

عَضْوِلَا) IKE و ASA IPsec ءَاطْخَا حِيْحَصْت TechNote ءَاطْخَا فَاشْكْتَسَا (IKEv1) يَسِيئِرْلَا ءَاَحَالِصَاو

تَايَوْتَحْمَلَا

[قَمْدَقْمَلَا](#)

[قَسِيسَاأَلَا تَابَلَطْتَمَلَا](#)

[تَابَلَطْتَمَلَا](#)

[قَمْدَخْتَسْمَلَا تَانُوْكْمَلَا](#)

[قَسِيسَاأَلَا سَمِ](#)

[وِيْرَانِيَس](#)

[قَمْدَخْتَسْمَلَا حِيْحَصْتَلَا رَمَاوَا](#)

[ASA نِيُوْكْت](#)

[ءَاطْخَاأَلَا حِيْحَصْت](#)

[قَلِصْتَاذْتَاْمَوْلَعْم](#)

قَمْدَقْمَلَا

مَادَخْتَسَا دِنَع (ASA) فَيَكْتَلَل لِبَاقِلَا نَامَاأَلَا زَاهَج يَلَع ءَاطْخَاأَلَا حِيْحَصْت دِنْتَسْمَلَا اذَه فِصِي
قَمَجْرْت قَشْقَانِم اَضِيَا مَتْت (PSK) اَقْبَسْم كَرْتَشْمَلَا حَاتْفَمَلَاو يَسِيئِرْلَا عَضْوِلَا نَم لَك
نِيُوْكْتَلَا يَلِ ءَاطْخَاأَلَا حِيْحَصْت رُوَطَس ضَعَب.

دَعَب تَانَايِبَلَا رُوْرْم قَكْرَح دِنْتَسْمَلَا اذَه يَفَا هَتَشْقَانِم مَتْت مَلِي تَلَا عِيضَاوْمَلَا نَمضَتْت
IPsec وَا (IKE) تَنْرَتْنِإَلَا حَاتْفَمَلَا لِدَابْتَل قَسِيسَاأَلَا مِيَهَاْفَمَلَاو قَفْنَلَا ءَاَشْنِإَلَا.

قَسِيسَاأَلَا تَابَلَطْتَمَلَا

تَابَلَطْتَمَلَا

قِيلَاتَلَا عِيضَاوْمَلَا ب قَفْرَعْم دِنْتَسْمَلَا اذَه ءَارِق يَدَل نُوْكِي نَأ بَحِي.

- PSK
- كِيَا

قَمْدَخْتَسْمَلَا تَانُوْكْمَلَا

قِيلَاتَلَا جَمَارِبَلَاو قَدَامَلَا تَانُوْكْمَلَا تَارَادِصَا يَلِ دِنْتَسْمَلَا اذَه يَف قَدْرَاوَلَا تَاْمَوْلَعْمَلَا دِنْتَسْت:

- Cisco ASA 9.3.2
- Cisco IOS® 12.4T رَادِصَاإَلَا، لِيغَشْتَلَا مَظَنَب لَمَعْت يَتَلَا تَاهَجُوْمَلَا

قَسِيسَاأَلَا سَمِ

اهم ادخاتس إك نكمي نكلو، ناخال ضعب يف ةرفشم IPsec و IKE اطاخأ ححصت تايلمع نوكت VPN IPsec قفن عاشن إلكشم عقوم مهفل

ويرانيس

ةكبش لىلإ (LAN) ةيلحم لةكبش لىل قافنأ نيب يسئىر لىل عضولا مادختس إمتي ام ةداع ةقداصم لىل تاداهش لىل مادختس إدن ع (EzVPN) دعب نع لوصولا ةلاح يف، وأ (LAN) ةيلحم لىل

جم انرب لىل نم 9.3.2 رادص إل نالغشت نيت لىل ASAs يتطقن نم اطاخأ لىل ححصت يتأي LAN ةكبش لىلإ LAN ةكبش نم قفن نازاه لىل لكشيس

نيسئىر ناهو ويرانيس فصيو:

- IKE لىل دابك ASA
- IKE لىل بيجتس مك ASA

ةمدختس ملىل ححصت لىل رمأ

```
debug crypto ikev1 127
```

```
debug crypto ipSec 127
```

ASA نيوكت

IPsec نيوكت:

```
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
crypto map MAP 10 match address VPN
crypto map MAP 10 set peer 10.0.0.2
crypto map MAP 10 set transform-set TRANSFORM
crypto map MAP 10 set reverse-route
crypto map MAP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
  pre-shared-key cisco
access-list VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
```

IP نيوكت:

```
ciscoasa#
```

```
show ip
```

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.0	manual
GigabitEthernet0/1	outside	10.0.0.1	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.0	manual
GigabitEthernet0/1	outside	10.0.0.1	255.255.255.0	manual

لي nat:

```
object network INSIDE-RANGE
  subnet 192.168.1.0 255.255.255.0 object network FOREIGN_NETWORK
  subnet 192.168.2.0 255.255.255
nat (inside,outside) source static INSIDE-RANGE INSIDE-RANGE destination static
FOREIGN_NETWORK FOREIGN_NETWORK no-proxy-arp route-lookup
```

اءاطخ ال احي حصت

```
[ IKEv1]: Pitcher: spi 0x0
IPSec(crypto_map_check)-3: 5 : prot=1 saddr=192.168.1.2 sport=2816
daddr=192.168.2.1 dport=2816
MM_NO_STATE. IPSec(crypto_map_check)-3: 10: .
ASA . [IKEv1]: IP = 10.0.0.2 IKE: 1 Intf IKE Peer 10.0.0.2 192.168.1.0
(MAP)
[ IKEv1]: IP = 10.0.0.2 ISAKMP SA [ IKEv1]: IP = 10.0.0.2 NAT-
Traversal VID ver 02
MM1 [ IKEv1]: IP = 10.0.0.2 NAT-Traversal VID 03
NAT-T . [ IKEv1]: IP = 10.0.0.2 NAT-Traversal vid ver RFC
[ IKEv1]: IP = 10.0.0.2 VID +
MM1. [IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=0) : HDR + SA
(1) + (13) + (13) + (13) + (13) + (0) : 168
=====
=====>
[IKEv1]: IP = 10.0.0.2 IKE_Decode Receive Message (msgid=0) with
payload: HDR + SA (1) + Vendor (13) + Vendor (13) + Vendor (13) + MM1 .
Vendor (13) + None (0) : 164
[ IKEv1]: IP = 10.0.0.2 SA MM1.
[ IKEv1]: IP = 10.0.0.2 Oakley ISAKMP/IKE.
[ IKEv1]: IP = 10.0.0.2 VID NAT-T.
[ IKEv1]: IP = 10.0.0.2 NAT-Traversal RFC VID :
[ IKEv1]: IP = 10.0.0.2 VID ISAKMP 10
[ IKEv1]: IP = 10.0.0.2 NAT-Traversal 03 VID 3des
[ IKEv1]: IP = 10.0.0.2 VID
[ IKEv1]: IP = 10.0.0.2 IKE SA 86400
[ IKEv1]: IP = 10.0.0.2 IKE SA # 1 # 1 IKE # 2
[ IKEv1]: IP = 10.0.0.2 ISAKMP SA MM2.
[ IKEv1]: IP = 10.0.0.2 NAT-Traversal VID 02 ISAKMP .
[ IKEv1]: IP = 10.0.0.2 VID + NAT-T .
[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=0) : HDR +
SA (1) + (13) + (13) + (0) : 128 MM2.
<=====
=====
MM2 . [IKEv1]: IP = 10.0.0.2 IKE_Decode Receive Message (msgid=0) : HDR +
SA (1) + Vendor (13) + None (0) : 104
MM2. [ IKEv1]: IP = 10.0.0.2 SA
[ IKEv1]: IP = 10.0.0.2 Oakley
[ IKEv1]: IP = 10.0.0.2 VID
[ IKEv1]: IP = 10.0.0.2 NAT-Traversal RFC VID
```

```

30 10:38:29 [ IKEv1]: IP = 10.0.0.2 ke
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 nonce
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 Cisco Unity VID
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 VID (UVID)
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 IOS VID
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 ASA IOS ( 1.0.0 : 2000001)
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 VID
30:38:29 [ IKEv1]: IP = 10.0.0.2 Altiga/Cisco VPN3000/Cisco ASA GW
VID
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 NAT-Discovery
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 NAT
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 NAT-Discovery
30 10:38:29 [ IKEv1]: IP = 10.0.0.2 NAT
[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=0) : HDR + KE
(4) + NONCE (10) + (13) + (13) + (13) + (13) + NAT-D (20) + NAT-D
(20) + NAT-D (20) + (0) : 304
=====mm3=====
=====>
[IKEv1]: IP = 10.0.0.2 IKE_Decode (msgid=0) : HDR + KE (4) +
NONCE (10) + (13) + (13) + NAT-D (130) + NAT-D (130) + NAT-D MM3 .
(130) + (0) : 284 :
[ IKEv1]: IP = 10.0.0.2 ke
[ IKEv1]: IP = 10.0.0.2 ISA_KE
[ IKEv1]: IP = 10.0.0.2
[ IKEv1]: IP = 10.0.0.2 VID
[ IKEv1]: IP = 10.0.0.2 DPD VID MM3.
[ IKEv1]: IP = 10.0.0.2 VID NAT-D NAT
[ IKEv1]: IP = 10.0.0.2 IOS/PIX (: 1.0.0 : 0000f6f) NAT.
[ IKEv1]: IP = 10.0.0.2 VID DH KE p g a.
[ IKEv1]: IP = 10.0.0.2 XAUTH V6 VID
[ IKEv1]: IP = 10.0.0.2 NAT-Discovery
[ IKEv1]: IP = 10.0.0.2 NAT
[ IKEv1]: IP = 10.0.0.2 NAT-Discovery
[ IKEv1]: IP = 10.0.0.2 NAT
[ IKEv1]: IP = 10.0.0.2 ke
[ IKEv1]: IP = 10.0.0.2 nonce
[IKEv1 debug]: IP = 10.0.0.2 Cisco Unity VID
[ IKEv1]: IP = 10.0.0.2 XAUTH V6 VID MM4.
[ IKEv1]: IP = 10.0.0.2 Send IOS VID NAT DH KE
[ IKEv1]: IP = 10.0.0.2 ASA IOS (: 1.0.0 : 2000001) rESPONDER "B" "s"
[ IKEv1]: IP = 10.0.0.2 VID ("B" InAtor) DPD
[ IKEv1]: IP = 10.0.0.2 Altiga/Cisco VPN3000/Cisco ASA GW VID VID.
[ IKEv1]: IP = 10.0.0.2 NAT-Discovery
[ IKEv1]: IP = 10.0.0.2 NAT
[ IKEv1]: IP = 10.0.0.2 NAT-Discovery
[ IKEv1]: IP = 10.0.0.2 NAT
[IKEv1]: IP = 10.0.0.2 tunnel_group 10.0.0.2 10.0.0.2 L2L "s"
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 ... .
[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=0) : HDR + KE
(4) + NONCE (10) + (13) + (13) + (13) + NAT-D (130) + NAT-D (130) + MM4.
NAT-D (130) + (0) : 304
<=====mm4=====
=====
[IKEv1]: IP = 10.0.0.2 IKE_Decode Receive Message (msgid=0) : HDR +
MM4 .
KE (4) + NONCE (10) + (13) + (13) + (13) + NAT-D (20) + NAT-D (20)
+ NAT-D (20) + (0) : 304
[ IKEv1]: IP = 10.0.0.2 IKE
[ IKEv1]: IP = 10.0.0.2 ISA_KE
MM4.
[ IKEv1]: IP = 10.0.0.2
NAT-D
[ IKEv1]: IP = 10.0.0.2 VID
NAT.
[IKEv1 debug]: IP = 10.0.0.2 Cisco Unity Client VID
[ IKEv1]: IP = 10.0.0.2 VID
DH KE i "B" "S".
[ IKEv1]: IP = 10.0.0.2 DPD VID
[ IKEv1]: IP = 10.0.0.2 VID

```

```

[ IKEv1]: IP = 10.0.0.2 IOS/PIX (: 1.0.0 : 0000f7f)
[ IKEv1]: IP = 10.0.0.2 VID
[ IKEv1]: IP = 10.0.0.2 XAUTH V6 VID
[ IKEv1]: IP = 10.0.0.2 NAT-Discovery
[ IKEv1]: IP = 10.0.0.2 NAT
[ IKEv1]: IP = 10.0.0.2 NAT-Discovery
[ IKEv1]: IP = 10.0.0.2 NAT
10.0.0.2 L2L [IKEv1]: IP = 10.0.0.2 tunnel_group 10.0.0.2
"S" . [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 ..
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
MM5. [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
: [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 ISAKMP
ISAKMP [ IKEv1]: IP = 10.0.0.2 IOS : =32767/32767 sec.
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 DPD vid
MM5. [IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=0) : HDR + ID
(5) + HASH (8) + IOS Keepalive (128) + (13) + (0) : 96
=====mm5=====
=====>
[IKEv1]: = [IKEv1]: IP = 10.0.0.2 IKE_Decode Receive Message MM5 .
10.0.0.2 IP = (msgid=0) : HDR + ID (5) + HASH (8) + NONE (0) : r (ID) C .
10.0.0.2 nat: nat: 64
nat nat
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 ID_IPv4_ADDR ID MM5.
10.0.0.2
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 ISAKMP
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 NAT 10.0.0.2 ipSEC-121
[IKEv1]: IP = 10.0.0.2 tunnel_group 10.0.0.2
: nat nat NAT-T .
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 MM6.
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 ISAKMP
[ IKEv1]: IP = 10.0.0.2 IOS : =32767/32767 sec.
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 DPD vid
[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=0) : HDR + ID MM6.
(5) + HASH (8) + IOS Keepalive (128) + (13) + (0) : 96
<=====
=====
.
ISAKMP.
:
ISAKMP 10
MM6 . [IKEv1]: IP = 10.0.0.2 IKE_Decode [IKEv1]: = 10.0.0.2 IP = 10.0.0.2
Receive Message (msgid=0) : HDR [IKEv1]: IP = 10.0.0.2 " " : DPD 3des
+ ID (5) + HASH (8) + NONE (0) : [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
64 rekey P1: 64800 .
86400
cisco# sh isakmp
ISAKMP
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 ID_IPv4_ADDR ID
10.0.0.2
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 ISAKMP
[IKEv1]: IP = 10.0.0.2 tunnel_group 10.0.0.2
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 Oakley
MM6.
r f .

```

```

[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 IKE QM: msg = 7b80c2b0
.
ISAKMP. [IKEv1]: = 10.0.0.2 IP = 10.0.0.2 1
: [IKEv1]: IP = 10.0.0.2 " " : DPD
10.0.0.2 ipSEC-I21 .
10.0.0.2 IPsec [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 P1: 82080 .
Cisco
IPSec: SA 0x53FC3C00
SCB: 0x53f90a00
:
SPI: 0xFD2D851F
( ). : 0x00006000
num VPIF: 0x000003
: 121
: esp
: 240
[IKEv1 debug]: = 10.0.0.2 IP = 10.0.0.2 IKE SPI : SPI = 0xfd2d851f
QM1. [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
IP . [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
: [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPsec SA
IPSec ESP-aes esp- [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPSec
sha-hmac [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2
-list VPN Extended [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 :
Permit ICMP : 192.168.1.0 255.255.255.0 1 0
192.168.1.0 : 192.168.2.0 255.255.255.0 1 0
255.255.255.0 (192.168.1.0/24) (192.168.2.0/24)
192.168.2.0 [IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 IKE
255.255.255.0 [ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 QM
[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 IKE QM pkt: msg = 7b80c2b0
[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=7b80c2b0) :
QM1. HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY
(11) + NONE (0) : 200
=====qm1=====
=====>
[ IKEv1]: IP = 10.0.0.2 IKE QM: msg id = 52481cf5
[IKEv1]: IP = 10.0.0.2 IKE_Decode Receive Message (msgid=52481cf5) : QM1 .
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) : 2 (QM).
172
QM1.
IP .
: IPsec ESP-AES
esp-sha-hmac
-list VPN Extended
Permit ICMP
192.168.1.0
255.255.255.0
192.168.2.0
255.255.255.0
10 VPN
[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 ID_IPv4_ADDR_SUBNET ID
—192.168.2.0—255.255.255.0[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IP :
192.6 8.2.0 255.255.255.0 1 0 (192.168.2.0/24)
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 192.168.1.0/24).
[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 ID_IPv4_ADDR_Subnet ID
—192.168.1.0-255.255.255.0
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IP : 192.168.1.0 255.255.255.0 1 0
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 QM IsReated ADDR
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 = MAP seq = 10...
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 seq = 10
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IKE :
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPsec SA
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPsec SA # 1 # 1 IPsec SA # 10
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IKE: SPI QM2.
IPSec: SA 0x53FC3698 (ACL) .

```

SCB: 0x53FC2998
:
SPI: 0x1698CAC7
: 0x00004000
num VPIF: 0x000003
: 121
: esp
: 240

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IKE SPI : SPI = 0x1698cac7
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPsec SA
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPsec
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 :
: 192.168.2.0 255.255.255.0 1 0
: 192.168.1.0 255.255.255.0 1 0
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 QM
[IKEv1 decode]: = 10.0.0.2 IP = 10.0.0.2 Ike Responder PKT QM: msg
= 52481cf5

[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message (msgid=52481cf5) :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) : QM2.
172

<=====qm2=====

QM2 .

[IKEv1]: IP = 10.0.0.2 IKE_Decode Receive Message (msgid=7b80c2b0) :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY
(11) + NONE (0) : 200

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 SA

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2

[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 ID_IPv4_ADDR_Subnet ID
—192.168.1.0-255.255.255.0

QM2.
R

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2

[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 ID_IPv4_ADDR_Subnet ID
—192.168.2.0—255.255.255.0

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2

[IKEv1]: (SPI[4]):

[IKEv1]: 0000: DDE50931 80010001 00020004 00000E10 ...1.....

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IPsec 28800 3600

ASA IPsec . rekey

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 (SAs) IPsec

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 !

"MAP" 10
"VPN."

[IKEv1 debug]: = 10.0.0.2 IP = 10.0.0.2 NP MAP 10 (ACL) VPN:
cs_id=53f11198 =53f11a90

[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 !

IPsec: SA 0x53FC3698

SCB: 0x53F910F0

:

SPI: 0xDDE50931

: 0x00006000

num VPIF: 0x000003

: 121

: esp

: 240

SPIs 0xfd2d851f
0xdd50931 .

IPsec: OBSA SPI 0xDDE50931

IPsec: VPN SPI 0xDDE50931

: 0x000005

SA: 0x53FC3698

SPI: 0xDDE50931

(MTU): 1500

VCID: 0x000000

: 0x000000

```

SCB: 0x01CF218F
: 0x4C69CB80
IPSec: VPN SPI 0xDDE50931
  VPN: 0x000161a4
IPSec: SPI 0xDDE50931
  SRC: 192.168.1.0
  SRC: 255.255.255.0
DST addr: 192.168.2.0
  DST: 255.255.255.0
  SRC
: 0
:

  DST
: 0
:

: 1
:
SPI: 0x000000
SPI:
IPSec: SPI 0xDDE50931
  : 0x53fc3ad8
IPSec: SPI 0xDDE50931
  SRC: 10.0.0.1
  SRC: 255.255.255.255
DST Addr: 10.0.0.2
  DST: 255.255.255.255
  SRC
: 0
:

  DST
: 0
:

: 50
:
SPI: 0xDDE50931
SPI:
IPSec: SPI 0xDDE50931
  : 0x53F91538
[IKEv1 debug]: = 10.0.0.2 IP = 10.0.0.2 NP MAP 10 (ACL) VPN:
cs_id=53f11198 =53f11a90
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 (LAN) (10.0.0.2) SPI = 0xfd2d851f
SPI = 0xdde50931
IPSec: IBSA SPI 0xFD2D851F
IPSec: VPN SPI 0xFD2D851F
: 0x000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
  (MTU): 0
VCID: 0x000000
: 0x000161a4
SCB: 0x01CEA8EF
: 0x4C69CB80
IPSec: VPN SPI 0xFD2D851F
  (VPN): 0x00018BBC
IPSec: VPN 0x000161A4 SPI 0xDDE50931
: 0x000005
SA: 0x53FC3698
SPI: 0xDDE50931
  (MTU): 1500
VCID: 0x000000

```

QM3.
SPIs .

: 0x00018BBC
SCB: 0x01CF218F
: 0x4C69CB80
IPSec: VPN SPI 0xDDE50931
VPN: 0x000161a4
IPSec: SPI 0xDDE50931
: 0x53fc3ad8
IPSec: SPD SPI 0xDDE50931
: 0x53F91538
IPSec: SPI 0xFD2D851F
SRC: 192.168.2.0
SRC: 255.255.255.0
DST addr: 192.168.1.0
DST: 255.255.255.0
SRC
: 0
:

DST
: 0
:

: 1
:
SPI: 0x000000
SPI:
IPSec: SPI 0xFD2D851F
: 0x53F91970
IPSec: SPI 0xFD2D851F
SRC: 10.0.0.2
SRC: 255.255.255.255
DST Addr: 10.0.0.1
DST: 255.255.255.255
SRC
: 0
:

DST
: 0
:

: 50
:
SPI: 0xFD2D851F
SPI:
IPSec: SPI 0xFD2D851F
: 0x53F91A08
IPSec: SPI 0xFD2D851F
SRC: 10.0.0.2
SRC: 255.255.255.255
DST Addr: 10.0.0.1
DST: 255.255.255.255
SRC
: 0
:

DST
: 0
:

: 50
:
SPI: 0xFD2D851F
SPI:

IPSec: SPI 0xFD2D851F
: 0x53F91A0
[IKEv1 Decode]: = 10.0.0.2 IP = 10.0.0.2 IKE QM pkt: msg id =
7b80c2b0

QM3.

=====qm3=====

[IKEv1]: IP = 10.0.0.2 IKE_Decode Send Message
(msgid=7b80c2b0) : HDR + HASH (8) + NONE (0) : [IKEv1]: IP =
76 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IKE KEY_ADD IKE_Decode
msg SA: SPI = 0xdde50931 Receive Message QM3 .
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 Pitcher: (msgid=52481cf5)
KEY_UPDATE spi 0xfd2d851f : HDR + (8) +
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 P2: 3060 . (0) : 52
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 2 (msgid=7b80c2b0)
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 (SAs) IPSec
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 !
[IKEv1 debug]: = 10.0.0.2 IP = 10.0.0.2 NP MAP 10 (ACL) VPN:
cs_id=53f11198 =53f11a90
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 !
IPSec: SA 0x53f18b00
SCB: 0x53F8A1C0
:
SPI: 0xDB680406
: 0x00004000
num VPIF: 0x000003
: 121
: esp
: 240
IPSec: OBSA SPI 0xDB680406
IPSec: VPN SPI 0xDB680406
: 0x000005
SA: 0x53F18B00
SPI: 0xDB680406
(MTU): 1500
VCID: 0x000000
: 0x000000 QM3.
SCB: 0x005E4849 (SAs) .
: 0x4C69CB80
IPSec: VPN SPI 0xDB680406 SPIs .
VPN: 0x0000E9B4
IPSec: SPI 0xDB680406
SRC: 192.168.1.0
SRC: 255.255.255.0
DST addr: 192.168.2.0
DST: 255.255.255.0
SRC
: 0
:
DST
: 0
:
: 1
:
SPI: 0x000000
SPI:
IPSec: SPI 0xDB680406
: 0x53f89160
IPSec: SPI 0xDB680406
SRC: 10.0.0.1

SPI .

QM3 .

QM3.

(SAs) .

SPIs .

SRC: 255.255.255.255
DST Addr: 10.0.0.2
DST: 255.255.255.255
SRC
: 0
:
DST
: 0
:
: 50
:
SPI: 0xDB680406
SPI:
IPSec: SPI 0xDB680406
: 0x53E47E88
[IKEv1 debug]: = 10.0.0.2 IP = 10.0.0.2 NP MAP 10 (ACL) VPN:
cs_id=53f11198 =53f11a90
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 (LAN) (10.0.0.2) SPI = 0x1698cac7
SPI = 0xdb680406
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 IKE KEY_ADD msg SA: SPI =
0xdb680406
IPSec: IBSA SPI 0x1698CAC7
IPSec: VPN SPI 0x1698CAC7
: 0x000006
SA: 0x53FC3698
SPI: 0x1698CAC7
(MTU): 0
VCID: 0x000000
: 0x0000E9B4
SCB: 0x005DAE51
: 0x4C69CB80
IPSec: VPN SPI 0x1698CAC7
VPN: 0x00011A8C
IPSec: VPN 0x0000E9B4 SPI 0xDB680406
: 0x000005
SA: 0x53F18B00
SPI: 0xDB680406
(MTU): 1500
VCID: 0x000000
: 0x00011a8c SPIs SAs .
SCB: 0x005E4849
: 0x4C69CB80
IPSec: VPN SPI 0xDB680406
VPN: 0x0000E9B4
IPSec: SPI 0xDB680406
: 0x53f89160
IPSec: SPD SPI 0xDB680406
: 0x53E47E88
IPSec: SPI 0x1698CAC7
SRC: 192.168.2.0
SRC: 255.255.255.0
DST addr: 192.168.1.0
DST: 255.255.255.0
SRC
: 0
:
DST
: 0
:
: 1

```

:
SPI: 0x000000
SPI:
IPSec: SPI 0x1698CAC7
: 0x53FC3E80
IPSec: SPI 0x1698CAC7
SRC: 10.0.0.2
SRC: 255.255.255.255
DST Addr: 10.0.0.1
DST: 255.255.255.255
SRC
: 0
:
DST
: 0
:
: 50
:
SPI: 0x1698CAC7
SPI:
IPSec: SPI 0x1698CAC7
: 0x53FC3F18
IPSec: SPI 0x1698CAC7
SRC: 10.0.0.2
SRC: 255.255.255.255
DST Addr: 10.0.0.1
DST: 255.255.255.255
SRC
: 0
:
DST
: 0
:
: 50
:
SPI: 0x1698CAC7
SPI:
IPSec: SPI 0x1698CAC7
: 0x53F8AEA8
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 Pitcher: KEY_UPDATE SPI
0x1698cac7
[ IKEv1]: = 10.0.0.2 IP = 10.0.0.2 P2: 3060 . IPsec.
[IKEv1]: = 10.0.0.2 IP = 10.0.0.2 2 (msgid=52481cf5) . / .

```

قفنللا نم ققحتلا

ذفنم يوس ليغشت متي ملف، قفنللا ليغشت ل ICMP لوكوتورب مادختسال ارطن: ةظحالم
IPSec دحواو . طقف دحواو IPsec .

show crypto ipsec sa

```

interface: outside
Crypto map tag: MAP, seq num: 10, local addr: 10.0.0.1
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/

```

1

/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/

1

/0)
current_peer: 10.0.0.2
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0
local crypto endpt.: 10.0.0.1/0, remote crypto endpt.: 10.0.0.2/0
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: DB680406
current inbound spi : 1698CAC7
inbound esp sas:
spi: 0x

1698CAC7

(379112135)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 16384, crypto-map: MAP
sa timing: remaining key lifetime (kB/sec): (3914999/3326)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
outbound esp sas:
spi: 0xDB680406 (3681027078)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 16384, crypto-map: MAP
sa timing: remaining key lifetime (kB/sec): (3914999/3326)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.0.0.2
Type :

L2L

Role :

responder

Rekey : no State :

MM_ACTIVE

قلمص تاذا تامولعم

- نم ريثكلا لىلع عجارملا وريياعملا يوتحت [IPSec عقوم لىلع لاقم](#) وه ءدبلل ديچ ناكم ءديفملا تامولعملا
- [اهم ادختس او ءاطخ ال احيصت رم او مهف :اهجالص او IPsec ءاطخ افاشكتسأ](#)
- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب
Cisco مچرت م ا م د ق م م ي ت ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ س م Cisco
Systems م (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ي ز م ل چ ن ا ل ا دن ت س م ل ا