

لوصول في مكحلتا عمئاق تادادع مهف ىلإ ةدنتسم ال VPN قافنا لخاد ريفشتلل ةسايسلا

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[طخملا](#)

[تاهوي رانيسلا](#)

[طش ن ريغ VPN قفن نوكي امنيب 1 هجوملا نم رورملا ةكرح تأدب :لوالا ويراني سلا](#)

[طش ن VPN قفن دوجو عانتأ 2 هجوملا نم رورملا ةكرح تأدب :يناثالا ويراني سلا](#)

[ن يوك تالا](#)

[1 هجوملا ىلع ريفشتلا ن يوك ت](#)

[2 هجوملا ىلع ريفشتلا ن يوك ت](#)

[قافنا لخاد ريفشتلل لوصول في مكحلتا عمئاق تادادع ل يكل سلا ليلحتلا VPN](#)

[طش ن ريغ VPN قفن نوكي امنيب 1 هجوملا نم رورملا ةكرح تأدب :لوالا ويراني سلا](#)

[طش ن VPN قفن دوجو عانتأ 2 هجوملا نم تأدب يتالا رورملا ةكرح :يناثالا ويراني سلا](#)

[نراقلا](#)

[ةيسيسئلا دئافلا](#)

ةمدقملا

قافنا لخاد (ACL) ريفشتلل لوصول في مكحلتا عمئاق تادادع كولس دنتسملا اذه فصي
ةسايسلا ىلإ ةدنتسم ال VPN.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا تاعوضوملا ةفرعمب Cisco ي صوت

- Cisco IOS® /Cisco IOS® XE يساسألا ماظنلا ىلع VPN عقوم ىلإ ةسايسلا ىلإ دنتسم عقوم
- Cisco IOS/Cisco IOS XE يساسألا ماظنلا ىلع لوصول في مكحلتا مئاق

ةمدختسملا تانوكملا

ة.فلتخم

نيوكتالا

تاهجوم نيب عقوم ىلا عقوم نم لصتيو ةسايسلا ىلا دنتسم VPN قفن نيوكتاب انمق
Cisco C8KV، عارظنك ني فنصمو، "csr2" مسا 2 هجوملا ىلع قلطي و "csr1" 1 هجوملا ىمسي.

1 هجوملا ىلع ريفشتلا نيوكت

```
csr1#sh ip int br
Interface      IP-Address      OK?  Method  Status  Protocol
GigabitEthernet1  10.106.62.62    YES  NVRAM    up       up
GigabitEthernet2  10.106.67.27    YES  NVRAM    up       up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
  set peer 10.106.44.144
  set transform-set new_ts
  set ikev2-profile new_profile
  match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
  10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
  20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
  30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...
```

Current configuration : 162 bytes

```
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

2 هجوملا ىلع ريفشتلا نيوكت

```
csr2#sh ip int br
Interface      IP-Address      OK?      Method      Status      Protocol
GigabitEthernet1  10.106.44.144   YES      NVRAM       up          up
GigabitEthernet2  10.106.45.145   YES      NVRAM       up          up
GigabitEthernet3  10.106.46.146   YES      NVRAM       up          up
GigabitEthernet4  10.106.63.13    YES      NVRAM       up          up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
  set peer 10.106.62.62
  set transform-set new_ts
  set ikev2-profile new_profile
  match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
  10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
  20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
  30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

لوصول الي ف م كحتال ةمئاق تاداعل ي كولسلال لي لحتال VPN قافنأ ل خاد ري ف شتلل

(ACL) لوصول الي ف م كحتال ةمئاق ىل لوصول تارم ددع ني زاهجال الكل نو كي ، ةي ادبل الي
امه ب ةصاخال ري ف شتلل لوصول ةمئاق ىل ع رفس

```
csr1#sh access-lists new_acl
Extended IP access list new_acl
  10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
  20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
  30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#

csr2#sh access-lists new_acl
Extended IP access list new_acl
  20 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
  30 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
  40 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
csr2#
```

ني ري ظنل ني زاهجال الك ىل ع مه ب ةصاخال ري ف شتلل لوصول ةمئاق ىل ع رفس ددع لوصول الي ف م كحتال ةمئاق رهظت

ريغ VPN قفن نوکي امنيب 1 هجومال نم رورمال ةکرح تادب :لوالا وييرانيسلا طشن

ة:لوالا ةلالا:

طشن ريغ (IP: 10.106.45.145) 2 هجومال او (IP: 10.106.67.27) 1 هجومالاب لصتي يذلا VPN قفن ايلاح.

ذختمل اءارال:

2. هجومال عم لاصتا عاشن فدهب ، 1 هجومال نم رورمال ةکرح ادب متي

تاطحال م:

1. (ACL) لوصولي ف مكحتل ةمئاق دادع كولس:

في مكحتل ةمئاق دادع في ةطوالم ةدايز كانه ، 1 هجومال نم رورمال ةکرح ادب دنع .أ. لواحي يتل ةطحلل في طقف ةدحاو ةرم ةدايزل هذه ثدحت .1 هجومال يلع (ACL) لوصول عاشن قفنل اهيف .

يلع يريصح لكشب (ACL) لوصولي ف مكحتل ةمئاق دادع في عافتلالا ةطحال م مت .ب. في تاريغيغت يا 2 هجومال سكعي ال .وييرانيسلا اذه في 1 هجومال وهو ،يديهمتل هجومال ةلحرمال هذه في هب صاخلا (ACL) لوصولي ف مكحتل ةمئاق دادع .

2. قفنل عاشن:

لوالا نيب قفنل عاشن حاجن م مت ،رورمال ةکرح ادبل ةلباقمال ةيلوالا ةدايزل دعب .أ. 2 هجومال او

الو 1 هجومال يلع (ACL) لوصولي ف مكحتل ةمئاق دادع رقتست ،قفنل عاشن دعب .ب. في مكحتل ةمئاق ةدعاق ةقباطم مت هنا يل ريشي امم ،ةيفاضا تاداي زيا رهظي .تباث لكشب مئاقلا قفنل ربع رورمال ةکرح نال حمست يهو ،(ACL) لوصول

3. قفنل ادب ةداع:

طقس اذا طقف ىرخا ةدايز 1 هجومال يلع (ACL) لوصولي ف مكحتل ةمئاق دادع ربتخي ةمئاق ةدعاق ليغشت متي هنا يل ريشي اذهو .عاشنالا ةداعا بلطتي ناكو قفنل ،قفنل عاشن لواحت يتل ةيلوالا رورمال ةکرح ادب لال خ نم (ACL) لوصولي ف مكحتل اطن قفنل نوکي نا درجمب رمتسمال تانايبلا لقن نم الدب .

1 هجومال يلع (ACL) لوصولي ف مكحتل ةمئاق دادع نا وييرانيسلا اذه حضوي ،راصتخاب قفن ليغشت درجمب اثباث لظي هنكلو قفنل عاشنالا ةيلوالا رورمال ةکرح تالواحمل ساسح VPN هليغشتو .

```

csr1#ping 10.106.45.145 source 10.106.67.27
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.106.45.145, timeout is 2 seconds:
Packet sent with a source address of 10.106.67.27
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
csr1#
csr1#
csr1#sh access
csr1#sh access-li
csr1#sh access-lists new_acl
Extended IP access list new_acl
10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
csr1#
csr1#
csr1#
csr1#ping 10.106.45.145 source 10.106.67.27
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.106.45.145, timeout is 2 seconds:
Packet sent with a source address of 10.106.67.27
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
csr1#
csr1#sh access-lists new_acl
Extended IP access list new_acl
10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#

csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#sh access
csr2#sh access-li
csr2#sh access-lists new_acl
Extended IP access list new_acl
20 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
30 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
40 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#
csr2#sh access-lists new_acl
Extended IP access list new_acl
20 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
30 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
40 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
csr2#
csr2#
csr2#

```

1 ايراي نيس

VPN ق فن دوجو ءانثأ 2 هجومال نم تآدب يتال رورمال ءكرح:يناثال ويرانيسال طشن

ة:لوال ءالاحل:

ةطشن (IP: 10.106.45.145) 2 هجومال او (IP: 10.106.67.27) 1 هجومال لب لصتي يذل VPN ق فن ي.الاحل تقولا ي ف ءيلغشتو

ذختمل ءارال:

1. ق فنل ليغشت ءانثأ 1 هجومال ل 2 هجومال نم رورمال ءكرح ءدب متي .
2. (هطبض ءداع و) ادمع ق فنل حسم متي ،كلذ دعبو .
3. ءاشنل ءداعال ىرخأ ءرم تانايبل رورم ءكرح ءدب 2 هجومال موق ي ،قفنل حسم دعب .للاصتال .

تاطاحلم:

1. ء:لوال رورمال ءكرح ءدب :

رييغت دجوي ال ،لعفلاب ق فنل ءاشنل ءانثأ 2 هجومال نم ءرم لوال رورمال ءكرح ءدب دنع أ .

(ACL) لوصول ي ف مكحتل ءمئاق ددع ي ف يروف

ل ي دؤي ال لعفلاب هؤاشنل مت ق فن لخد ءرمتسمل رورمال ءكرح نأ ل يريشي اذهو .ب

(ACL) لوصول ي ف مكحتل ءمئاق ددع ءدايز
2. هلغشت ءداعو ق فنل حسم :

تقؤم لكشب 2 هجومال لوال نيب ددحمل للاصتال لي طعت متي ،قفنل حسم دنع أ .

ةقحال رورم ءكرح ي ءةلمع سيسيأت ءداع كلذ بلطتيو

ةطحالم لل ءلباق ءدايز دجوت ،قفنل حسم دعب Router2 نم رورمال ءكرح ءدب ءداع دنع .ب

متي هنأ ل ءدايزل هذه ريشت .2 هجومال لعل لوصول ي ف مكحتل ءمئاق ددع ي ف

قفنل ءاشنل لي هستل ىرخأ ءرم لوصول ي ف مكحتل ءمئاق ددع ي ف ضوافتل
3. (ACL) لوصول ي ف مكحتل ءمئاق ددع لي صافت :

موق ي يذل بنال لعل طقف (ACL) لوصول ي ف مكحتل ءمئاق ددع ي ف ءدايزل ثدحت

بيجستسي 2 هجوم الى لوصولي ف م كحتلا عمئاق دادع نأ ويرانيسيلا اذه حضوي ،راضتخاب
 فيداعلا رورملا كرح قفدت عم دادعلا ديازتي الو. VPN قفن عاشن اذاعا دنع رورملا كرح ادبل
 عبتتلا نمضي امم ،قفنلا عاشن اذاعا الى اذاحلا عم لعافتي هنكلو طشن قفن لخاد
 قفنلا ادب اذاحال قيقدلا.

```

csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#sh access-lists new_acl
Extended IP access list new_acl
 10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
 20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
 30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#
csr1#sh access-lists new_acl
Extended IP access list new_acl
 10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
 20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
 30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
csr1#
csr1#sh access-lists new_acl
Extended IP access list new_acl
 10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log (1 match)
 20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
 30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
csr1#
csr1#

```

رارقلا:

تارم ددع يف ةدايزلا ةطحالم متت ،Router1 نم قفنل ادب متي امدنع :ئدابلاب ةصاخلا ةدايزلا لوصول تارم ددع عف تري ،Router2 نم ادبلا ثدح اذا ،لثملابو . Router1 ىلع طقف لوصول ةبقارم يف (ACL) لوصول يف مكحتلا ةمئاق رود ىلع عوضلا طلسي اذهو . Router2 ىلع طقف ردصملا يف رورملا ةكرح ادب ةيلمع .

في مكحات التأميق اتادع يقبت، حاجنب قفنل اءاشنل درجب :سئسأتلل دعب رارقتسالل
ءاطخألل نم دئزم ثودح مدع إلل رئشئ امم، رئئغئ نود نئرنظنل الك إلل (ACL) لوصولل
رورمل الك دعب قلولاحم مئتو، هئئئعت قءاعل وأ قفنل احسم مئئئ ىتحر رارقتسالل اءه رمئتسئو
ئخأ قرم
قؤلوالل قلحرملل بققعت ئل لوصولل ئل مكحاتل مئأوق فئأظوئلل كؤلسلل اءه دكؤئ

قفننللا لخاد قحلالل تانايبلا قفدت ريثأت مدع نمضي امم ،اهي ف مكحتلاو قفننلا عاشننلا
اياحضللا دادعأ ىلع هؤاشنن مت يذلا

ةيسيئرلا دئاوللا

لوصولا ي ف مكحتلا ةمئاق تادادع موقت (ACL) لوصولا ي ف مكحتلا ةمئاق دادع كولس
ىل ريشي اذهو .قفننلا ادب ةيلمع ءانثأ ئدابلا بناج ىلع يرصح لكشب تادايزلا ليحسب
قفننلا عاشنن ليغشتب موقت يتلا ةيلوالا رورملا ةكرح ةبقارملا ةممصم تادادعلا نأ

مكحتلا ةمئاق تادادع لظتس ،هنوكتو قفننلا طيشنت درجمب :ةتباثلا تادادعلا عاشنن دعب
مزليو قفننلا نييعت ةداعإ مت مل ام رخآ طاشنن يأسكعت ال يهو .رييغت نود لوصولا ي ف
ةيلوالا رورملا ةكرح ثادحأ ىلع زيكرتلا دكؤي امم ،هليغشت ةداعإ

ةصاخ (ACL) لوصولا ي ف مكحتلا ةمئاق ىل لوصولا تارم دادعأ دعت :رورملا ةكرح ادب ديدحت
بناجلل قيقدلا عبتتلا ديدحتلا هذه نمضت .قفننلا ليغشتب موق يذلا ريظنلاب
مكحتلاو ةبقارملا ةقذب حمسي امم ،VPN لاصتا ادب نع لوؤسملا

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي 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 ي 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل آل ا 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 م ا ة 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