schnittstellenzuordnung mit der IIF-ID und den GPNs
21	show platform software fed [switch active ifm if-id	Drucken Sie die Informationen zur Schnittstellenkonfiguration und zur Affinität zum ASIC. Dieser Befehl ist hilfreich, um zu überprüfen, welche Schnittstelle ASIC und CORE sind.

22	set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug|error â€¦]	Festlegen der Ablaufverfolgung für eine bestimmte Funktion in FED.
23	request platform software trace rotate all	Löschen des Ablaufverfolgungspuffers
24	show platform software trace message fed [switch] active	Der Ablaufverfolgungspuffer für FED wird gedruckt.
25	set platform software trace forwarding-manager [switch] [active] f0 fman [debug|error â€¦]	Aktivieren der Spuren für FMAN.
26	show platform software trace message forwarding-manager [switch] [active] f0	Der Ablaufverfolgungspuffer für FMAN wird gedruckt.
27	debug platform software infrastructure punt detail	Legen Sie das Debugging auf PUNT fest.
28	debug ip cef packet all input rate 100	CEF-Paketdebugging ist aktiviert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.