

AnyConnect ميسيقتلا ءانثتسا نيوكت FlexVPN مادختساب ISE

تايوتحمل

[تمدقمل](#)

[قيسسالاتابلطممل](#)

[تابلطممل](#)

[تمدخلتسملاتانوكمل](#)

[نيوكتل](#)

[ةكبشيلطيطختلامسيل](#)

[تانيوكتل](#)

[فوجولانيوكت](#)

[\(ISE\) قيوهلا تامدخلكرحمنيوكت](#)

[تحصلاتنم قرحتل](#)

[اهحالص او عاطخألا فاشكتس](#)

[عجارمل](#)

تمدقمل

لاصتال IKEv2 مادختساب ميسيقتلا ءانثتسا نيوكت عارجإ دنتسملا اذه فصي AnyConnect Cisco IOS® XE.

قيسسالاتابلطممل

تابلطممل

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكتنأب Cisco يصوت:

- ججوم ىلع AnyConnect IPsec نيوكت ةبرجت
- Cisco (ISE) نم قيوهلا تامدخلكرحمنيوكت
- Cisco (CSC) نم نمآلاليمعلا
- RADIUS لوكوتورب

تمدخلتسملاتانوكمل

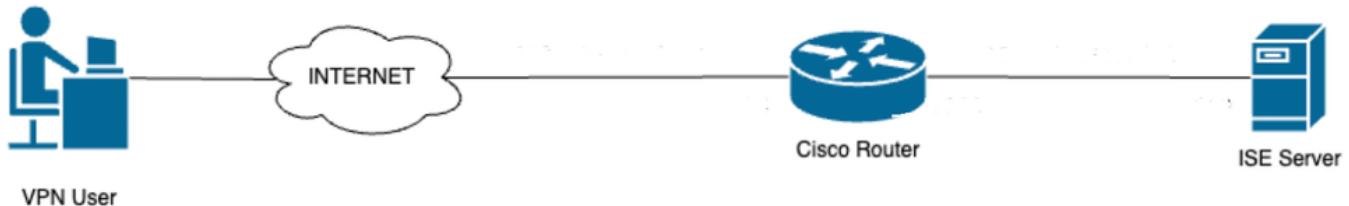
ةيلاتلا ئداملا تانوكمل او جماربللا تارادصا ىلإ دنتسملا اذه يف ةدراولا تامولعمل دنتسست:

- Cisco Catalyst 8000V (C8000V) - 17.12.04
- Cisco Secure Client - 5.0.02075
- Cisco ISE - 3.2.0
- Windows 10 ليغشتلا ماظن

ةـصـاخـ ةـيـلـمـعـ مـ ةـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ ءـاعـشـنـاـ مـتـ
تـنـاـكـ اـذـاـ.ـ(ـيـضـارـتـفـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ
رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

نـيـوـكـتـلـاـ

ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ

تـانـيـوـكـتـلـاـ

مـاسـقـأـلـاـ هـذـهـ رـابـتـعـاـلـاـ يـفـ عـضـ،ـنـيـوـكـتـلـاـ لـامـكـاـ لـجـأـ نـمـ.

هـجـوـمـلـاـ نـيـوـكـتـ

1. زـاهـجـلـاـ ىـلـعـ يـلـحـمـلـاـ لـيـوـخـتـلـاـوـ ةـقـدـاصـمـلـلـ RADIUSـ مـدـاخـ نـيـوـكـتـ:

```
radius server ISE
address ipv4 10.127.197.105 auth-port 1812 acct-port 1813
timeout 120
key cisco123

aaa new-model
aaa group server radius FlexVPN_auth_server
server name ISE

aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network a-eap-author-grp local
```

2. يـهـ هـجـوـمـلـاـ ةـيـلـحـمـلـاـ ةـقـدـاصـمـلـاـ نـأـ اـمـبـ.ـهـجـوـمـلـاـ ةـدـاهـشـ تـيـبـثـتـلـ اـهـ قـوـثـومـ ةـطـقـنـ نـيـوـكـتـ.
عـوـجـرـلـاـ كـنـكـمـيـ.ـةـدـاهـشـ مـادـخـتـسـاـبـ هـسـفـنـ ةـقـدـاصـمـبـ مـدـاخـلـاـ مـوـقـيـ نـأـ زـاهـجـلـاـ بـلـطـتـيـ،ـRSAـ عـونـ
لـيـصـافـتـلـاـ نـمـ دـيـزـمـ ىـلـعـ لـوـصـحـلـلـ [PKI-2](#)ـ لـ [PKI-1](#)ـ لـ دـاهـشـلـاـ لـيـجـسـتـ وـ [PKI-1](#)ـ لـ دـاهـشـلـاـ لـيـجـسـتـ ىـلـ
ةـدـاهـشـلـاـ ءـاعـشـنـاـ لـوـحـ:

```
crypto pki trustpoint flex
enrollment terminal
ip-address none
subject-name CN=flexserver.cisco.com
```

```
revocation-check none
rsakeypair flex1
hash sha256
```

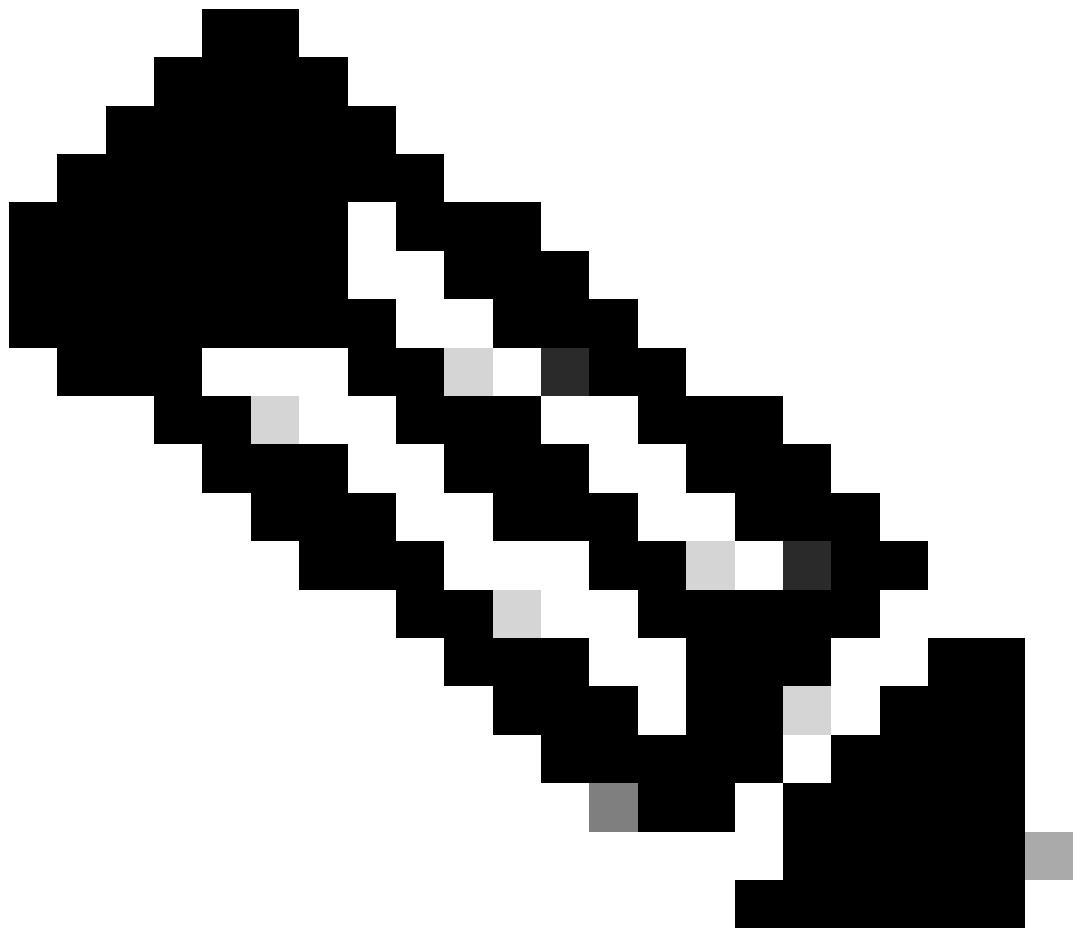
3. دنع AnyConnect VPN لاصتا ئىلەنلا بىيىعتل يىلەنلا IP عەمچىت دەجىنلە:

```
ip local pool ACPPOOL 172.16.10.5 172.16.10.30
```

4. IKEv2 ل ئىلەن صىخىرت ئەسلىق ئاشناب مۇق:

ىلۇغ Radius مەداخ نەم اھىفدىت يىتلە تامىسىلا اذە يىف ئەدەم جەنلە ئەم جەنلە قىيىبىت مەتىنىيەمدىختىسىلە

```
crypto ikev2 authorization policy ikev2-auth-policy
pool ACPPOOL
dns 8.8.8.8
```



جەن مادختسە مەتى ، صىخەملا IKEv2 لىيۆخت جەن نىوكت مەدع ۋەلاج يىف : ئەظحالم تامسلا عفدىنىڭ كەمىي . لىيۆختللى يىضارتفالا ئىمسىي يىذلا يىضارتفالا لىيۆختللا - لىصف ۋەمىس عفدىلىا جاتحت IKEv2 ربع مەداخ . RADIUS نىمۇض ۋەدەجملا مەداخ نەم ئانىتىسى رADIUS.

تايىضارتفالا مادختسە مەتى ، ھەنئىوكت مەدع ۋەلاج يىف) IKEv2 جەن وەرتقىم ئاشنا . (يەرایىتىخ) 5 ئەي كەذلە:

```
crypto ikev2 proposal IKEv2-prop1
    encryption aes-cbc-256
    integrity sha256
    group 19
```

```
crypto ikev2 policy IKEv2-pol
    proposal IKEv2-prop1
```

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac  
mode tunnel
```

يرهاظل لوصولا تاهج او موقت .يمه و IP ناونع مادختساب عاجرسا ٰهجاو نيوكتب مق 7:
هـنـم IP نـاـونـع ضـارـتـقـابـ

```
interface Loopback100  
    ip address 10.0.0.1 255.255.255.255
```

8: يەھاظللا لوصوللا تاھجاو خسەن هلالخ نم متي پەرەاظ بلاق نیوکت.

```
interface Virtual-Template100 type tunnel  
    ip unnumbered Loopback100  
    ip mtu 1400
```

فيريغتلا فلم ددح و هجوملل ديهمتلل اوركاڈ ای AnyConnect ليمع فيريعت فلم ليمحتب مق 9: حضور وہ امک

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

لاصتاً اب قلعتملا تامولعملاء يموج لعل يوتحي IKEv2 فـيـرـعـت فـلـمـ نـيـوـكـرـنـيـقـ.

```
crypto ikev2 profile prof1
match identity remote key-id *$AnyConnectClient$*
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint flex
aaa authentication eap FlexVPN_auth
aaa authorization group eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user eap cached
virtual-template 100
anyconnect profile acvpn
```

KEV2: افريقيا فلم رصانعلا هذه مادختساً متّي و

- ليمعل اقيوهه اىلا ريشي - *\$AnyConnectClient\$* حاتفممل ديعبلا ئي وهل ا فرعم ئقباطم عونلا نم ئي ضارت فالا IKE key-id.
 - ئقباطمل AnyConnect فلم يف اي ودي ئي وهل ا هذه رئيغت نكمي ، كلذ عم و رشنلا تاجايتحا.
 - ليمعل ا ئقداصمل EAP لوكوتورب مادختسا بجي هنأ اىلا ريشي - دعب نع ئقداصمل ا.
 - ئيلحمل ا ئقداصمل تاداهشلا مادختسا بجي هنأ ركذت - ئيلحمل ا ئقداصمل ا.
 - AAA Authentication EAP - ئقداصم عانثأ - FlexVPN_AUTH مداخل RADIUS.
 - ئكبشلا ئمهماق مادختس ، ليوختلا عانثأ - AAA ضيوفت ئعومجمب ئصالخا EAP a-EAP-author-GRP ليوختلا ikev2-auth-policy.
 - مادختسمل ا نم ينمضا ليوخت نيكمنت - اتقؤم انيرخت لماعتسملا ليوخت.
 - خسن متيس يرهاظلا بلاقلا يأ ددحي - 100 يرهاظلا بلاقلا.
 - ان هـ 9. ئوطخل ايف ددحمل ا ليمعل ا فيرعت فلم قي بط متي - اذه AnyConnect Profile acvpn.
- انه 9. ئوطخل ايف ددحمل ا ليمعل ا فيرعت فلم قي بط متي - اذه AnyConnect Profile acvpn.

11. فيرعت فلم نيوك:

```
crypto ipsec profile AnyConnect-EAP
set transform-set TS
set ikev2-profile prof1
```

12. يرهاظلا بلاقلا اىلا IPsec فيرعت فلم ئفاضا:

```
interface Virtual-Template100 type tunnel
tunnel mode ipsec ipv4
tunnel protection ipsec profile AnyConnect-EAP
```

13. جوملا اىلع HTTP-URL مداخلو HTTP اىلا دنتسملا ئدادشلا شحب ليطبعتب مق:

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

14. فيرعتلا IP WAN SSL ددحو جوملا بصالخا SSL نيوكتب مق:

```
crypto ssl policy ssl-server
pki trustpoint flex sign
ip address local 10.106.67.33 port 443

crypto ssl profile ssl_prof
```

```
match policy ssl-server
```

فيريغت فلم XML (AnyConnect) فيريغت فلم نم ٰصاصلق

لابقتسالا ٰدحو نم فيريغت لايزنٰت رفوت ال، Cisco IOS XE 16.9.1، فلم تاليزنٰت رفوت ال، 16.9.1، دعب ثبل او لابقتسالا، ثبل او.

```
<#root>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>

<HostName>
flex
</HostName>
<HostAddress>
```

flexserver.cisco.com

```
</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
```

EAP-MD5

```
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

نويوكت (ISE) تامدخ كرحم نويوكت

ل كرتشمل ارسلا حاتفملا نويوكتب مقو ISE ىلع حلاص ئاكبىش زاهجك هجوملا لجس. نويوكتل ئفاضا قوف رقنا. ئاكبىشلا دراوم > ئارادا ىل لقتنا، اذهل AAA: RADIUS،

The screenshot shows the 'Network Device' configuration page in Cisco ISE. The device is named '8kv-33'. The 'Network Device Group' is set to 'All Locations'. Under 'RADIUS Authentication Settings', the 'Protocol' is set to 'RADIUS' and the 'Shared Secret' field contains a redacted password. The 'CoA Port' is set to 1700.

Setting	Value										
Name	8kv-33										
Description	(empty)										
IP Address	10.106.67.33 / 32										
Device Profile	Cisco										
Model Name	C8000v										
Software Version	17.12.4										
Network Device Group	All Locations										
Location	All Locations										
IPSEC	No										
Device Type	All Device Types										
RADIUS Authentication Settings	<table border="1"><thead><tr><th>Protocol</th><th>RADIUS</th></tr></thead><tbody><tr><td>Shared Secret</td><td>.....</td></tr><tr><td>Use Second Shared Secret</td><td><input type="checkbox"/></td></tr><tr><td>Second Shared Secret</td><td>.....</td></tr><tr><td>CoA Port</td><td>1700</td></tr></tbody></table>	Protocol	RADIUS	Shared Secret	Use Second Shared Secret	<input type="checkbox"/>	Second Shared Secret	CoA Port	1700
Protocol	RADIUS										
Shared Secret										
Use Second Shared Secret	<input type="checkbox"/>										
Second Shared Secret										
CoA Port	1700										

ئاكبىش زاهج ئفاضا

نويوكت (ISE) تامدخ كرحم نويوكت:

نومساقتى نيذل او قلثامم صئاصخ بنيمدختسملا نارقال ئي وهلا تاعومجم فيرعتب مقو ئي وهلا ئارادا > ئارادا ىل لقتنا. ئيلاتلا تاوطلخا يف رصانعلا هذه مادختسما متى. قلثامم نوذا > ئفاضا قوف رقنا مث، مدخلتسملار ئي وهلا تاعومجم > تاعومجم:

es Groups External Identity Sources Identity Source Sequences Settings

User Identity Groups > AC_Split_test

Identity Groups

Identity Group

* Name **AC_Split**

Description

Save Reset

ةيوهلا ةعومجم عاشنإ

3. ةيوهلا تابعه ةعومجم بني مدخلت سملانارقا:

> تابعه ةيوهلا > ةيوهلا ةرادا > ةيوجهلا ةعومجم بني مدخلت سملانارقا.

ةيوهلا ةعومجم ئلا مدخلت سملانارقا

4. تاسايس ةعومجم عاشنإ:

لاثملانارقا اذه يف. ةسمايسلا قباطت يتلا طورشلا ديدحت و ةديدج تاسايس ةعومجم ديدحتب مق تابعه ةعومجم جهنلائلا لقتنا، كلذب مايقلل. طورشلا تحت ةزهجألا عاونأ عيمجب حامسلانارقا:

Policy Sets						Reset	Reset Policyset Hitcounts	Save
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View	
<input type="text"/> Search								
<input checked="" type="checkbox"/>	AnyConnect_C8000v_Policy		DEVICE-Device Type EQUALS All Device Types	Default Network Access	4			

جنهن ةعومجم عاشنإ

5. ليوطت ةسمايس عاشنإ:

تابعه ةعومجم نيمضت نم دكأت. جنهنلا ةقباطمل ةبولطملا طورشلاب ديدج ليوطت جنهن ديدحتب مق طرشك 2 ةوطخلاب يف اهؤاشنإ مت يتلا ةيوهلا.

The screenshot shows the Cisco Umbrella Policy Editor. At the top, there's a search bar and a navigation bar with the following items: AnyConnect_C8000v_Policy, DEVICE-Device Type EQUALS All Device Types, Default Network Access, and a plus sign icon with the number 4. Below the navigation bar, there's a tree view of policies:

- > Authentication Policy (1)
- > Authorization Policy - Local Exceptions
- > Authorization Policy - Global Exceptions
- ✓ Authorization Policy (2)

Under the 'Authorization Policy (2)' node, there's a 'Results' table:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	AC_Split_Users	AND DEVICE-Device Type EQUALS All Device Types IdentityGroup-Name EQUALS User Identity Groups:AC_Split	Select from list	Select from list	4	
✓	Default		DenyAccess	Select from list	0	

لیوختلا ةسایس عاشنإ

The screenshot shows the Cisco Umbrella Policy Editor with two main panes: 'Library' and 'Editor'.

Library: A sidebar listing various network access policies:

- 5G
- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed

Editor: The main pane where policies are built. It shows a complex condition being constructed:

```

AND
  DEVICE-Device Type
    Equals All Device Types
  IdentityGroup-Name
    Equals User Identity Groups:AC_Split
  +
  Set to 'Is not'
  NEW AND OR
  
```

Buttons at the bottom right include 'Duplicate', 'Save', 'Close', and a large blue 'Use' button.

لیوختلا جهـن يـف طورـش رـايـتـخـا

6. لـيـوـخـتـ فـيـرـعـتـ فـلـمـ عـاـشـنـإـ:

لـيـوـخـتـ ةـسـاـيـسـ ةـقـبـاطـمـ دـنـعـ اـهـذـاخـتـاـ مـتـيـ يـتـلـاـ تـاءـارـجـإـلـاـ لـيـوـخـتـلـاـ فـيـرـعـتـ فـلـمـ نـمـضـتـيـ:ـةـيـلـاتـلـاـ تـامـسـلـاـ نـمـضـتـيـ دـيـدـجـ لـيـوـخـتـ فـيـرـعـتـ فـلـمـ عـاـشـنـإـ

لـوـصـولـاـ عـونـ = ACCESS_ACCEPT

Cisco-av-pair = ipsSec:split-exclude= IPv4 <ip_network>/<subnet_mask>

Results

Status	Rule Name	Conditions	Profiles	Security Groups	Hits
<input checked="" type="radio"/>	AC_Split_Users	AND DEVICE-Device Type EQUALS All Device Types IdentityGroup-Name EQUALS User Identity Groups:AC_Split	Select from list	Select from list	4
<input checked="" type="radio"/>	Default		Create a New Authorization Profile	Select from list	0

دیج لیوخت فیرعت فلم عاشن

Authorization Profile

* Name **AC_Router_Split**

Description Split exclude for AC users

* Access Type **ACCESS_ACCEPT**

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

لیوختلا فیرعت فلم نیوکت

Advanced Attributes Settings

Cisco:cisco-av-pair = ipsec:split-exclude= ipv4 ...

Cisco:cisco-av-pair = ipsec:split-exclude= ipv4 ...

ipsec:split-exclude= ipv4
192.168.2.0/255.255.255.0

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0
cisco-av-pair = ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0

لیوختلا فیرعت فلم یف تامسلا نیوکت

لیوختلا فیرعت فلم نیوکت ۃعجارم 7.

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles (highlighted)

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profile

* Name: AC_Router_Split

Description: Split exclude for AC users

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: (checkbox)

Track Movement: (checkbox)

Agentless Posture: (checkbox)

Passive Identity Tracking: (checkbox)

> Common Tasks

> Advanced Attributes Settings

Cisco:cisco-av-pair = ipsec:split-exclude= ipv4 ...

Cisco:cisco-av-pair = ipsec:split-exclude= ipv4 ...

> Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0
 cisco-av-pair = ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0

لیوختلا فیرعت فلم نیوکت ةعجارم

8. ةبولطملا فیرعتلا تافلم دیدحت دعب جهناج یف لیوختلا ئومجم نیوکت وە اذە:

AnyConnect_C8000v_Policy DEVICE-Device Type EQUALS All Device Types Default Network Access

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

< Authorization Policy (2)

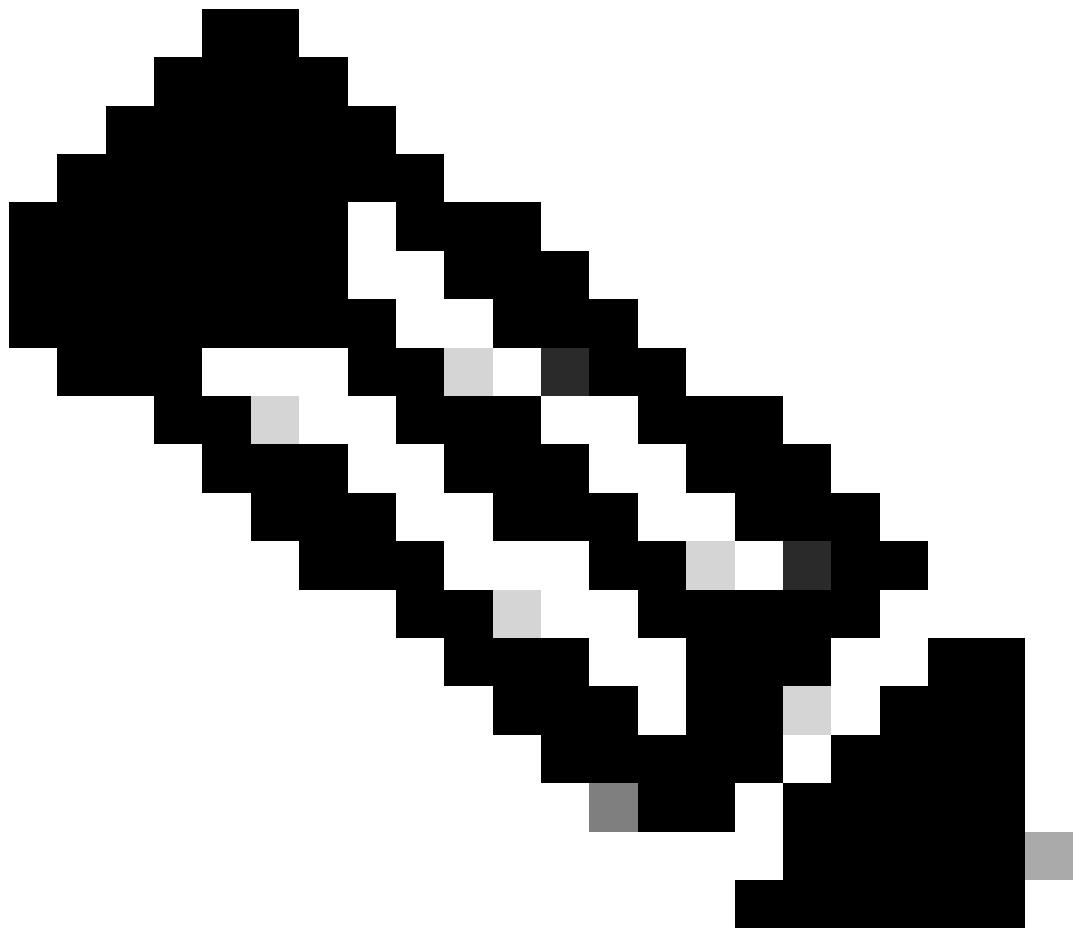
Results

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	AC_Split_Users	AND DEVICE-Device Type EQUALS All Device Types IdentityGroup-Name EQUALS User Identity Groups:AC_Split	AC_Router_Split (highlighted)	Select from list	4	
✓	Default		DenyAccess	Select from list	0	

Reset Save

لیوختلا جهناج یاھنلا نیوکتلما

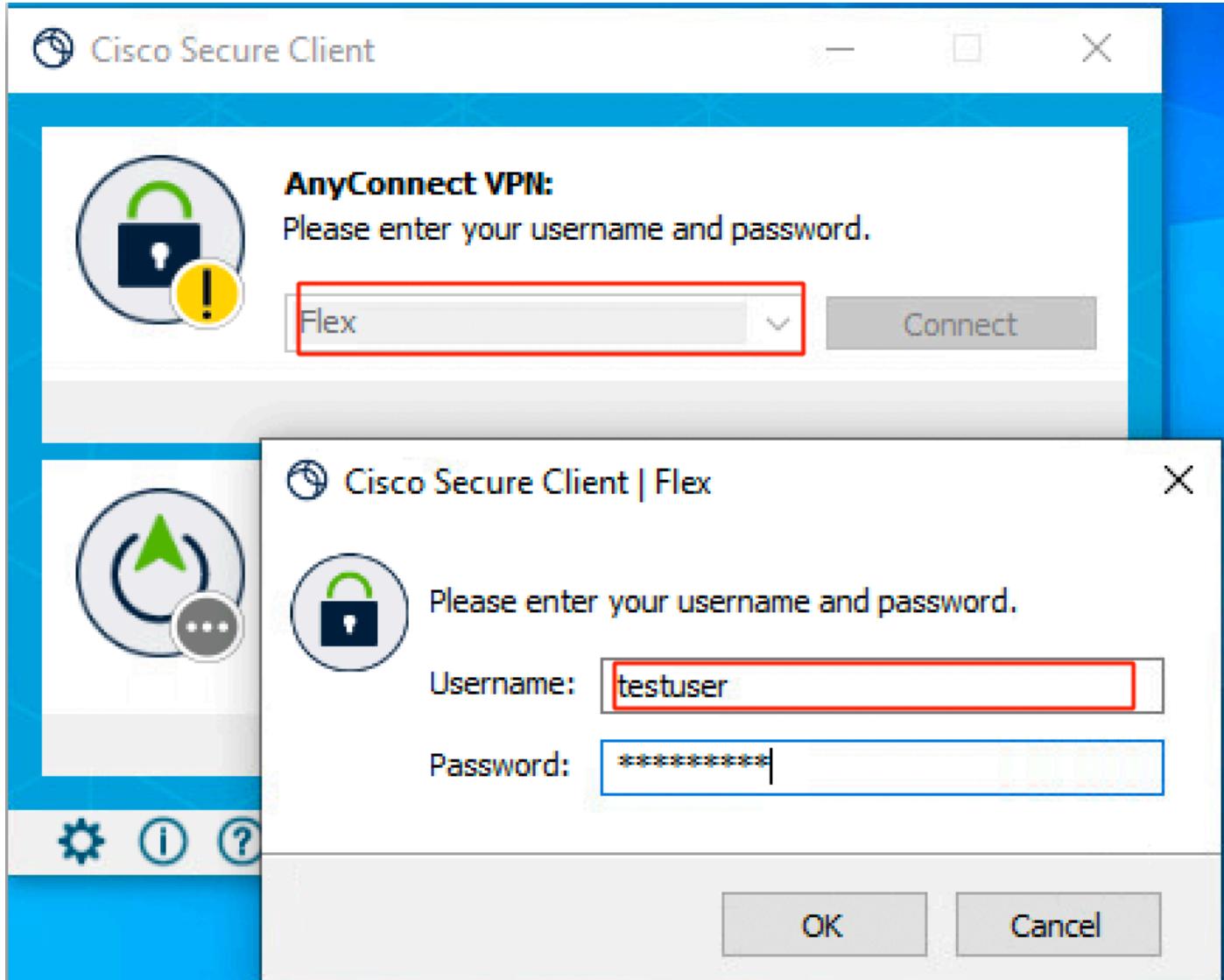
نیوکت لالخ نم VPN ۆكبش رباع رورملانم تاکبشلا داعبتسا کنکمی، اذە نیوکتلما لاثم عم مدختسملما اھیلا یمتنی یتلما ئیوهلا ئومجم ىلعمئاقلا ISE.



زاهج ىلإ ماسقنا إلأ عانثتسا ل طقف ةدح او ةيعرف ةكبش عفد نكمي :ةظحال Cisco IOS XE ب ةصالخا ثبلاولابقتتسا ل ةدحو مادختسا دنع ليمنع رتويبمكلا Cisco نم ءاطخألا حيحصت فرعم ةطساوب رمألا اذه ةجلاعم مت دقو. RA VPN. لاصتسا 17.12.4. نم عانثتسا-لصف تاذ ةددعتم ةيعرف تاكبش عفد نكمي و [CSCwj38106](#) عجا را. ةتباثلا تارادص إلأ لوح ليصافتلا نم ديزم ىلع لوصحلل ءاطخلا ىلإ.

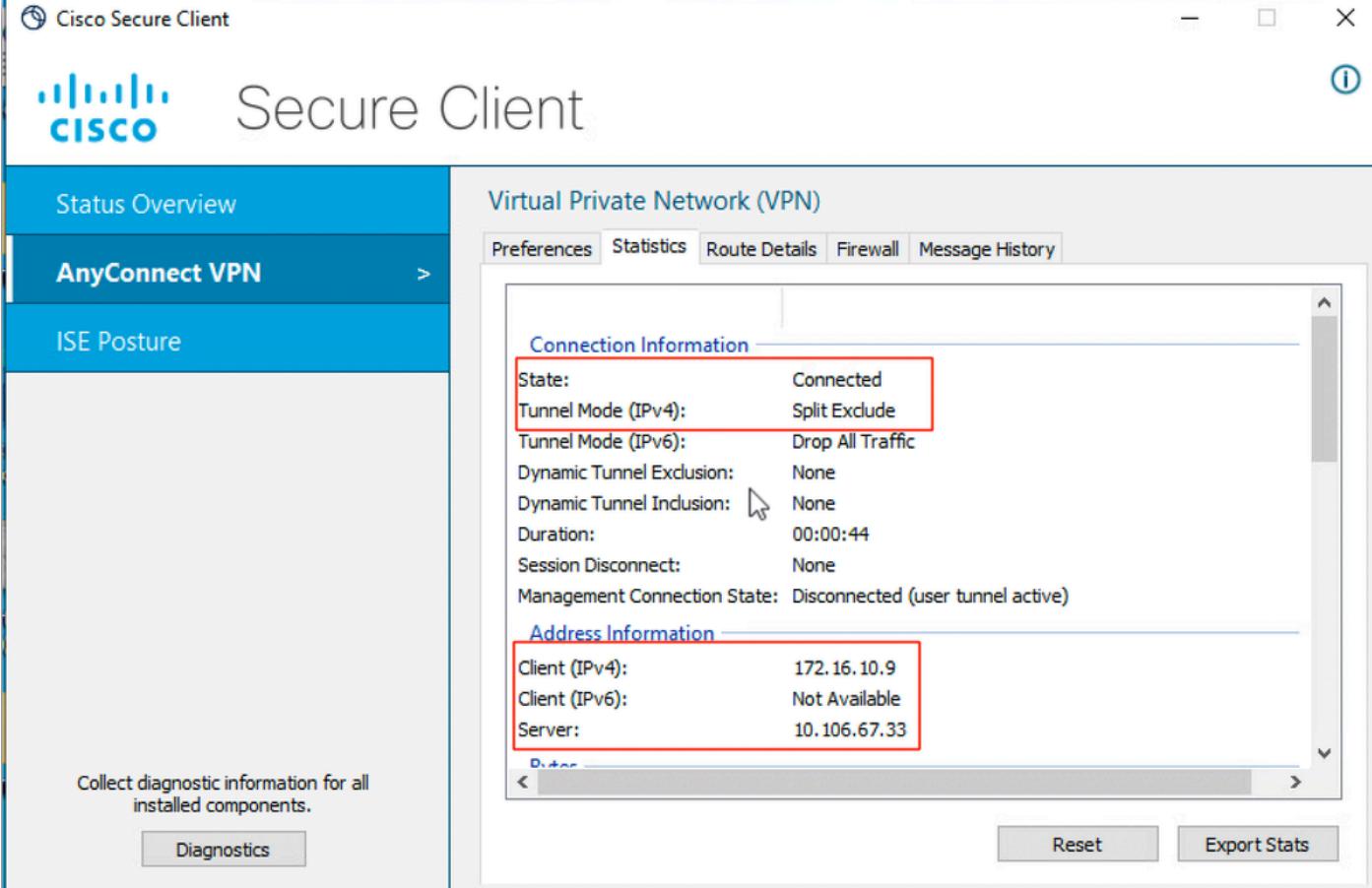
ةحصلانم ققحتلا

لالخ نم مدختسملأا رتويبمك نم C8000V زارتلاپ لاصتسا لاب مق ،ةقداصملأا رابتخلال. AnyConnect تانايبلخ داؤ.



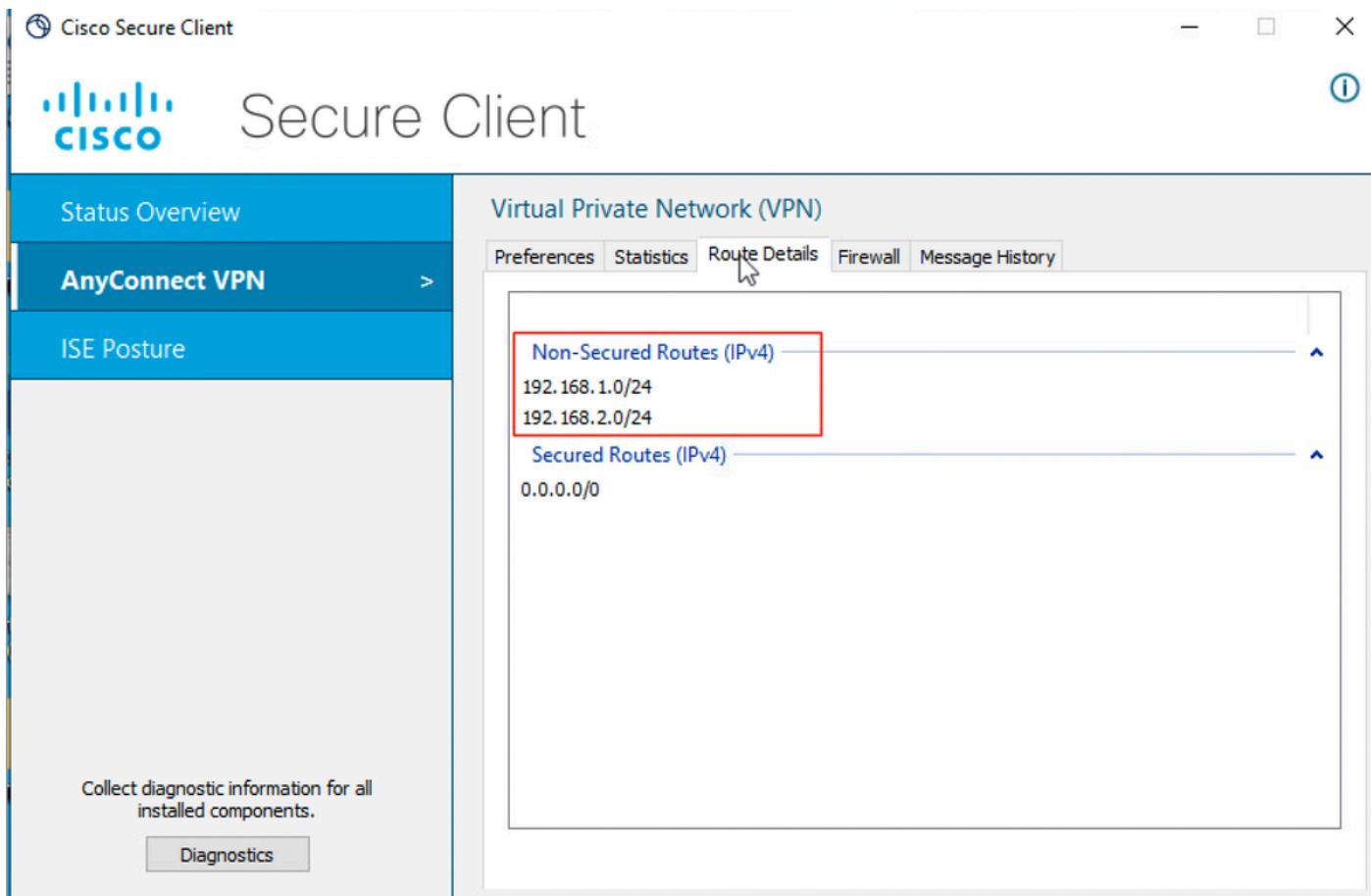
ىلى اىلوجسلى لىخدا AnyConnect

لقتناو (ىلفسلا ىرسىللا ۋىازلا) داتعىلا ئنوقىأ قوف رقنا، لاصتالا سىسىأت درجمب 2. مىسىقت دارملا قىفنلا عضو داعبتسى ديكأت AnyConnect VPN > Statistics ىلى.



تايئاصح إلأ ٰ حص نم ققحتلأ

قف اوتت ٰ ضورعملأ تامولعملا نأ نم دكأت و راسملأ ليصافت AnyConnect VPN > إلإ لقتنا ٰ نمآلأ ريغ تاراسملأو ٰ نمآلأ تاراسملأ ع



راسملـا ليـصـافـتـةـ حـصـنـمـ قـقـحـتـلـا

ةـكـبـشـلـاـبـ ةـصـاخـلـاـ ثـبـلـاـوـ لـابـقـتـسـالـاـ ةـدـحـوـىـلـعـ لـاصـتـالـاـ لـيـصـافـتـةـ نـمـ قـقـحـتـلـاـ كـنـكـمـيـ اـمـكـ (VPN):

1. IKEv2 parameters

```
<#root>
8kv#
show crypto ikev2 sa detail
```

```
IPv4 Crypto IKEv2 SA
```

```
Tunnel-id Local Remote fvrf/ivrf Status
```

```
1 10.106.67.33/4500 10.106.50.91/55811 none/none READY
```

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth verify: EAP
```

```
Life/Active Time: 86400/22 sec
```

CE id: 1012, Session-id: 6

Local spi: E8C6C5EEF0F0EF72 Remote spi: 7827644A7CA8F1A5

Status Description: Negotiation done

Local id: 10.106.67.33

Remote id: *\$AnyConnectClient\$*

Remote EAP id: testuser

Local req msg id: 0 Remote req msg id: 6

Local next msg id: 0 Remote next msg id: 6

Local req queued: 0 Remote req queued: 6

Local window: 5 Remote window: 1

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Dynamic Route Update: disabled

Extended Authentication configured.

NAT-T is detected outside

Cisco Trust Security SGT is disabled

Assigned host addr: 172.16.10.10

Initiator of SA : No

Post NATed Address : 10.106.67.33

PEER TYPE: Other

IPv6 Crypto IKEv2 SA

2.This is the crypto session detail for the VPN session:

<#root>

8kv#

show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

R - IKE Auto Reconnect, U - IKE Dynamic Route Update

S - SIP VPN

Interface: Virtual-Access1

Profile: prof1

Uptime: 00:00:44

Session status: UP-ACTIVE

Peer: 10.106.50.91 port 55811 fvrf: (none) ivrf: (none)

```
Phase1_id: *$AnyConnectClient$*
```

```
Desc: (none)
```

```
Session ID: 16
```

```
IKEv2 SA: local 10.106.67.33/4500 remote 10.106.50.91/55811 Active
```

```
Capabilities:NX connid:1 lifetime:23:59:16
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.10.10
```

```
Active SAs: 2, origin: crypto map
```

```
Inbound: #pkts dec'ed 114 drop 0 life (KB/Sec) 4607987/3556
```

```
Outbound: #pkts enc'ed 96 drop 0 life (KB/Sec) 4608000/3556
```

3. Verify on ISE live logs.

اھالص او عاطخألا فاشكتس ا

ع جوم ىل Cisco:

لابقتس الـ IKEv2 و IPsec نم ققحتلـ ضـ وافتـ لـ نـ مـ حـ يـ حـ صـ تـ مـ دـ خـ تـ سـ أـ .
لـ يـ مـ عـ لـ اوـ ثـ بـ لـ اوـ

```
debug crypto condition peer ipv4 <public_ip>
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

تامـ سـ لـ اـ نـ يـ يـ عـ تـ نـ مـ قـ قـ حـ تـ لـ لـ (AAA) ةـ بـ سـ اـ حـ مـ لـ اوـ ضـ يـ وـ فـ تـ لـ اوـ ةـ قـ دـ اـ صـ مـ لـ اـ عـ اـ طـ خـ اـ مـ دـ خـ تـ سـ اـ .
ةـ دـ يـ عـ بـ لـ اـ وـ اـ وـ ةـ يـ لـ حـ مـ لـ اـ

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

ىلـ ISE:

رسـابـمـلـا ثـبـلـا تـالـجـسـ > تـايـلـمـعـلـا ىـلـا لـقـنـتـلـابـ رـشـابـمـلـا RADIUS تـالـجـسـ مـدـخـتـسـأـ.

لمـعـلـا وـيـرـانـيـسـ

حـجـانـلـا لـاصـتـالـا عـاطـخـأـ حـيـحـصـتـ وـهـ اـذـهـ:

<#root>

```
*Oct 13 10:01:25.928: RADIUS/ENCODE(0000012D):Orig. component type = VPN IPSEC
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): dropping service type, "radius-server attribute 6 on-for
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IP: 0.0.0.0
*Oct 13 10:01:25.929: vrfid: [65535] ipv6 tableid : [0]
*Oct 13 10:01:25.929: idb is NULL
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IPv6: ::

*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): acct_session_id: 4291
*Oct 13 10:01:25.929: RADIUS(0000012D): sending
*Oct 13 10:01:25.929: RADIUS/ENCODE: Best Local IP-Address 10.106.67.33 for Radius-Server 10.127.197.10
*Oct 13 10:01:25.929: RADIUS: Message Authenticator encoded
*Oct 13 10:01:25.929: RADIUS(0000012D): Send Access-Request to 10.127.197.105:1812 id 1645/24, len 344
RADIUS: authenticator 85 AC BF 77 BF 42 0B C7 - DE 85 A3 9A AF 40 E5 DC
*Oct 13 10:01:25.929: RADIUS: Service-Type [6] 6 Login [1]
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 26
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 45

*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 39 "isakmp-phase1-id=*$AnyConnectClient$*"

*Oct 13 10:01:25.929: RADIUS: Calling-Station-Id [31] 14 "10.106.50.91"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 64
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L40A6A4321Z02L40A6A325BZH1194CC58
*Oct 13 10:01:25.929: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 21
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
*Oct 13 10:01:25.929: RADIUS: EAP-Message [79] 24
RADIUS: 02 8E 00 16 04 10 8A 09 BB 0D 4B A9 D6 2B 59 1C C8 FE 1C 90 56 F5 [ K+YV]
*Oct 13 10:01:25.929: RADIUS: Message-Authenticato[80] 18
RADIUS: 54 85 1B AC BE A8 DA EF 24 AE 4D 28 46 32 8C 48 [ T$M(F2H]
*Oct 13 10:01:25.929: RADIUS: State [24] 90
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 30 41 36 41 34 33 32 31 5A 4F 32 4C 34 [2L40A6A4321Z02L4]
RADIUS: 30 41 36 41 33 32 35 42 5A 48 31 31 39 34 43 43 [0A6A325BZH1194CC]
RADIUS: 35 38 5A 4E 31 32 3B 33 30 53 65 73 73 69 6F 6E [58ZN12;30Session]
RADIUS: 49 44 3D 69 73 65 2D 70 73 6E 2F 35 31 37 31 33 [ID=ise-psn/51713]
RADIUS: 35 39 30 30 2F 33 38 3B [ 5900/38;]
*Oct 13 10:01:25.929: RADIUS: NAS-IP-Address [4] 6 10.106.67.33
*Oct 13 10:01:25.929: RADIUS(0000012D): Sending a IPv4 Radius Packet
*Oct 13 10:01:25.929: RADIUS(0000012D): Started 120 sec timeout

*Oct 13 10:01:25.998: RADIUS: Received from id 1645/24 10.127.197.105:1812, Access-Accept, len 239
```

```

RADIUS: authenticator BC 19 F2 EE 10 67 80 C5 - 9F D9 30 9A EA 7E 5E D3
*Oct 13 10:01:25.998: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.998: RADIUS: Class [25] 67
RADIUS: 43 41 43 53 3A 4C 32 4C 34 30 41 36 41 34 33 32 [CACS:L2L40A6A432]
RADIUS: 31 5A 4F 32 4C 34 30 41 36 41 33 32 35 42 5A 48 [1Z02L40A6A325BZH]
RADIUS: 31 31 39 34 43 43 35 38 5A 4E 31 32 3A 69 73 65 [1194CC58ZN12:ise]
RADIUS: 2D 70 73 6E 2F 35 31 37 31 33 35 39 30 30 2F 33 [-psn/517135900/3]
RADIUS: 38 [ 8]
*Oct 13 10:01:25.998: RADIUS: EAP-Message [79] 6
RADIUS: 03 8E 00 04
*Oct 13 10:01:25.998: RADIUS: Message-Authenticato[80] 18
RADIUS: F9 61 C1 FD 6D 26 31 A2 89 04 72 BC DD 32 A9 29 [ am&lr2])
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59

*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0"

*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59

*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0"

*Oct 13 10:01:25.998: RADIUS(0000012D): Received from id 1645/24
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
8kv#

```

عجاarma

- [قد عا ق ماد ختس اب IKEv2 ل دع ب نع لو ص ول ل FlexVPN ث ب ل او ل ا ب ق ت س ال ا د ح و ن ي و كت](#)
- [ي ل ح م ل ا م د خ ت س م ل ا ت ان اي ب](#)
- [و ق د اص م ماد ختس اب AnyConnect FlexVPN EAP DUO](#)
- [ماد ختس اب AnyConnect IKEv2 EAP-MD5](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).