

مادختساب اهحالصإو مزحلا عاطخأ فاشكتسأ ىلع (ACLs) لوصولا يف مكحتلا مئوق Nexus يساسألا ماضنلا

تايوتحملا

[عمدقملا](#)

[قيساسألا تابلطتملا](#)

[تابلطتملا](#)

[مدختسملا نوكملا](#)

[ططخملا](#)

[اهفئاظو لوصولا يف مكحتلا مئوق ىلع قرصنخم عماع قرظن](#)

[RACL و PACL](#)

[فدهلا](#)

[ططخملا حرش](#)

[اهحالصإو عاطخألا فاشكتسأ](#)

[N9K-3 و N9K-2 \(SVI 10 و SVI 20\) و N9K-1 \(ETH1/1\) نيم L3 تاهجاو ىلع RACL نيوكت 1. قوطخلا \(ETH1/14\)](#)

[L2 تاهجاو ىلع \(PACL\) ذفنم لاب قضاخلا لوصولا يف مكحتلا مئوق نيوكت 2. قوطخلا Switchport ل N9K-2](#)

[TCAM شقن](#)

[TCAM ققطنم نيوكت عارج](#)

[TCAM ققطنم تاليدعت 1. قوطخلا](#)

[ققطنملا مجح ليلقت 2. قوطخلا](#)

[TCAM ل ing-ifac ل ققطنم قداي 3. قوطخلا](#)

[نيوكتلا ظفح 4. قوطخلا](#)

[ليمححتلا قداغل 5. قوطخلا](#)

[ليمححتلا قداغل دعب ققحتلا](#)

[IP ذفنم ليل لوصولا قعومجم نيوكت](#)

[عاجرتسا 3. قوطخلا](#)

[IP ردصملا مادختساب N9K-3 نيم لاصتا رابتخلا لاسراو رورم قكرخ عاش نيب مق 4. قوطخلا 192.168.20.2 ل La0 192.168.0.10 نيم N9K-1](#)

[N9K-3 و N9K-2 و N9K-1 لوج RACL و PACL تايئاصحا تامولعم نم ققحتلا 5. قوطخلا](#)

عمدقملا

يف مكحتلا مئوق مادختساب اهحالصإو مزحلا عاطخأ فاشكتسأ قيفي ك دنتسملا اذه حضوي
Nexus يساسألا ماضنلا ىلع (ACLs) لوصولا

قيساسألا تابلطتملا

تابلطتملا

ة:للاتل عيضاوملاب ةفرعم كيذل نوكت ناب Cisco يصوت

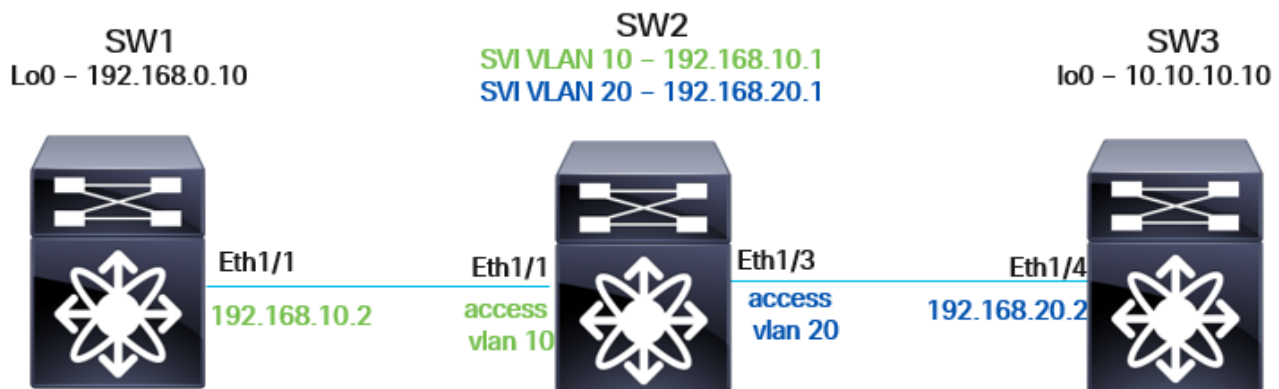
- NXOS ياساسالماظنلا
- لوصولا ف مكحتلا مئوق

مدختسملانوكملا

N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

عيمجتأب. ةيلمعم ةئيب ف Nexus ةزها نم دنتسمل اذه ف ةدراولا تامولعمل اءاشنإ مت ةكبش مدختست تنك اذإ. اقبس م دوجوم نيوكت يا نود دنتسمل اذه ف ةمدختسمل ةزهاال رما يال لمحتمل ريثألل كمهف نم دكأف ،ةرشابم

ططخملا



لوصولا ف مكحتلا مئوق ىلع ةرصتخم ةماع ةرظن اهفئاظوو

رورملا ةكرح ةيفصتل ياساسا لكشب (ACL) لوصولا ف مكحتلا ةمئاق مادختسا متي ةيفصتلا ،لاثملا ليبس ىلع) ةبولطملا ريياعملاو دعاوقلا نم ةلسلس ىلا اءانتسا اطورش قباطت مزحلا تناك اذإ ام دعاوقلا هذه ددحت .(ةهوجل/ردصم لل IP نيوانع ىلا اءانتسا ةمئاق ددحت ،طسبأ تاحلطمبو .اهضفر وأ اهب حامسلا متيس ناك اذإ ام دي دحتل ةددحم اءانتسا اهضفر نكمي وأ رورملا ةكبشلا مزحل حامسلا نكمي ناك اذإ ام لوصولا ف مكحتلا طساوب اهتجالعم مت ،صيخرتلا دعاوق طورش مزحلا تفوتسا اذإ .اهلخاد ةددحملا دعاوقلا ىلا صلختلا متيس ،ضفرلا طورش عم مزحلا تقباطت اذإ ،كلذ نم سكعلال ىلعو . Nexus لوجم اهنم

ريفوت ىلع اهتردق ف (ACL) لوصولا ف مكحتلا مئوقل ةيسيئرلا تازيمل اذإ لثمت

دعاوق قباطت يتل مزحل دد عبتت تب تادادل هذه موقت .مزحل قفدتل قئاصحل تادادل عاقلأ فاشكتسأ دنل قئاعلل قديفم نوكت نأ نكمي يتلاو ،لوصولل ف مكحتل قئاق اءالصلل مزحل نادقل تاهوئرانيس .

نم لقأ لبقتسي هنكلو ،مزحل نم انيعم ادعل لسري زاهلل ناك اذا ،لائمل لئبس ىلعل زعل ف لوصولل ف مكحتل قئاق نم قئاصحلل تادادلل دلاست نأ نكمي ،عقولملل قكبشلل لءاد اهل ف مزحل طاقسل مئل يتلل قطقنلل .

PACL و RACL

ىلعل اهل قئبطل مئل اذا ام ىلعل ءانب لوصولل ف مكحتل قئاق ذئفنت فلتلئل نأ نكمي ىلل امئف . (VACL) VLAN تاكلشل وأ ، (RACL) 3 قئبطلل تاهللو ، (PACL) 2 قئبطلل تاهللو :بئلالسلل هذلل قءوم قنراقم :

- ف مكحتل قئاق قئبطل مئل : (PACL) ذئللل ىلل لوصولل ف مكحتل قئاق (L2) 2 قئبطلل switchport ذئلل قءلعل (ACL) لوصولل .
- ف مكحتل قئاق قئبطل مئل : (RACL) ءلوملل ىلل لوصولل ف مكحتل قئاق (L3) 3 قئبطلل قءوم قءلعل (ACL) لوصولل .

قئبطلل ءلعل	ءارءلل	قءلعل	ءون قئاق مكحتل ف لوصولل ACL
ىلل قءراولل رورملل قءرل - طقلل قءراولل قءلعل.	Switchport تاهللو مكحتل قئاق قئبطل مئل اذا طقل قءلعل لوصولل ف ىلعل لمعلل اءنفل ،لاصلل لانائل رورمل قءرل قئفصلل VLAN تاكلشل عئملل طقل ىلعل اءل ءومسلل لاصلل.	L2	PACL
لمعلل - ءاوس ءل ىلعل رءاصلل قءراولل قءراولل قئفصلل لماع رورمل قءرل ،قءلعل ىلل قءراولل قءراولل قئفصلل لماع لمعلل امنئل رورمل قءرل قئفصلل ىلعل قءراولل قءرل .	SVI قئلعلل تاهللو L3 و Physical L3	L3	RACL

فدهل

حېحص لكشېب اهل اسرا متي يتي مزحل اعيمج مالتسإ نم دكأتال يوررضل نم

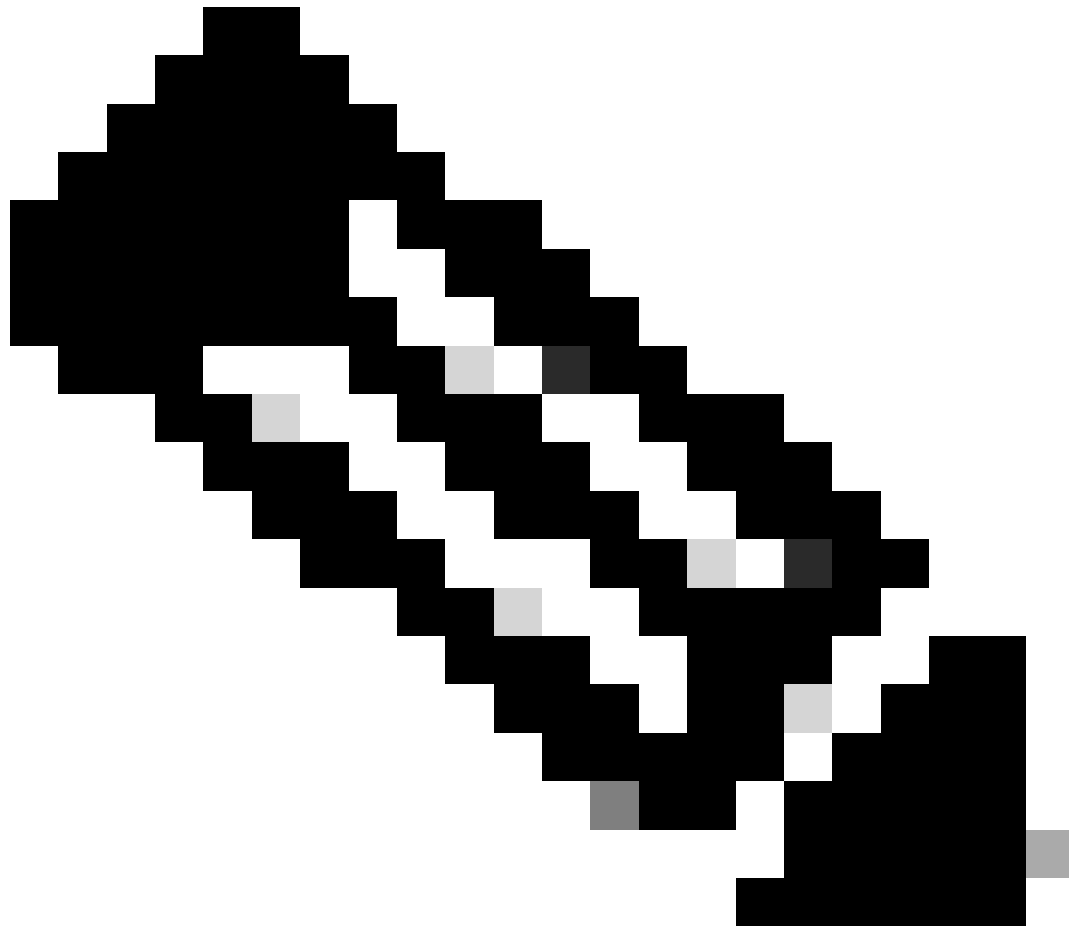
ططخملل حرش

- نم ةهجوم ةهجاوك N9K-1 ىلع ETH1/1 ةهجاو نيوكت متي N9K-2 عم L3 لاصتا هيذل N9K-1 ةمالع عضو مت يتي L2 switchport ةهجاو يه N9K-2's ETH1/1 امنېب ، ثلثال ىوتسمال VLAN 10 عم اهيلع
- L2 ةهجاو يه N9K-2 ىلع ETH1/3 ةهجاو N9K-3 عم L3 لاصتا ىلع N9K-2 ىوتحي امك نيوكت متي و ، 20 مقرر VLAN ةكبش مادختساب اهيلع ةمالع عضو مت يتي switchport L3 زارط ةهجوم ةهجاوك N9K-3 ب ةصاخل Eth1/4 ةهجاو
- مادختسا بجي . ةنوكمل Lo0 ةهجاو ىلع N9K-2 و N9K-1 نم لك ىوتحت : عاجرتسال نيوكت نېزاهجل نېب ICMP لاصتا رابتخا مزحل لاسرال هذو Lo0 تاهجاو

اهحالصإو عاطخالل فاشكتسا

اهتحص نم ققحتلالو PACL و RACL نيوكتل ةيليصفتل ةيلمعل تاوطخ ىلع روثلعل اعارل ذفنملا ىلإ لوصولل ي ف مكحتل مئاق ةعجارم متي ، ةيلمعل هذو لالحو N9K. زهجا ىلع لاسرا متي ناك اذا ام ديدحتو ةمزحل قفدت ليلحتل هجوملا ىلإ لوصولل ي ف مكحتل مئاقو و حېحص لكشېب اهل ابقتساو مزحل اعيمج

SVI 10 و N9K-2 (SVI 10 و N9K-1 (ETH1/1) نم L3 تاهجاو ىلع RACL نيوكت 1. ةوطخل N9K-3 (ETH1/14) و (20



لوصول إلى مكدت عملاق نيوكت مزل، ةرداصل الةمزلال قفدت ةبقارمل :ةطالال
نم ةيدامل الةهجوم الةاهاول الةل رقتفت N9K-2 نأل ارطن .N9K-2 لعل ةيفاضا (ACL)
نإف ، SVI و L2 switchport تاهاول لعل ةوتحت اهانف ،كلذ نم الةب) ثلثال ةوتسمل
طقف ةدراوال رورمل الةكرح معدت (PACL) ذفنملاب ةصاخال لوصول الةل مكدتال عملاق.

ةديء (ACL) لوصول الةل مكدت عملاق ءاشنل نكمي ،ةرداصل الةمزلال تاقباطت طاقثلال
L3. تاهاول لعل اهقبطتو

N9K-1 و N9K-2 و N9K-3 لعل (ACL) لوصول الةل مكدتال عملاق ققبطت مئي

```
ip access-list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any
```

```
ip access-list TAC-OUT
```

```
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any
```

N9K-1

```
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown
```

N9K-2

```
interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.10.1/30
```

```
interface Vlan20
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.20.1/30
```

N9K-3

```
interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

يُستخدم (PACL) لمنع الوصول إلى مكدس التوجيه في مكدس التوجيه 2. ويطبق على L2 Switchport J N9K-2

تكوين TCAM

تتمثل العملية في تكوين (ACL) للوصول إلى مكدس التوجيه في مكدس التوجيه 2. ويطبق على L2 Switchport J N9K-2. ويطبق على L2 Switchport J N9K-2.

[تكوين TCAM على Nexus 9000](#)

تتمثل العملية في تكوين (PACL) لمنع الوصول إلى مكدس التوجيه في مكدس التوجيه 2. ويطبق على L2 Switchport J N9K-2. ويطبق على L2 Switchport J N9K-2. ويطبق على L2 Switchport J N9K-2.



افىظن جارخإلأءاقبإل فوفصلأضعب ةلازا تمت :ةظحالـ

```
N9K-C93180YC-2# conf
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2
N9K-C93180YC-2(config-if)# ip port access-group TAC-IN in
ERROR: TCAM region is not configured. Please configure TCAM region Ingress PACL [ing-ifac1] and retry t
N9K-C93180YC-2(config-if)#
```

TCAM ةقطنـ نيوكـ ءارجإ

TCAM ةقطنـ ءالـ ءعت 1. ةوطخلأ

لكل لكـ فلـتـخي نأ نكـمي شيـح، ءرح ءحاسـم ريـفوت اهنـكـمي يتـلأ ةقطنـمـلأ ميـيـقت ءارجلأ
ةئـيـب.

N9K-C93180YC-2# show system internal access-list globals

slot 1
=====

LOU Threshold Value : 5

INSTANCE 0 TCAM Region Information:

Ingress:

Region TID Base Size Width

NAT 13 0 0 1
Ingress PACL 1 0 0 1 >>>>>> Size of 0
Ingress VACL 2 0 0 1
Ingress RACL 3 0 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 1792 256 1
Ingress L3/VLAN QOS 6 2048 512 1 >>>>>> Size of 512
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1

Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region

ققحتلل ليدب بولسأ.

```
N9K-C93180YC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
Ingress PACL [ing-ifacl] size = 0 >>>>>> Size of 0
VACL [vac1] size = 0
Ingress RACL [ing-rac1] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 512 >>>>>> Size of 512
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-rac1] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vac1-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C93180YC-2#
```

ةقطنمالمجج ليلقت 2: ةوطخال

(ةئيب لكل اذه فلتخي). ing-l3-vlan-qos ل ةصصخمالمةقطنمالمجج ليلقتب مق

N9K-C93180YC-2(config)# access-list tcam area ing-l3-vlan-qos 256 >> صيصختلال ليلقت 256. الى 512 نم

نيوكتال يرسى لكل ماظننالمجحت ةداعاوينيوكتال ظفح يجرى.

ةقطنمة TCAM ل ing-ifacl ةوطخال 3.

N9K-C93180YC-2(config)# hardware access-list tcam region ing-ifacl 256

نيوكتال يرسى لكل ماظننالمجحت ةداعاوينيوكتال ظفحب مق

N9K-C93180YC-2(config)#

نڤيوكتال ظفح 4. ةوطخال

```
N9K-C93180YC-2(config)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
N9K-C93180YC-2(config)#
```

لڤمحتال ةداعا 5. ةوطخال

```
N9K-C93180YC-2(config)# reload
This command will reboot the system. (y/n)? [n] y
```

لڤمحتال ةداعا دعب ققحتال

تارڤيغتال ناڤرس نم ققحت، لڤمحتال ةداعا دعب

```
N9K-C93180YC-2# sh system internal access-list globals
```

```
slot 1
=====
```

```
-----
INSTANCE 0 TCAM Region Information:
-----
```

```
Ingress:
-----
```

```
Region TID Base Size Width
-----
```

```
NAT 13 0 0 1
Ingress PACL 1 0 256 1 >>> The size value is now 256.
Ingress VACL 2 0 0 1
Ingress RACL 3 256 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 2048 256 1
Ingress L3/VLAN QOS 6 2304 256 1 >>> The size value is now 256.
```

```
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1
```

Total configured size: 4096

Remaining free size: 0

Note: Ingress SUP region includes Redirect region

ققحتلل ليدب بولسأ.

N9K-C93180YC-2# sh hardware access-list tcam region

NAT ACL[nat] size = 0

Ingress PACL [ing-ifacl] size = 256 >>> The size value is now 256.

VACL [vac1] size = 0

Ingress RACL [ing-racl] size = 1792

Ingress L2 QOS [ing-l2-qos] size = 256

Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 256 >>> The size value is now 256.

Ingress SUP [ing-sup] size = 512

Ingress L2 SPAN filter [ing-l2-span-filter] size = 256

Ingress L3 SPAN filter [ing-l3-span-filter] size = 256

Ingress FSTAT [ing-fstat] size = 0

span [span] size = 512

Egress RACL [egr-racl] size = 1792

Egress SUP [egr-sup] size = 256

Ingress Redirect [ing-redirect] size = 0

Egress L2 QOS [egr-l2-qos] size = 0

Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0

Ingress Netflow/Analytics [ing-netflow] size = 0

Ingress NBM [ing-nbm] size = 0

TCP NAT ACL[tcp-nat] size = 0

```

Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C93180YC-2#

```

IP ذفنم ىلى لوصول ةعومجم نيوكت

يناثل لىوتسمال نم ةيدامال تاهجاوال ىلى IP ذفنم ىلى لوصول ةعومجم نيوكتب مق

```

N9K-C93180YC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2,e1/51
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress direction >>>>>>>
N9K-C93180YC-2(config-if-range)#

```

```

interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown

```

```

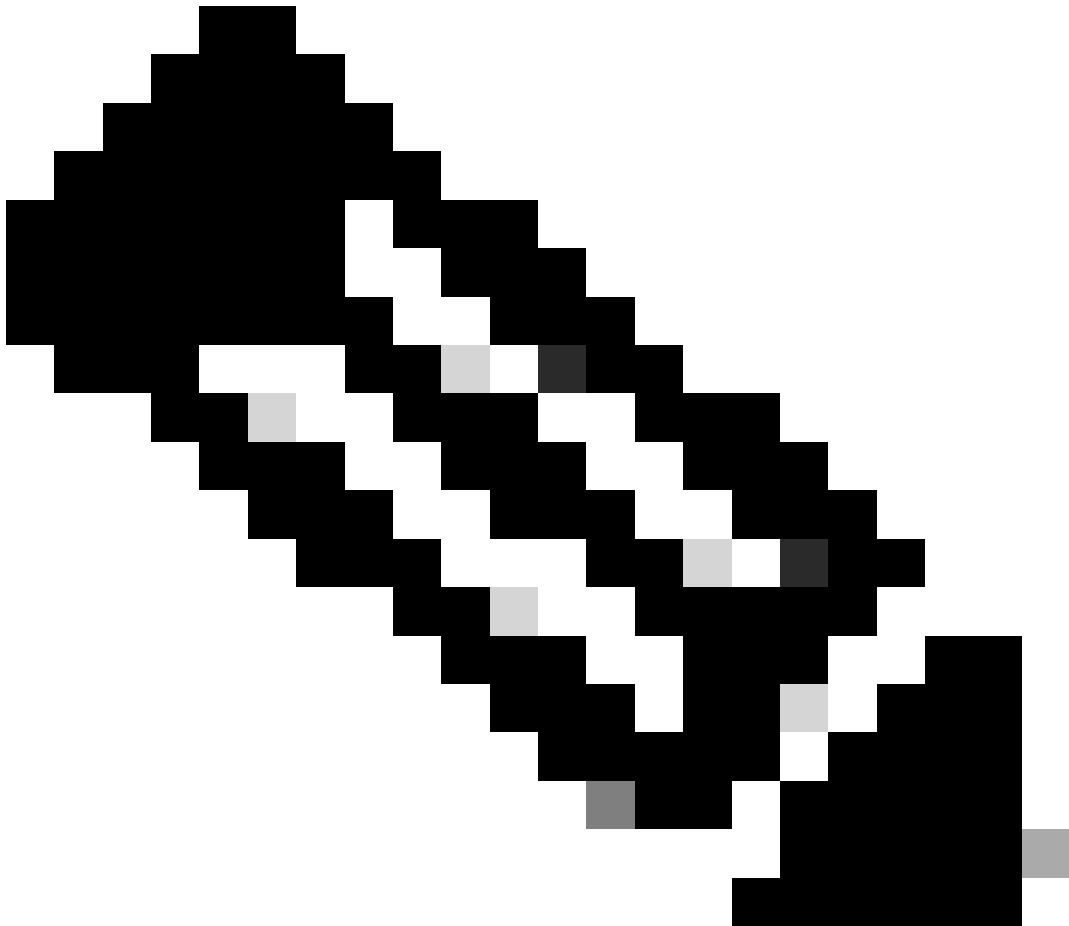
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> Inboud only
no shutdown

```

عاجرتسإ 3. ةوطخال

مادختسإ N9K-3 ل نكمي امنبي، ردصمك اهب صاخال N9K-1 Loopback0 (Lo0) مدختست
 ةياغك اهب صاخال Loopback0 (Lo0).

رابتخال اضارغل اهمدختست يتل عاجرتسال تاهجاوال هليغشت يراجال نيوكتل حيضوت متي



هيجوت لوكوتورب مادختساب اقبس م 3 ةقبطلا لاصتا نيوكت مت :ةظالم

```
***N9K-1***
interface loopback0
ip address 192.168.0.10/32
```

```
***N9K-3***
interface loopback0
ip address 10.10.10.10/30
```

مادختساب N9K-3 نم لاصتا رابتخا لاسراو رورم ةكرح عاشناب مق 4. ةوطخلا
N9K-1 نم Lo0 192.168.0.10 ىلإ IP 192.168.20.2 ردصملا

```

N9K-3# ping 192.168.0.10 source 192.168.20.2
PING 192.168.0.10 (192.168.0.10) from 192.168.20.2: 56 data bytes
64 bytes from 192.168.0.10: icmp_seq=0 ttl=253 time=1.163 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=253 time=0.738 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=253 time=0.706 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=253 time=0.668 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=253 time=0.692 ms

--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.668/0.793/1.163 ms
N9K-3#

```

و N9K-2 و N9K-1 لوح RACL و PACL تايئاصحإ تامولعم نم ققحتلا 5. ةوطخل N9K-3

- تابلط مزح يقلت نم ققحتلا يرورضلا نمف، N9K-3 نم اهؤاشنإ متي ICMP مزح نأ امب N9K-2. ةطساوب سمخلل ICMP.
- نم N9K-2 ىلع (PACL) ذفنم لاب ةصاخلا لوصولي ف مكحتلا ةمئاق نم ققحتلا نوكت ثيحب، (N9K-3 نم ETH1/4) 192.168.20.2 نم أشنت مزح سمخ مالتسا عقوقتملا N9K-1'Lo0 (192.168.0.10) ةهوجل.

```

N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]

```

N9K-2 نم ETH1/3 في ةلصل وذي نوكتلا

```

interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> PACL
no shutdown

```

- N9K-1 ىلى اههيجوت ةداعإ راجو N9K-2 ةكرات ICMP تابلط مزح 5 نع RACL غلبت، N9K-2 في 1.
- رداصللا هاجتإلا معدت ال (PACL) ذفنم لاب ةصاخلا لوصولي ف مكحتلا ةمئاق نأ امب، متي تلى رخلآا (TAC-OUT-SVI) لوصولي ف مكحتلا ةمئاق نم ققحتلا يرورضلا نمف لوصولي ف مكحت ةمئاقك اهنوكت متي تلى او، VLAN 10 ةكبشل SVI ىلى اهنوكت

يُف محركات المواءمة على موعدم رداصل الهاجإلأ نأل ارطن) (RACL ذفملماب ةصاخلا
N9K-1 و N9K-2 نيب لاصتالا VLAN 10 ةكبش رفوت. (RACL) ذفملماب ةصاخلا لوصولا

```
N9K-2# show ip access-lists TAC-OUT-SVI
```

```
IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

configuration associated:

```
interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>>>
ip address 192.168.10.1/30
```

مت يتال ICMP بلط مزح عم مزح نادقف يا دوجو مدع ديكأت مت ،ةقباسلا جئاتنلإ إلإ ادانتسا
N9K-3 نم اهلأسرا

- نم ققحتلاو (N9K-1 ةهجولا) يلاتل زاهجلا إلإ ةعباتملا ي في ةيلاتلا ةوطخل لثمتت
N9K-3 نم ICMP تابلط مزح ددع سفن يقلت
- N9K-3 نم ICMP تابلط مزح 5 لاسراب موقي N9K-2 نأ إلإ RACL تايئاصحإ ريشت

```
N9K-1# show ip access-lists TAC-IN
```

```
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

N9K-1 نم ETH1/1 في ةلصلال وذيوكتل

```
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>> RACL
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown
```

- N9K-3 نم (ICMP بلط) مزحلل دقف يأ دوجو مدع نم دكأتال مت ، تامولعمل إلى إادانتسا إلى N9K-2. 192.168.0.10 إلى Lo0
- N9K-1 Lo0 نم أشنت يتال ICMP إلى درلا مزح بقعت يف ةللالات ةوطخل لثمتت 192.168.20.2. 192.168.0.10 إلى ةهجومالو N9K-3
- درلا مزح يقلت تناك إذا امم ققحتالو N9K-2 إلى لاقتنال يرورضل نم ، كلذ دعبو 192.168.20.2. إلى 192.168.0.10 نم ICMP لوكتوربل سمخل
- لوصولا يف مكحتال ةمئاق نم ققحتال مزلي ، N9K-1 نم ICMP إلى درلا مزح بقعتل لوصولا ETH1/1. إلى اهنيوكت مت يتال (TAC-IN) ذفنملاب ةصاخال

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp reply coming from 192.168.0.10 to 192.168.20.2
30 permit ip any any [match=0]

interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> PACL (Inbound direction only)
no shutdown
```

- مزح نادقف يأ دوجو مدع نم دكأتال مت ، اقبس م اهم يدقت مت يتال تامولعمل إلى إادانتسا إلى N9K-2. N9K-1 نم رورمل ةكرح إلى
- حيحص لكشب ICMP در مزح لسري N9K-2 نأ إلى ديكأتال يف ةللالات ةوطخل لثمتت هاجتإل معدت ال (PACL) ذفنملاب ةصاخال لوصولا يف مكحتال ةمئاق نأ امبو. N9K-3 إلى (TAC-OUT-SVI) رخأل لوصولا يف مكحتال ةمئاق نم ققحتال يرورضل نم ف ، رداصل يف مكحت ةمئاقك اهنيوكت مت يتالو ، VLAN 20 ةكبشل SVI إلى اهنيوكت مت يتال يف مكحتال مئاق إلى لموعدم رداصل هاجتإل نأ ثيح) (RACL) ةكبش إلى لوصولا N9K-2 و N9K-3 نيب لاصلتال VLAN 20 ةكبش رفوت. (RACL) ذفنملاب ةصاخال لوصولا

```
N9K-2# show ip access-lists TAC-OUT-SVI
IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 ICMP reply packets are being sent out to 192.168.0.10
```

ةلصلال يذنيوكتال:

```
interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>> RACL outbound direction
```

```
ip address 192.168.20.1/30
```

N9K-1 نأ نم دكأتال مت، هالغأ جارخال نم (ACL) لوصولا يف مكحتال عمئاق تادادع ىلإ ادانتسا N9K-2. ىلإ حيحص لكشب ICMP بةصاخال سمخال درال مزح لاسراب موقى

- N9K-3 ىلإ N9K-2 نم ثدحى مزحلل دق فىأ دجوى ال
- اذا ام ققحتالو، N9K-3، رورمالا كرح ردصم ىلإ عباتملا يف عئاهنلا عوطخال لثمتت ICMP. ىلعل سمخال درال مزح ىقللت تناك
- N9K-1 Lo0 نم عدرالو ICMP دودرل ACL TAC-In ىلإ لصت سمخال ICMP مزح نأ دكؤملا نم (192.168.0.10).
لابقتسالل لوصولا يف مكحتال عمئاق عجارم ىرورضلا نم، قىقحتال نم دىزمللو (TAC-IN) ىف ETH1/4.

```
N9K-3# sh ip access-lists TAC-IN
```

```
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp replies coming from Lo0 N9K-1
30 permit ip any any [match=0]
```

ةلصلال ذىوكتال:

```
interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>>
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

- ققحتال مت، اقبسما هدىدحت مت ىتال اهالصلإو عاخالأ فاشكتسأ تاوطخ مادختساب
ةوجلل و ردصملا نىب لجنج ساسأ ىلعل عمزحلل رداصلالو درال راسملا عحص نم

ICMP مزح عىمى قىلت مت هنأل ارظن مزحلل نادقف فىأ دوجو مدع دىكأت مت، لاثملا لىبس ىلعل زاهج لك ىلعل حيحص لكشب اههچوت عداعإو سمخال

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا