

# NAD لاصتا نيمأتل IPsec 2.2 ISE نيوكت (IOS)

## تايوت حمل

[عمدق مل](#)

[سياس الابلط مل](#)

[تابلط مل](#)

[عمدخت سمل تانوك مل](#)

[سياس ا تامول عم](#)

[ISE IPsec ة ني](#)

[كك بشلل يطي طختل مسرل](#)

[\(عبرمل جراخ\) اقوسم كرتشم حاتفم مادختساب IPsec VPN IKEv1 نيوكت](#)

[IOS هجومل رماوالا رطس ة هجاو نيوكت](#)

[تاهجاو نيوكت](#)

[ISAKMP \(IKEv1\) ة سايس نيوكت](#)

[ريفش ت ISAKMP حاتفم نيوكت](#)

[ة مهال تاذ VPN رورم ة كرحل \(ACL\) لوصولا يف مكحت ة مئاق نيوكت](#)

[لويحت ة عومجم نيوكت](#)

[ة هجاو يل عاهق يبطت وري فشت ة طيرخ نيوكت](#)

[IOS يئاهنل نيوكت](#)

[ISE نيوكت](#)

[ISE يلع IP ناو نع نيوكت](#)

[ISE يلع IPsec ة عومجم يل نAD ة فاضا](#)

[ISE يلع IPsec نيكم ت](#)

[ISE يلع Tacacs جهن نيي عت](#)

[ة حصلا نم ققحتل](#)

[IOS هجوم](#)

[ESR](#)

[\(ISE\) ة يوهل فشكل تامدخ كرحم](#)

[اهجالص او عاطخال فاشكت سا](#)

[ISE 2.2 و NAD ني \(SVTI يل DVTI نم\) FlexVPN ة كك بش عقوم يل عقوم نيوكت](#)

[Flex VPN ميمصت ايازم](#)

[هجومل نيوكت](#)

[ISE يلع ESR نيوكت](#)

[FlexVPN ميمصت تارابتعا](#)

## عمدق مل

نيمأتل اهجالص او هئاطخال فاشكت ساو IPsec TACACS نيوكت ة يفكي دنن سمل اذه فصري نكمي (NAD). كك بشلل يل لوصولا زاهج - Cisco 2.2 نم (ISE) ة يوهل عمدخ كرحم لاصتا نم (IKEv2) 2 رادصلال تنرتنل حاتفم لدابت قفن مادختساب TACACS رورم ة كرح ريفشت نيوكت عجز دنن سمل اذه يطيغي ال. ISE و هجومل ني (LAN-to-LAN) عقوم يل عقوم نم IPsec TACACS.

# ةيساس الابلطتم ال

## تابلطتم ال

ةيلال ال عيضاوم لابل ةفرعم كيدل نوكت نابل Cisco ي صوت:

- ةيوه ال فشك تامدخ كرحم (ISE)
- هجوم Cisco
- ةماع ال IPSec ميهافم
- ةماع ال TACACS ل ميهافم ال

## ةمدختسم ال تانوكم ال

ةيلال ال ةيدام ال تانوكم لاولجم رابل تارادصل ال دننتسم ال اذه يف ةدراول تامولعمل دننتست:

- جم انرب ال نم 15.4(3)S2 رادصل ال لغشي يذل Cisco ISR4451-X Router هجوم ال
- Cisco Identity Service Engine، رادصل ال 2.2
- Windows ل لغش التل ماطنل 1 ةمدخل ال ةمزح

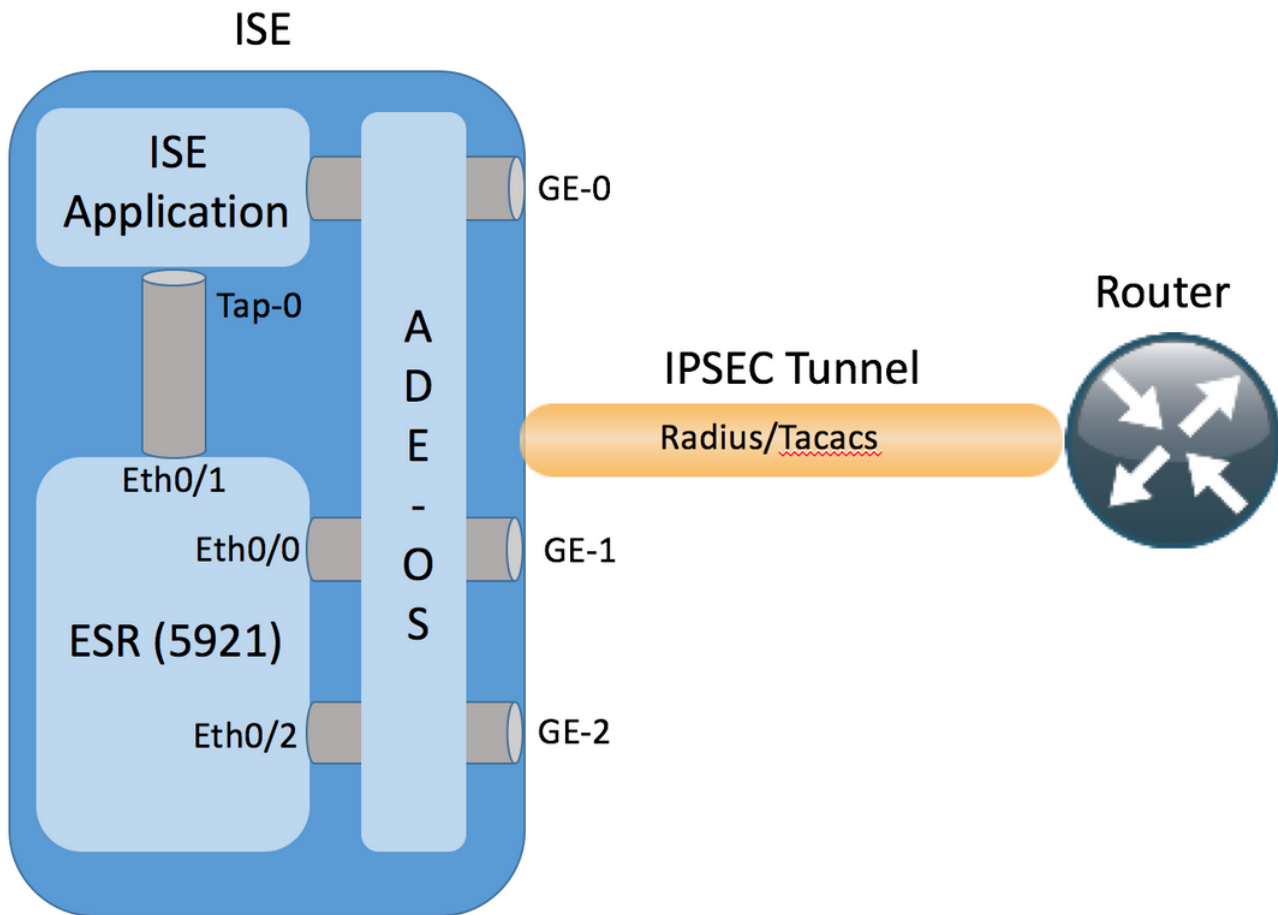
ةصاخ ةيلمعم ةئيب يف ةدوجوم ال ةزهجال نم دننتسم ال اذه يف ةدراول تامولعمل عاشن اتم تناك اذ. (يضا رتفا) حوسمم نيوكتب دننتسم ال اذه يف ةمدختسم ال ةزهجال اعيمج تادب رما يال لم تحم ال ريثاتلل كمهف نم دكأتف، ةرشابم كتكبش

## ةيساس ا تامولعم

TACACS و RADIUS و ةنم ال ريغ MD5 ةئزجت ممدختست يتل التالوكوتورب ال ني مات وه فدهل او رابتع ال ني عب اهذخ ابحي يتل قئاقحل نم ليلق IPSec.

- لقلنل او قفنل يعضوي يف IPSec لوكوتورب Cisco ISE معددي.
- Cisco ISE و NAD ني ب IPSec قفن عاشن اتم تي، Cisco ISE ةهجاو لعل IPSec ني كم ت دنع لاصل ال ني ماتل.
- IPSec ةقداصل X.509 تاداهش ممدختست او اقبس م كرتشم حاتفم ديدحت كنكمي.
- لعل IPSec تل كش عي طتسي تنأ. ETH5 تاهجاو لال خ نم ETH1 لعل IPSec ني كم ت كنكمي لعل PSN ل كل نراق Cisco ISE دحاو طقف.

## ةيساس ال IPSec



ةنمضملا تامدخلا هجوم ضررت عي ، GE-1 ISE ةهجاو ةطساوب ةرفشملا مزحلا مالتسا درجمب (ESR) ةهجاو ىلع مزحلا (ESR).

```
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 10.48.17.87 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
```

ةمجرت ذي فنن تب اقبسم اهن يوكت مت يتي NAT دع او قل اق فوو اهري فشت ك فب ESR موقبي Ethernet0/0 ةهجاو ناو نع ىلإ (NAD وحن) ةرداصل RADIUS/TACACS مزح ةمجرت مت . ناو نع ال . كلذ دع ب اهري فشت و .

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
access-list 1 permit 10.1.1.0 0.0.0.3
```

ETH0/1 ةهجاو ربع RADIUS/TACACS ذفانم ىلع ETH0/0 ةهجاو ىلإ ةهجوملا مزحلا لاسرا بجي ETH0/1 ل ESR نيوكت . ISE ل يلخادلا ناو نع ال وهو ، IP 10.1.1.2 ناو نع ىلإ

```
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
```

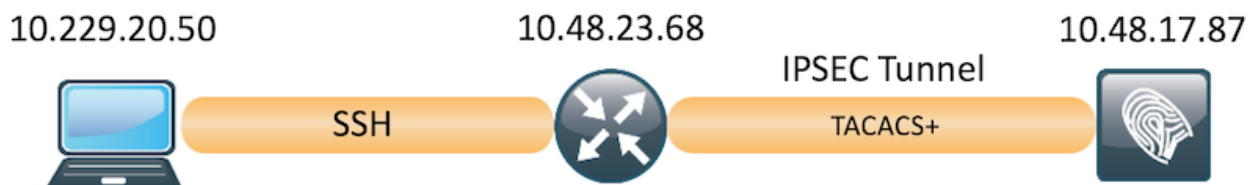
```
ip nat inside
ip virtual-reassembly in
no ip route-cache
```

تة: لي ادلا TAP-0 ةه اولا ISE ني وك ت

```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.1.1.2 netmask 255.255.255.252 broadcast 10.1.1.3
inet6 fe80::6c2e:37ff:fe5f:b609 prefixlen 64 scopeid 0x20<link>
ether 6e:2e:37:5f:b6:09 txqueuelen 500 (Ethernet)
RX packets 81462 bytes 8927953 (8.5 MiB)
RX errors 0 dropped 68798 overruns 0 frame 0
TX packets 105 bytes 8405 (8.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## ة ك ب ش ل ل ي ط ي ط خ ت ل م س ر ل ا

ي ل ل ت ل ل ة ك ب ش ل ل دادع | دن ت س م ل ا ذه ي ف ة در اول ا تام ول عمل م مدخت ست



## اق ب س م ك ر ت ش م ح ا ت ف م م ا د خ ت س ا ب IKeV1 IPsec VPN ني وك ت (ع ب ر م ل ا ج ر ا خ)

I SE و IOS CLI ت ان ي وك ت ل ا م ك | ة ي ف ي ك م س ق ل ل ا ذه ح ض و ي

## IOS ه ج و م ل ر م او ال ا ر ط س ة ه ج او ني وك ت

### ت ا ه ج اول ا ني وك ت

ي ل ي ام ي ف . ل ق ال ا ل ع WAN ة ه ج او ني وك ت ب ج ي ف ، د ع ب IOS ه ج و م ت ا ه ج او ني وك ت م ت ي م ل ا ذ ا ل ل ا ت :

```
interface GigabitEthernet0/0/0
ip address 10.48.23.68 255.255.255.0
negotiation auto
no shutdown
!
```

ن م VPN ة ك ب ش ق ف ن ا ش ن ا ل ه م ا د خ ت س ا ب ج ي ي ذ ل ا د ي ع ب ل ر ي ظ ن ل ا ب ل ا ص ت ا د و ج و ن م د ك ا ت ي س ا س ال ا ل ا ص ت ال ا ن م ق ق ح ت ل ل ل ا ص ت ال ا ر ا ب ت خ | م ا د خ ت س ا ب ك ن ك م ي . ع ق و م ي ل ا ع ق و م

### ISAKMP (IKeV1) ة س ا ي س ني وك ت

ة س ا ي س crypto isakmp ل ل ، ل ي ص و ت IKeV1 ل ل ة س ا ي س isakmp ل ل ت ل ك ش in order to ت ل خ د

لائم يلى اميف .بولسأ ليكشت لماش يف رمأ <priority>

```
crypto isakmp policy 10
  encr aes
  hash sha256
  authentication pre-share
  group 16
```

ءدب دنع IPsec يف كراشيف ريظن لك ىلع ءدعتم IKE تاسايس نيوكت كنكمي :ءظالم نم لك ىلع اهنويوكت مت ءكرتشم ءسايس ىلع روٲعلا لواحي هناف ،IKE ضواف ءيعبل ريظنلا ىلع اهءيحت مت يتل ايلعلا ءيولوال تاسايس بءب وءارظنلا

## ريفشت ISAKMP حاتفم نيوكت

لماش يف رمأ حاتفم crypto isakmp ل ،حاتفم ءيوه ءحص قباس تلكش in order to تلخد بولسأ ليكشت :

```
crypto isakmp key Krakow123 address 10.48.17.87
```

## ءيمهالا تاء VPN رورم ءكرل (ACL) لوصول يف مكحت ءمئاق نيوكت

اهتياح بجي يتل رورملا ءكرل ءيحتل ءامسمل وأ ءعسوملا لوصول ءمئاق مءختسأ لائم يلى اميف .ريفشتلاب :

```
access-list 101 permit ip 10.48.23.68 0.0.0.0 10.48.17.87 0.0.0.0
```

رءصم لل IP نيوانع VPN رورم ءكرل لوصول يف مكحتل ءمئاق مءختست :ءظالم ءع ءهءولواو NAT.

## ليوحت ءعومجم نيوكت

رمأ لءءا ،(تايمزراولواو نامألا تالوكوتورب نم ءلوبقم ءعومجم) IPsec ليوحت ءعومجم ءيحتل لائم يلى اميف .ماعلا نيوكتلا ءضو يف crypto ipsec transform-set

```
crypto ipsec transform-set SET esp-aes esp-sha256-hmac
  mode transport
```

## ءهءاولىل اهقيبطتو ريفشت ءطيخ نيوكت

بولسأ ليكشت ءطيخ crypto ل تلءءاولءدم ءطيخ ريفشت تلءءع وأ تقلء in order to تلخد بئاوئل ضعب كانه ،ريفشتل ءطيخ لءءا لمءكي ىءء .رمأ ليكشت لماش crypto map ل ىنءا ءءاهفءعت بجي يتل :

- مه ءالؤه .اهلل ءيمءملا رورملا ءكرل هءءوت ءءاعل نكمي يتل IPsec رءاظن ءيحت بجي يف ريظن IPsec تنيع in order to ءءء .ءءء ءءاسم ءاشنل مهءم نكمي نيءل نارقألا .رمأ ريظن ءعومءملا ،لءءم ءطيخ ريفشت
- in order to تلخد .ءيمءملا رورملا ءكرل عم مءءءسالل ءلوبقملا ليوحتل تاوعومءم ءيحت بجي ،لءءم ءطيخ crypto ل عم تلمءسا تنك عيظءسي نأ ءعومءم ليوحتل تنيع in order to ،رمأ ل-set ليوحت ءعومءملا

ل عملاق ذفنم عسوم تنيع in order to تلخد. اهتياح بجي يتل رورملا ةكرح ديدحت بجي •  
رمأ ناونع **crypto map** ل، لخدمة طيرخ **crypto**.  
لاثم يلي اميف:

```
crypto map MAP 10 ipsec-isakmp
set peer 10.48.17.87
set transform-set SET
match address 101
```

ةهجاو ىلع اقبسمة ددحمل ريفش تلال ةطيرخة عومجم قيبطت يف ةريخألا ةوطخل لثمتت  
رمأ ليكشت نراق **crypto map** ل، اذه تقببط in order to تلخد:

```
interface GigabitEthernet0/0
crypto map MAP
```

## IOS نياهنل نيوكتل

نيياهنل IOS هجومل CLI نيوكت يلي اميف:

```
aaa group server tacacs+ ISE_TACACS
server name ISE22
!
aaa authentication login default group ISE_TACACS
aaa authorization exec default group ISE_TACACS
!
crypto isakmp policy 10
encr aes
hash sha256
authentication pre-share
group 16
!
crypto isakmp key Krakow123 address 10.48.17.87
!
crypto ipsec transform-set SET esp-aes esp-sha256-hmac
mode transport
!
crypto map MAP 10 ipsec-isakmp
set peer 10.48.17.87
set transform-set SET
match address 101
!
access-list 101 permit ip 10.48.23.68 0.0.0.0 10.48.17.87 0.0.0.0
!
interface GigabitEthernet0/0/0
ip address 10.48.23.68 255.255.255.0
negotiation auto
no shutdown
!
crypto map MAP 10 ipsec-isakmp
set peer 10.48.17.87
set transform-set SET
match address 101
!
tacacs server ISE22
address ipv4 10.48.17.87
key cisco
```

## ISE نيوكت

## ISE یل ع IP ناونع نیوكت

ge0. مع د م تي ال ،رم او ال رطس ةه جاو نم GE5-ge1 ةه جاو ال یل ع ناونع ال نیوكت بجي

```
interface GigabitEthernet 1
ip address 10.48.17.87 255.255.255.0
ipv6 address autoconfig
ipv6 enable
```

ةه جاو ال یل ع IP ناونع نیوكت دعب قي بطت ال لي غشت ةداع م ت :  
ISE تامدخ لي غشت ةداع ال یل ع IP ناونع ري غت ي دوي دق %  
IP؟ ناونع ري غت عم ةع باتم ال ديرت له Y/N [N]: Y

## ISE یل ع IPSec ةومجم ال نAD فاضا

نیوكت نم دكأت (Add) ة فاضا قوف رقنا . ةك بش ال ةزهجأ > ةك بش ال دراوم > ةراد ال یل ع لقتنا  
ةومجم لباقم "معن" ددح م ت ،NAD نم IPSec ق فن ةاهن ال . كرتشم ال رسالو IP ناونعو مسال ال  
IPSec ةك بش ةزهجأ

The screenshot displays the 'Network Devices' configuration page in the Cisco Identity Services Engine (ISE) web interface. The page is organized into a sidebar on the left and a main configuration area on the right. The sidebar includes 'Network devices', 'Default Device', and 'Device Security Settings'. The main area contains several sections: 'Name' (ISR\_4451), 'Description', 'IP Address' (10.48.23.68 / 32), 'Device Profile' (Cisco), 'Model Name', 'Software Version', 'Network Device Group' (Device Type: All Device Types, IPSEC: Yes, Location: All Locations), 'RADIUS Authentication Settings', 'TACACS Authentication Settings' (checked), 'Shared Secret' (masked with dots), and 'Enable Single Connect Mode' (unchecked).

ةك رح نأ نامضل ،(ISE) ةي وه ال تامدخ كرحم ال یل ع ي فاضا راسم ةاشن بجي ،NAD ة فاضا درجم بو  
اھري فشت م تي و ESR لوكت و ر ب ربع رم ت RADIUS رورم

```
ip route 10.48.23.68 255.255.255.255 gateway 10.1.1.1
```

## ISE یل ع IPSec نیوكت م

PSN ددح IPsec قوف مٲ RADIUS قوف رقنا . تاداع | ماطن > ةراد | ل ل ل ق ت ن ا ةداع | . ظفح ةق طوط . ةق داصم ل بولس ا ددحو ةه جاولا رتخاو ، ني كمت را يخ ددح (ي ل ك / ددعت م / يداع ا) . ةق ن ل ل هذ ه ي ة ددح م ل ا ةدق ع ل ل ي ف ت ا مدخل ل ل ي غ ش ت

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu on the left includes 'Client Provisioning', 'FIPS Mode', 'Alarm Settings', 'Posture', 'Profiling', 'Protocols', 'EAP-FAST', 'EAP-TLS', 'PEAP', 'EAP-TTLS', 'RADIUS', 'IPsec', 'Security Settings', 'Proxy', 'SMTP Server', 'SMS Gateway', 'System Time', 'Policy Sets', 'ERS Settings', 'Smart Call Home', 'DHCP & DNS Services', and 'Max Sessions'. The main content area is titled 'IPsec Deployment' and contains the following sections:

- Activate ISE Nodes for IPsec:** A table with 4 columns: 'ISE Nodes', 'IPsec Status', 'IPsec Interface', and 'Authentication Type'. It shows two rows: 'ISE22-2ek' (Enabled) and 'ISE22-3ek' (Disabled). Below the table are two notes: 'Note: Please be aware that the application server will restart on the selected nodes.' and 'Note: Proper licensing must be installed and configured on ESR. Please see IPsec documentation.'
- Enable/Disable IPsec for selected nodes:** Radio buttons for 'Enable' (selected) and 'Disable'.
- IPsec interface for selected nodes:** A dropdown menu set to 'Gigabit Ethernet 1'.
- Authentication for selected nodes:** Radio buttons for 'Pre-shared Key' (selected) and 'X.509 Certificates'. Below 'Pre-shared Key' is a text input field containing 'Krakow123'.

At the bottom right, there are 'Cancel' and 'Save' buttons.

ISE ب ةصاخ ل ا (CLI) رم او ال ا رطس ةه ج او ني وكت موق ي ت ا مدخل ل ل ي غ ش ت ةداع | دعب ه ن ا ظح ال ن ا ع قو ت م ل ا ن م ، ل ي غ ش ت ل ل ا ق ي ا ل ا ح ي ف و IP ا و ن ع ن و د ب ا ه ني وكت م ت ي ت ل ل ا ةه ج اول ا ضرع ب ن ا ISE ةه ج او ي ف م ك ح ت ل ل ا ب ( ة ن م ضم م ل ا ت ا مدخل ل ل ا ه ج و م ) ESR موق ي ف

```
interface GigabitEthernet 1
shutdown
ipv6 address autoconfig
ipv6 enable
```

ESR عون ESR ل ل ل و د ل ل ل ي ج س ت ل . ESR ة في ظو ني كمت م ت ي ، ت ا مدخل ل ل ي غ ش ت ةداع | درج م ب رم او ال ا رطس ي ف

```
ISE22-1ek/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.
```

Press RETURN to get started, <CTRL-C> to exit



```
ise-esr5921>en
```

```
ise-esr5921#
```

مادختساب IPsec ق فن ءاهنإل ايفاك نوکي يذلاو، اذه ري فشتلا نيوكت عم ESR يتأي  
اقبسم ةكرتشم حيتافم:

```
crypto keyring MVPN-spokes
  pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
!
crypto isakmp policy 10
  encr aes
  hash sha256
  authentication pre-share
  group 16
!
crypto isakmp policy 20
  encr aes
  hash sha256
  authentication pre-share
  group 14
!
crypto isakmp key Krakow123 address 0.0.0.0
!
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
  mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
  mode transport
!
crypto dynamic-map MVPN-dynmap 10
  set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
```

ةرفشملا مزحلا لاسرلا راسم هي دل ESR نأ نم دكأت

```
ip route 0.0.0.0 0.0.0.0 10.48.26.1
```

ISE لى Tacacs جهن نييعت

The screenshot displays the Cisco ISE Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The breadcrumb trail is 'Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID'. The main content area is titled 'Policy Sets' and contains a search bar, a 'Summary of Policies' section, and a 'Global Exceptions' section. The 'Default' policy set is selected, showing a table with columns for Status, Name, and Description. Below this, there are sections for 'Proxy Server Sequence', 'Authentication Policy', and 'Authorization Policy'. The 'Authorization Policy' section shows a table of rules with columns for Status, Rule Name, Conditions, Command Sets, and Shell Profiles.

## تحصيل نام ققحتال

### IOS هجوم

تطشن VPN تالاصت إدوت ال، هجوم ال SSH ةسلج ادب لب ق

```
ISR4451#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
```

```
IPv6 Crypto ISAKMP SA
```

ISE 2.2 ةقداصم ردصم مادختس إدع، هجوم لاب ليم ال لصتي

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh alice@10.48.23.68
Password:
ISR4451#
```

قوف نوکي قفنل ان ام، VPN ةسلج عاشن لئغشتب موقت يتل او، TACACS ةمزح IOS لسري تهتنا دق قفنل نام لوالا ةلحرمل نا دكؤي هن. ديدخت جاحسمل ال لعتي أراتن اذه

```
ISR4451#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.48.17.87 10.48.23.68 QM_IDLE 1962 ACTIVE
```

```
IPv6 Crypto ISAKMP SA
```

```
ISR4451#
```

اهري فشت كفو مزحل ريفشت متي و، لئغشتل دي ق 2 ةلحرمل نوكت

```
ISR4451#sh cry ipsec sa
```

```
interface: GigabitEthernet0/0/0
Crypto map tag: MAP, local addr 10.48.23.68

protected vrf: (none)
```

```

local ident (addr/mask/prot/port): (10.48.23.68/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.48.17.87/255.255.255.255/0/0)
current_peer 10.48.17.87 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
#pkts decaps: 48, #pkts decrypt: 48, #pkts verify: 48
#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.: 10.48.23.68, remote crypto endpt.: 10.48.17.87
plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
current outbound spi: 0x64BD51B8(1690128824)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xFAE51DF8(4209319416)
  transform: esp-aes esp-sha256-hmac ,
  in use settings ={Transport, }
  conn id: 2681, flow_id: ESG:681, sibling_flags FFFFFFFF80004008, crypto map: MAP
  sa timing: remaining key lifetime (k/sec): (4607998/3127)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x64BD51B8(1690128824)
  transform: esp-aes esp-sha256-hmac ,
  in use settings ={Transport, }
  conn id: 2682, flow_id: ESG:682, sibling_flags FFFFFFFF80004008, crypto map: MAP
  sa timing: remaining key lifetime (k/sec): (4607997/3127)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

```

```
ISR4451#
```

## ESR

ليغشت ال دي قى لوالا ةلحرمل ال ESR، لىل ع تاجخرم ال س فن نم ققحت ال نكمي:

```

ise-esr5921#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.48.17.87  10.48.23.68  QM_IDLE       1002 ACTIVE

```

```
IPv6 Crypto ISAKMP SA
```

```
ise-esr5921#
```

حاجن ب اهري فشت ك فو مزحل ريفشت متي وو، ليغشت ال دي قى 2 ةلحرمل نوكت:

```
ise-esr5921#sh cry ipsec sa
```

```
interface: Ethernet0/0
  Crypto map tag: radius, local addr 10.48.17.87

protected vrf: (none)
local ident (addr/mask/prot/port): (10.48.17.87/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.48.23.68/255.255.255.255/0/0)
current_peer 10.48.23.68 port 500
  PERMIT, flags={}
#pkts encaps: 48, #pkts encrypt: 48, #pkts digest: 48
#pkts decaps: 48, #pkts decrypt: 48, #pkts verify: 48
#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.: 10.48.17.87, remote crypto endpt.: 10.48.23.68
plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xFAE51DF8(4209319416)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x64BD51B8(1690128824)
  transform: esp-aes esp-sha256-hmac ,
  in use settings ={Transport, }
  conn id: 3, flow_id: SW:3, sibling_flags 80000000, crypto map: radius
  sa timing: remaining key lifetime (k/sec): (4242722/3056)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xFAE51DF8(4209319416)
  transform: esp-aes esp-sha256-hmac ,
  in use settings ={Transport, }
  conn id: 4, flow_id: SW:4, sibling_flags 80000000, crypto map: radius
  sa timing: remaining key lifetime (k/sec): (4242722/3056)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
ise-esr5921#
```

## إي سي إي (ISE) فاشك تامدخ كرحم

إي سي إي PAPI ASCII ةقداصم يلى ةرشابم ال ةقداصم ال ريشت

Logged Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...
Feb 23, 2017 04:59:08.171 PM	✓		alice	Authorization		Tacacs_Default >> Admin_Access	ISE22-2ek	ISR_4451
Feb 23, 2017 04:59:08.032 PM	✓		alice	Authentication	Tacacs_Default >> Default >> Default		ISE22-2ek	ISR_4451

تمت يتيلاو ISE رادصالاب ةصاخال GE1 ةهجاو يلع اهطاقتلا مت يتيلا تاطاقتلالا دكؤت صن يي TACACS لوكوتورب دوچوم مدع، TACACS و ESP لوكوتورب مادختساب اهتيفصت: تانايايبلارورم تاكرح عيمج ريفشت متي و، حضاو

No.	Time	Source	Destination	Protocol	Length	Info
19	2017-02-23 17:07:32.507137	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
20	2017-02-23 17:07:32.507931	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
21	2017-02-23 17:07:32.508670	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
22	2017-02-23 17:07:32.508777	10.48.23.68	10.48.17.87	ESP	138	ESP (SPI=0x64bd51b8)
23	2017-02-23 17:07:32.509295	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
24	2017-02-23 17:07:32.514016	10.48.17.87	10.48.23.68	ESP	138	ESP (SPI=0xfae51df8)
26	2017-02-23 17:07:32.715546	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
37	2017-02-23 17:07:34.739569	10.48.23.68	10.48.17.87	ESP	122	ESP (SPI=0x64bd51b8)
38	2017-02-23 17:07:34.795997	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
42	2017-02-23 17:07:35.324360	10.48.17.87	10.48.23.68	ESP	122	ESP (SPI=0xfae51df8)
43	2017-02-23 17:07:35.324394	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
44	2017-02-23 17:07:35.325050	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
45	2017-02-23 17:07:35.325151	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
46	2017-02-23 17:07:35.326705	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
48	2017-02-23 17:07:35.460148	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
49	2017-02-23 17:07:35.460850	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
50	2017-02-23 17:07:35.461600	10.48.23.68	10.48.17.87	ESP	106	ESP (SPI=0x64bd51b8)
51	2017-02-23 17:07:35.461616	10.48.23.68	10.48.17.87	ESP	170	ESP (SPI=0x64bd51b8)
52	2017-02-23 17:07:35.462195	10.48.17.87	10.48.23.68	ESP	106	ESP (SPI=0xfae51df8)
53	2017-02-23 17:07:35.616897	10.48.17.87	10.48.23.68	ESP	138	ESP (SPI=0xfae51df8)

## اهحالصاو ءاطخال فاشكتسا

IPSec ءاطخال فاشكتسال ةعئاشلال اھحالصاو VPN ءاطخال فاشكتسأ ةينقت قي ببطت نكمي هاندأ ةديفم قئاثو يلع روثعال كنكمي. اھحالصاو

[ءاطخال فاشكتسأ PSKs عم عقوم يلا عقوم نم VPN ةكبش IOS IKEv2 ءاطخال ححصت تاي لمع اھحالصاو TechNote](#)

[ASA IKEv2 ءاطخال ححصت PSKs عم عقوم يلا عقوم نم VPN ةكبش](#)

[اهمادختساو ءاطخال ححصت رم او مهف: اھحالصاو IPsec ءاطخال فاشكتسأ](#)

## SVTI (ىل DVTI نم) FlexVPN ةكبش عقوم يلا عقوم نيوكت ISE 2.2 و NAD نيپ

ططخملا مادختسا متي. FlexVPN مادختساب RADIUS تانايايبلارورم ةكرح ةيامح نكمي امك يليلال لاثملا يي يليلال

10.48.23.68



Interface lo0 – 100.100.100.100

IPSEC Tunnel

Radius/Tacacs

10.48.26.170



Interface Tap0 – 10.1.1.2

انه لي صاف لال نم ديزم يلع روثع لال نكمي .مات لال حوض ولاب FlexVPN ة ئيه ت مستت

<http://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html>

## Flex VPN ميمصت ايازم

- مظعم حيتت .كيدل ة قباس لال VPN IPsec تاكبش عيمج يلع Flex ليغشت كنكمي نرمل رادصل او قباس لال نيوكت لال عم شيعات لال ة ينالكم تاهوي رانيس لال
- لوكوت ورب نم يناث لال رادصل لال ة نرمل لال (VPN) ة ره اظلال ة صاخلال ة كبش لال دنست نيسحت يلع لمعي يذال ، (IKEv1) تنرتن لال لوكوت ورب نم لوألال رادصل لال لال سيلو IKEv2 ابيرقت لوكوت ورب لال رارق تساو صوافت لال بناوج عيمج
- دحاو لمع راطل ي ف اه قيقحت نكمي ة ددعت م فئاظو .
- و اتاسايس ديدحت لال جاتحت ال - ة قطنم ة يضارتفا تاداعل مادختساب ة ئيه تال ة لوهس متو ة قطنم ة يضارتفا تاداعل ين ب دق IKEv2 ن لب ، كلذ لال امو ليوحت تاعومجم اهثيدحت

## ءجوم لال نيوكت

```
aaa new-model
!
!
aaa group server tacacs+ ISE_TACACS
server name ISE22_VRF
ip vrf forwarding TACACS
!
aaa authentication login default group ISE_TACACS
aaa authorization exec default group ISE_TACACS
aaa authorization network default local
!
crypto ikev2 authorization policy default
route set interface Loopback0
no route set interface
!
!
crypto ikev2 keyring mykeys
peer ISE22
address 10.48.17.87
pre-shared-key Krakow123
!
!
!
crypto ikev2 profile default
match identity remote address 10.48.17.87 255.255.255.255
authentication remote pre-share (with the command authentication remote pre-share key in place
```

```
keyring is not required)
 authentication local pre-share
 keyring local mykeys
 aaa authorization group psk list default default
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
crypto ipsec profile default
 set ikev2-profile default (it is default configuration)
!
!
!
interface Loopback0
ip vrf forwarding TACACS
 ip address 100.100.100.100 255.255.255.0
!
interface Tunnel0
ip vrf forwarding TACACS
 ip address 10.1.12.1 255.255.255.0
 tunnel source GigabitEthernet0/0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.48.17.87
 tunnel protection ipsec profile default
!
interface GigabitEthernet0/0/0
 ip address 10.48.23.68 255.255.255.0
 negotiation auto
!
!
ip route 0.0.0.0 0.0.0.0 10.48.23.1
ip tacacs source-interface Loopback0
!
!
tacacs server ISE22_VRF
 address ipv4 10.1.1.2
 key cisco
!
ISR4451#
```

## ISE على ESR نيوكت

```
ise-esr5921#sh run
Building configuration...
```

```
Current configuration : 5778 bytes
```

```
!
! Last configuration change at 17:32:58 CET Thu Feb 23 2017
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service call-home
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
```

```
!  
!  
no aaa new-model  
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2  
clock timezone CET 1 0  
mmi polling-interval 60  
no mmi auto-configure  
no mmi pvc  
mmi snmp-timeout 180  
call-home  
    ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com  
    ! the email address configured in Cisco Smart License Portal will be used as contact email  
    address to send SCH notifications.  
    contact-email-addr sch-smart-licensing@cisco.com  
    profile "CiscoTAC-1"  
    active  
    destination transport-method http  
    no destination transport-method email  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
ip cef  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
crypto pki trustpoint SLA-TrustPoint  
    enrollment pkcs12  
    revocation-check crl  
!  
!  
crypto pki certificate chain SLA-TrustPoint  
    certificate ca 01  
    30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030  
    32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363  
    6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934  
    3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305  
    43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720  
    526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030  
    82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D  
    CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520  
    1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE  
    4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC  
    7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188  
    68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
```



```
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
```

quit

```
license udi pid CISCO5921-K9 sn 98492083R3X
username lab password 0 lab
!
redundancy
!
!
!
crypto keyring MVPN-spokes
  pre-shared-key address 0.0.0.0 0.0.0.0 key Krakow123
crypto ikev2 authorization policy default
  route set interface
  route set remote ipv4 10.1.1.0 255.255.255.0
!
!
!
crypto ikev2 keyring mykeys
  peer ISR4451
  address 10.48.23.68
  pre-shared-key Krakow123
!
!
!
crypto ikev2 profile default
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local mykeys
  aaa authorization group psk list default default local
  virtual-template 1
!
!
crypto isakmp policy 10
  encr aes
  hash sha256
  authentication pre-share
  group 16
!
crypto isakmp policy 20
  encr aes
  hash sha256
  authentication pre-share
  group 14
crypto isakmp key Krakow123 address 0.0.0.0
crypto isakmp profile MVPN-profile
  description LAN-to-LAN for spoke router(s) connection
  keyring MVPN-spokes
  match identity address 0.0.0.0
!
!
```

```
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
 mode transport
!
!
!
crypto dynamic-map MVPN-dynmap 10
 set transform-set radius radius-2
!
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
!
!
!
!
interface Loopback0
 ip address 10.1.12.2 255.255.255.0
!
interface Ethernet0/0
 description e0/0->connection to external NAD
 ip address 10.48.17.87 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 no ip route-cache
 crypto map radius
!
interface Ethernet0/1
 description e0/1->tap0 internal connection to ISE
 ip address 10.1.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet0/2
 description e0/2->connection to CSSM backend license server
 no ip address
 ip virtual-reassembly in
 no ip route-cache
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Virtual-Templatel type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
ip route 0.0.0.0 0.0.0.0 10.48.17.1
!
```

```
!  
!  
access-list 1 permit 10.1.1.0 0.0.0.3  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
line con 0  
  logging synchronous  
line aux 0  
line vty 0 4  
  login  
  transport input none  
!  
!  
end
```

## FlexVPN مېمصة تارابتعا

- ل E0/0 ةهجاو يه يتلاو، ل ISE ل G0/1 ةهجاو ل Radius لاصتا اهان بجي تالاحل مظعم في م ادختساب ةديفملا رورملا ةكرح فيرعت بجي، ريفشتلا طئارخ م ادختسا انثأ ESR. ةهجاو ل نيت هجوم نيوكت مت اذ، لمعي نل. هيجوتلا م ادختساب - SVTI عم، لوصولا مئوق سفن قبطنت. (قفنلا اشن) ةهجاو ل ربع ةدحاو (رفشي) قفنلا ربع ةدحاو ISE هجوملا نيوكت لعل ةلكشملا.
- ةهجاو ني ب (Encrypted Radius) مامتهال ل ةريثملا رورملا ةكرح ليصوت متي ببسلا اذلو، ببسلا اذلو. (ESR لعل ةلحال هذه في nat لى ل ةحال) ل ISE ل Tap0 ةهجاو، هجومل ل Lo0 ربع رورملا لعل RADIUS رورم ةكرح رابحال، تنرتنل لوكوتورب راسم نيوكت نكمي ريفشتلا لعل لوصحلاو قفنلا.
- في هعضو نكمي في، (10.1.1.2) تباث ISE ب ةصاخلا Tap0 ةهجاو ب صاخلا IP ناو نع نا امب قفنلا لالخنمو TACACS ل طقف اذو IP ناو نع لاصتالا ثودح نامضل، هجوملا لعل VRF طقف.

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. ةصاأل مه تلبل  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لاعل او  
ىل إأمئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزلچنل دن تسمل