

عقوم ىلإ عقوم نم FlexVPN ق فن نيوكت IP ناو نع مادختساب ريظن مادختساب يكي مانيد

تايوت حمل

[عمدقم](#)

[سياسات ابلطت](#)

[تابلطت](#)

[عمدختسمل تانوكم](#)

[سياسات امولعم](#)

[كبش لىطىطختل مسر](#)

[تانويوتل](#)

[رقملا هجوم لىع نيوكتل](#)

[يعرف هجوم نيوكت](#)

[هيجوتل نيوكت](#)

[رقملا هجوم لىمكل نيوكتل](#)

[يعرفل هجوم لىمكل نيوكتل](#)

[قحصلا نم ققختل](#)

[اهجالص او اعاطخ افاشكتسا](#)

[قحص تاذا امولعم](#)

عمدقم

تاهجوم نيوب عقوم ىلإ FlexVPN عقوم نم VPN ق فن نيوكت ةيفيكي دنتسمل اذه فصى
يكي مانيد IP ناو نع ديعبل ريظنل نوكي ام دنع Cisco 2.

سياسات ابلطت

تابلطت

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- FlexVPN
- IKEv2 لوكوتورب

عمدختسمل تانوكم

ةيلاتل ةيدامل تانوكملاو اوجماربل تارادصل ىلإ دنتسمل اذه في ةدراول امولعملا دنتست:

- CSR1000V زاهاج

- 17.3.4 رادصلال، Cisco IOS® XE، جم انرب

ةصاخ ةي لمعم ةئيبي ف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تأدب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتل ديقتك تكبش

ةيساسأ تامولعمل

ةكبش ل ل يطيختل مسرل



يكيما نيديلا ريظنلا ططخم

ةهجاو يلع يكيما نيدي IP ناو نع هيديل رخآ Cisco هجومو Cisco هجوم لاثملا اذه يف ططخملا حضوي هبة ةصاخلا ةماعلا ةهجاولا

تانيوكتل

امدنع Cisco هجوم يلع عقوم يلا عقوم نم FlexVPN قفن نيوكت ةي فيكي مسقلا اذه فصوي يكيما نيدي IP ناو نع ديعلال ريظنلا مدختسي

عمو (PSK) pre-shared-key هي ةمدختسمل ةقداصلما ةقيرط نوكت، اذه نيوكتل لاثم يف اضيا (PKI) ماعلا حاتفم لل ةيساسألا ةينبال مادختسا نكمي، كلذ

رقملا هجوم يلع نيوكتل

ةزيم لمعت. هجوملا نم IKEv2 ل ةي كذلا ةيضا رتفال ادادعإل مادختسا مت، لاثملا اذه يف مظعم ةي طغت لالخم نم FlexVPN نيوكت لي لقت يلع IKEv2 ل ةي كذلا ةيضا رتفال ادادعإل مادختسا لالخم مادختسا لالخم ل IKEv2 ل ةي كذلا ةيضا رتفال ادادعإل صي صخت نكمي. مادختسا لالخم لي وخت ةسايس ةي كذلا ةيضا رتفال ادادعإل نمضتت. كلذب ي صوي ال هنا مغر، ةني عم ةعومجمو، (IPsec) تنرتنإل لوكتورب نامأ فيرعت فلم، IKEv2، جهن، IKEv2، حرتقم، IKEv2، ةعومجمو، IPsec لي وحت

هاندا ةجردملا رماوأللا ليغشت كنكمي، كزاهج يف ةيضا رتفال ميقلا ةعجارمل

- ريفشتلل IKEv2 لي وخت جهنل يضا رتفال ادادعإل راهظا
- ريفشتلل حرتقم يضا رتفال راهظا
- ريفشمل IKEv2 جهنل يضا رتفال ادادعإل راهظا
- يضا رتفال show crypto ipSec profile

- show crypto ipSec transform-set default

IKEv2 حيتافم ةق لحن نيوكتب مق 1 ةوطخال

- هنوكل ارظن ريظنل IP ناوع فرعي ال يسيئرلا زكرملا هجوم نأل ارظن، ةلاجل هذه في IP ناوع ياعم اهقباطي يتل ةيوهلا نإف، ايكيميانيدي
- ةيحلحمل او ةيديبل حيتافملا نيوكتب مت امك
- فعض يانبحتل ةيوق حيتافم كالتما ي صوي

```
crypto ikev2 keyring FLEXVPN_KEYRING
peer spoke
address 0.0.0.0 0.0.0.0
pre-shared-key local Cisco123
pre-shared-key remote Cisco123
```

ةبسا حمل او ضيوفتلاو ةقداصلما جذومن نيوكتب مق 2 ةوطخال (AAA).

- اذهب لاصتالا مهنكمي نيذلا نيمدختسملل ةرادلا لمع راطا ءاشنإ ل اذ ي دؤي ليثمل
- ةيحلحمل تانايبلا ةدعاق ل جذومنلا ريشي، زاهلا اذ نم لاصتالا ضوافت ادبل ارظن نيولوخمل نيمدختسمل ديحتل هب ةصاخلا

```
aaa new-model
aaa authorization network FLEXVPN local
```

IKEv2 فيرعت فلم نيوكتب مق 3 ةوطخال

- دحم IP ناوع مادختسا كنكمي ال، ايكيميانيدي ديبل ريظنل IP ناوع ناضارتفاب ريظنل فيرعتل
- دحم لاحتفملا فرعم أو FQDN أو لاجملا بسح ديبل ريظنل فيرعت كنكمي، كلذعمو ريظنل زاهج ل
- فلم ليوختلا ةقيرطل (AAA) ةبسا حمل او ضيوفتلاو ةقداصلما ةعومجم ةفاضا مزلي ةمدختسمل ةقيرطل اليه PSK دحت يتل فيرعتل
- PKI نم الدب ققحت اهنأ ل ع دحم يه انه PKI يه ةقداصلما ةقيرط اذا
- فيرعتل فلم نإف، (dVTI) ةيكميانيدي دل ةيرهظلا قفنلا ةهجاو ءاشنإ وه فدهلا نأ امب يرهظ بل اقب طبترم اذ

```
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote key-id Peer123
identity local address 172.16.1.1
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
aaa authorization group psk list FLEXVPN default
```

virtual-template 1

IPsec فيرعت فلم نيوكت ب مق 4 ةوطخال

- يضارت فالال فيرعتال فلم مدختست مل اذا صصخم IPsec فيرعت فلم نيوكت نكمي.
- IPsec فيرعت فلم يل ع 3 ةوطخال في هؤاشن مت يذال IKEv2 فيرعت فلم نيوعت متي اذا.

```
crypto ipsec profile default
set ikev2-profile FLEXVPN_PROFILE
```

يرهاظلال بلالقل ةهجاووعاچرتسالال ةهجاو نيوكت ب مق 5 ةوطخال

- بلالقل نم dVTI ءاشن مل زي، كيماني دي IP ناووع يل ع يوتحي ديعل زاهجال نا امب.
- Virtual-Access تاهجاو ءاشن هلالخ نم متي نيوكت بلالقل هه يرهاظلال بلالقل ةهجاو ةيكي ماني دل.

```
interface Loopback1
ip address 192.168.1.1 255.255.255.0
```

```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback1
tunnel protection ipsec profile default
```

ي عرف هجوم نيوكت

فيرعت فلم و AAA جومنو IKEv2 حيتافم ةقلح نيوكت ب مق، ي عرفال هجوملل ةبس نلاب نيوكتال تاريغت عم ةقباسلال تاوطخال يل ع حجوم وه امك IKEv2 فيرعت فلم و IPsec ةيالاتل ةفوصومال تاريغتال او ةرورضال:

1. فرمك رقمال هجوم يل اهالاسرا متي يتل ةيحلحمال ةيوهال نيوكت ب مق.

```
crypto ikev2 profile FLEXVPN_PROFILE
identity local key-id Peer123
match identity remote address 172.16.1.1
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
aaa authorization group psk list FLEXVPN default
```

ةتباتل ليره اظلال قف نلال ةه جاو نيوك ت 5 ةوطخل

- يكيتات اسإ نكاس VTI ت لكش، ريغت ي الو فور عم رقم ل هجوم ل IP ناو نغ نأ ضارت فاب .

```
interface Tunnel0
ip address 192.168.1.10 255.255.255.0
tunnel source GigabitEthernet0
tunnel destination 172.16.1.1
tunnel protection ipsec profile default
```

هيجوتل ل نيوك ت

ةمئاق نيوك ت عم (SA) IKEv2 نامأ نارتقا عاش نإ ءانثأ هيجوتل ل دي دحت متي، لاثم ل اذ ه ي اضيأ كنكم ي . VPN ل ربع تلسرأ نو ك ي نأ رورم ة ك رحل ل ني ع ي اذ ه . لوصول ي ف م ك ح ت ل ل دن ت س م ل اذ ه قاطن ي ف ت س ي ل ي ه ف ك ل ذ ع م و ، ة ي ك ي م ا ن ي د ل ه ي ج و ت ل ل ت ا ل و ك و ت و ر ب ن ي و ك ت

(ACL) لوصول ي ف م ك ح ت ل ل ةمئاق دي دحت . 5 ةوطخل

يس ي ل ل رقم ل هجوم :

```
ip access-list standard Flex-ACL
permit 10.10.10.0 255.255.255.0
```

عر ف ل هجوم :

```
ip access-list standard Flex-ACL
permit 10.20.20.0 255.255.255.0
```

م ك ح ت ل ل ةمئاق ني ع ي ل ل هجوم ل ك ل ع IKEv2 ل ي و خ ت ف ي ر ع ت ت ا ف ل م ل ي د ع ت ب م ق . 6 ةوطخل (ACL) لوصول ي ف

```
crypto ikev2 authorization policy default
route set interface
route set access-list Flex-ACL
```

رقم ل هجوم ل ل م ك ل ل نيوك ت ل

```
aaa new-model
```

```
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
  route set interface
  route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
  peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
  match identity remote key-id Peer123
  identity local address 172.16.1.1
  authentication remote pre-share
  authentication local pre-share
  keyring local FLEXVPN_KEYRING
  aaa authorization group psk list FLEXVPN default
  virtual-template 1

crypto ipsec profile default
  set ikev2-profile FLEXVPN_PROFILE

interface Loopback1
  ip address 192.168.1.1 255.255.255.0

interface Loopback10
  ip address 10.10.10.10 255.255.255.255

interface GigabitEthernet0
  ip address 172.16.1.1 255.255.255.0

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback1
  tunnel protection ipsec profile default

ip access-list standard Flex-ACL
  5 permit 10.10.10.0 255.255.255.0
```

يعرف ال هجوم لل لم الك ال ني وك ال

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
  route set interface
  route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
  peer HUB
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
  identity local key-id Peer123
```

```
match identity remote address 172.16.1.1
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
aaa authorization group psk list FLEXVPN default
```

```
crypto ipsec profile default
set ikev2-profile FLEXVPN_PROFILE
```

```
interface Loopback20
ip address 10.20.20.20 255.255.255.255
```

```
interface Tunnel0
ip address 192.168.1.10 255.255.255.0
tunnel source GigabitEthernet0
tunnel destination 172.16.1.1
tunnel protection ipsec profile default
```

```
interface GigabitEthernet0
ip address dhcp
negotiation auto
```

```
ip access-list standard Flex-ACL
10 permit 10.20.20.0 255.255.255.0
```

تحصلنا من قوقحتنا

حيحصل لكشباب امهلمع و 2 ةلحرملاو 1 ةلحرملا ليغشت نم قوقحتنا بجي، قوقحتنا نم قوقحتنا

```
Headquarter#show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA
```

Tunnel-id	Local	Remote	fvr/f/ivrf	Status
1	172.16.1.1/500	172.16.2.1/500	none/none	READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: P
Life/Active Time: 86400/74645 sec
CE id: 61256, Session-id: 1
Status Description: Negotiation done
Local spi: D5129F36B1180175 Remote spi: F9298874F90BFEC7
Local id: 172.16.1.1
Remote id: 172.16.2.1
Local req msg id: 16 Remote req msg id: 31
Local next msg id: 16 Remote next msg id: 31
Local req queued: 16 Remote req queued: 31
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Dynamic Route Update: enabled
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
Remote subnets: -----> This section shows the traffic to be routed across
192.168.1.10 255.255.255.255
10.20.20.20 255.255.255.255

IPv6 Crypto IKEv2 SA

IPSec: الةناتل ةلحرمل

Headquarter#show crypto ipsec sa

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)

current_peer 172.16.2.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 225, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 225, #pkts decrypt: 225, #pkts verify: 225

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1

plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0

current outbound spi: 0xC124D7C1(3240417217)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xC2AADCAB(3265977515)

transform: esp-aes esp-sha-hmac ,

in use settings = {Transport, }

conn id: 2912, flow_id: CSR:912, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-head-0

sa timing: remaining key lifetime (k/sec): (4607993/628)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xC124D7C1(3240417217)

transform: esp-aes esp-sha-hmac ,

in use settings = {Transport, }

conn id: 2911, flow_id: CSR:911, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-head-0

sa timing: remaining key lifetime (k/sec): (4608000/628)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

UP ةلح يف يره اظلال لوصول ةهجاو نأ نم ققحتللا لىل اضى اجاتحت


```

show interface Virtual-Access1
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (192.168.1.1)
  MTU 9934 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.16.1.1, destination 172.16.2.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "default")
  Last input 20:53:34, output 20:53:34, output hang never
  Last clearing of "show interface" counters 20:55:43
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    586 packets input, 149182 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    15 packets output, 1860 bytes, 0 underruns
    Output 0 broadcasts (0 IP multicasts)
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out

```

اهحال صاوا عااطخاا فاشك ت سا

اهحال صاوا ق فنللا عاشن ا عااطخا فاشك ت سا ةي فيك مس قلا اذه حضوي

IKE: ضوافت لش ف اذا ةي لاللا تاوطلخا ل مكا

1. رما اذه عم ي لاللا ةلحالا تقود:

- show crypto ikev2 sa
- show crypto ipsec sa
- ريفش تاللا ةسلج ضرع

2. ق فنللا ضوافت ةي لمع عااطخا احي حصت ل رما وائللا هذه مدخت سا:

- debug crypto ikev2

- debug crypto ipSec

ةلص تاذا تامولعم

- [Cisco نيم تاليزن تلالاوين فللا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل