

ISE لمات مادختس اپ FlexVPN نیوک

تایوتھملا

قدمي

قىس اس، ئالا تاب ل طت ملما

تابلط ملا

مدختن ملأتان وكملا

نیوکل

ةكبش للي طخت لا مس رلا

عزملا نیوکت: 1 ۋە طخلار

ب ث د ح ت ل ا م ت ي ذ ل ا ن ي و ك ت ل ا : 2 ق و ط خ ل ا

ISE نیوکت: 3: ۋە طاخلا

٣-١: مدخلات عاشنا

جەنلائۇمۇجىم نېوکت: 3.2: ۋەطخىلا

لیوختلا جه نیوکت: 3.3: ۋەطخىلا

قحص لانم ققحتلا

احالص او عاطخآل افاشکتسا

لِمَعْلَمٍ وَيَرَانِي س

ةمدقم

Cisco نم (ISE) ۆيەلە تامدەنگەرەم مادختسەاب FlexVPN نى يوكىت ۆي فېيك دەنەتسەملە اذە فەصىي يىكىمانىي دلەكشەب ئازىچەللىك تانىي وكتىلا نىيۇعتل.

ةيـسـاسـاـلـاـ تـابـلـطـتـمـلـا

تابلطتما

Cisco نأب نوك دل ئەفرۇم كىيىدىلىنىڭ عىضاوەملاب ئەيلاتلا يىصوت:

- Cisco (ISE) نم ئي وهلا تامدخ كرحم نويوكىت
 - RADIUS لوكوتورب
 - (FlexVPN) ئنرملا ئيرهاظلا ئصاصخلا ئكبسلىا

ةمدى سملاتان وكملا

- Cisco CSR1000V (VXE) - 17.03.04a رادص إلـا
 - Cisco Identity Services Engine (ISE) - 3.1

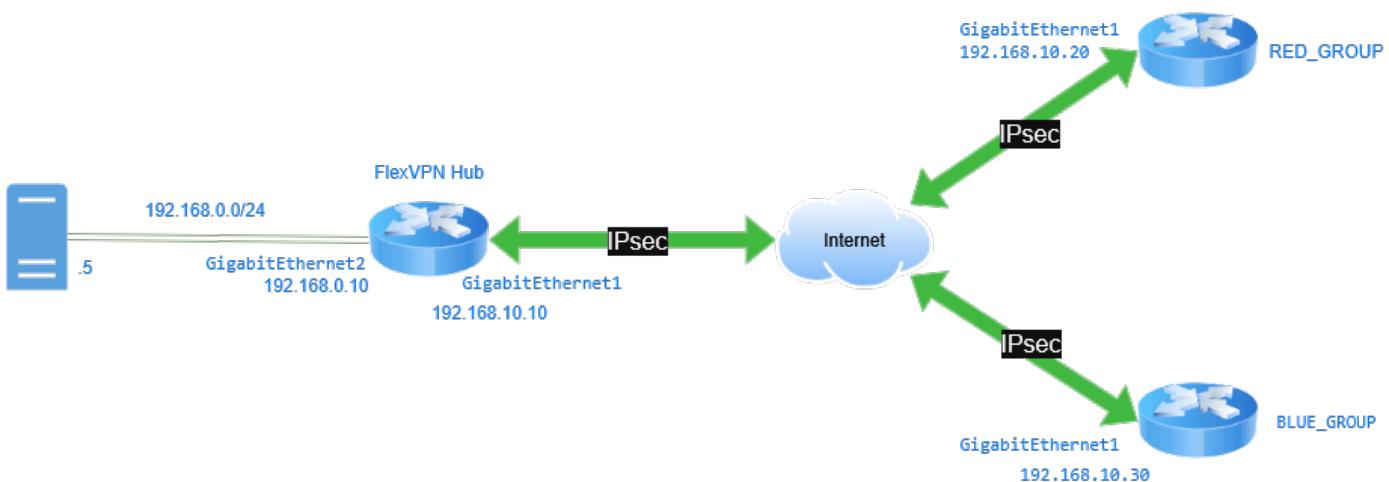
ةـصـاخـ ةـيـلـمـعـمـ ةـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاـشـنـاـ مـتـ
تـنـاـكـ اـذـاـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـرـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـقـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ

رما يألا لمتحمل ريا ثأتلل كمهف نم داكتف ،ليغشتلا ديق كتكبش.

نيوكتل

وكبش للي طختلا مسرا

ةرادا حيت ةنيلع تانيلوكت صيصختو كالسألااب لاصتا عاشناب FlexVPN موقد نأ نكمي ع FlexVPN لماكت ئيفيك اذه حضوي ،ططخملارلا ئل ادانتسا .تانايبلارلا رورم ئكرحو تالاصتا اقفو DHCP عمجتو قفنلار داصم تاملمع نيليعت متى ،جوملاب ام ئملك لاصتا دناع ،ئتح ISE مث ،عورفلارلا ئق داصمل صيخرتلارلا مدخلتسى هن .ثدحتملا هيلا يمتنى يذلا عرفلا وأ ئعومجممل ISE بساحم وليوخت مداخك RADIUS.



FlexVPN مع جمـ IE

عزملا نيلوكت: 1 ئوطخلا

عورفلارلا ئق داصمل تاداهشلا مادختسا متى .جوملارلا ئداداھش نيزختل atrustpoint نيلوكتب مق .

```
crypto pki trustpoint FlexVPNCA
  enrollment url http://10.10.10.10:80
  subject-name cn=FlexvpnServer, o=Cisco, OU=IT_GROUP
  revocation-check crl
```

ئل ادانتسا تاداهشلا ئقباطم و فيرعت وه هجوملارلا certificate map نم ضرغلا نيلوكت .ب .ةتبثم ئدمعتم تاداهش هي دل هجوملارلا ئل اچ يف ،ةددحملارلا تامولعملا.

```
crypto pki certificate map CERT_MAP 5
  issuer-name co ca-server.cisco.com
```

زاهجلارلا ئل ع ئبساحمل او ليوختل aRADIUS server نيلوكت ج:

```
aaa new-model
!
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
```

لاصتالا ذفانمو هب صالحا IP ناوونع مادختس اب رمألا RADIUS server group فيرعتب مق. د. رورم ةكرحل ردىصملأا ٰههج اوو كرتشمملأا حاتفمل او

```
radius server ISE25
  address ipv4 192.168.0.5 auth-port 1645 acct-port 1646
  key cisco1234

aaa group server radius ISE
  server name ISE25
  ip radius source-interface g2
```

```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

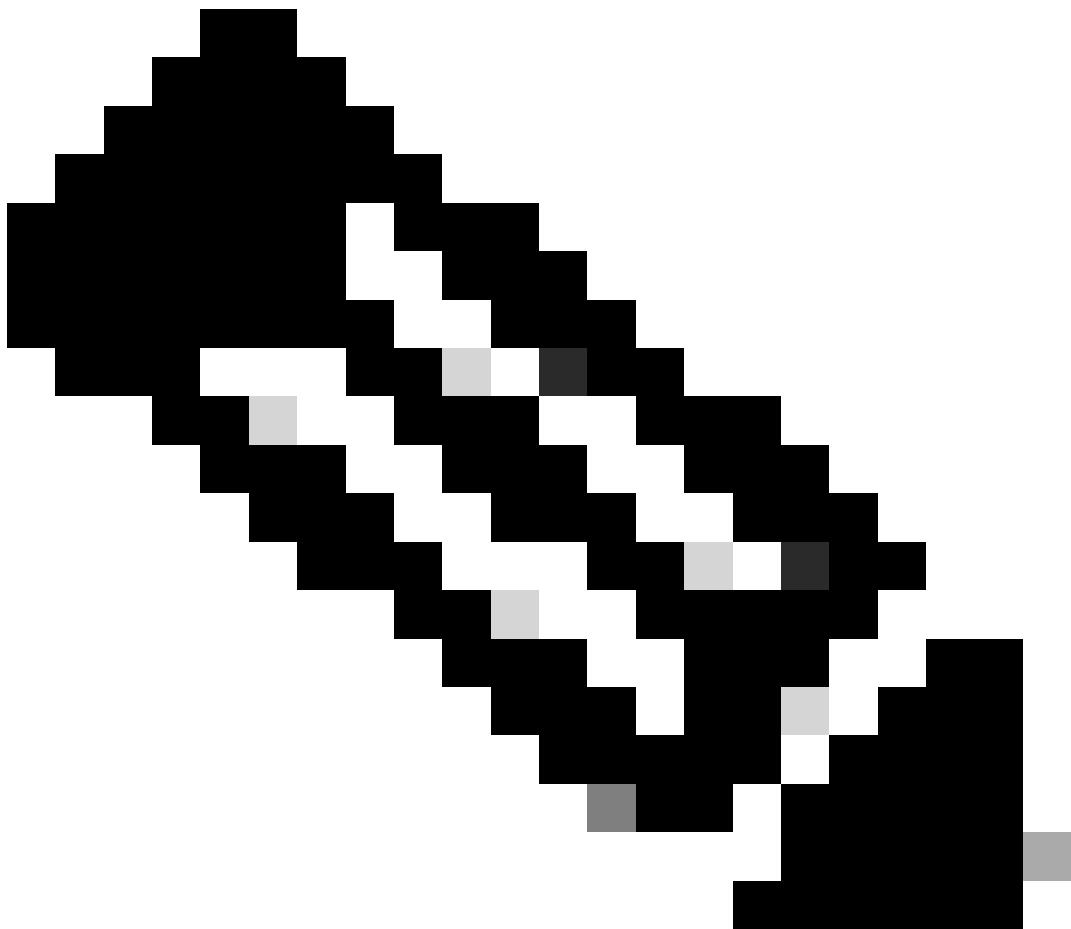
وَعِمَجْ مُلْكِ IP local pool فِي رِعْتَبِ مَقْ.

```
ip local pool RED_POOL 172.16.10.10 172.16.10.254  
ip local pool BLUE_POOL 172.16.0.10 172.16.0.254
```

و مجمّع EIGRP لـ Cisco، نـيـوـكـوتـ.ـزـ.

```
router eigrp Flexvpn
address-family ipv4 unicast autonomous-system 10
topology base
exit-af-topology
network 10.100.100.0 0.0.0.255
network 10.10.1.0 0.0.0.255
network 10.200.200.0 0.0.0.255
network 10.10.2.0 0.0.0.255
```

network 172.16.0.0



و OSPF و EIGRP و FlexVPN هي جو تلا تالوكوتورب مع دت: ظحالم
BGP مادختس! مت ي، لي لدلا اذه يف. VPN. ةكبش قافنأ رب ع EIGRP.

مسا صالحتسا ال رمألا IKEv2 name mangler نيوكتب مق. ح
 IKEv2 Organization-
 تامولعم مادختسال اهن يوكت مت ي، ئلاحلا هذه يفو. ضيوفتل مدختسم
 ليو ختلل مدخلت مساك عورفلارىل ع دوجوملا تاداهشلا نم Unit.

```
crypto ikev2 name-mangler NM  
dn organization-unit
```

فلم يف، certificate map، AAA server group و name mangler، ئلا ئراش إلا متت. IKEv2 profile نيوكتب مق. ط
 فيرعت IKEv2.

اذه يف يلاتل RSA-SIG وحنلا ىلع دعب نع ٰقاداصمل او ٰيلحـمـلا ٰقاداصـمـلا نـيـوـكـتـ مـتـيـ دـدـحـمـلا وـيـرـانـيـسـلا.

ع^م قباطتی مدخلت سم مس اس اس RADIUS server ىلع ىلجم مدخلت سم باسح عاشن ا بجي
هان دا نيوكتل اي ف ددم و ه امك) رورمل ا قمل ك organization-unit Cisco1234.

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint FlexVPNCA
dpd 10 2 periodic
aaa authorization group cert list FLEX name-mangler NM password Cisco1234
aaa accounting cert FLEX
virtual-template 1 mode auto
```

عجم و مقتب IPsec profile و نیوکت مقتب IKEv2 profile.

```
crypto ipsec profile IPSEC_FlexPROFILE  
set ikev2-profile Flex_PROFILE
```

مٽ يذلا طابتراءو virtual-template. IPsec profile virtual-access interface عاشن إل ھم ادختسا متى عاشن إل فواشنا.

لاب تنیع نوکی اذه نا امب، ناوونع نم ام عم virtual-template لاتتبث RADIUS server.

```
interface Virtual-Template2 type tunnel
no ip address
tunnel source GigabitEthernet1
tunnel destination dynamic
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

ةيـلـخـادـ ةـكـبـشـ ةـاـحـمـلـ loopbacksـ يـنـثـاـ نـيـوـكـتـ بـ مـقـ

```
interface Loopback1010
ip address 10.10.1.10 255.255.255.255
!
interface Loopback1020
ip address 10.10.2.10 255.255.255.255
```

٥- ثدحتلا مت يذلا نيوكتلا: 2 ٰوطخلا

```
crypto pki trustpoint FlexVPNSpoke  
  enrollment url http://10.10.10.10:80  
  subject-name cn=FlexVPNSpoke, o=Cisco, OU=RED_GROUP  
  revocation-check crl
```

ىلإ ادانتسا تاداهشلا ٰقباطم و فيرعت وه جوملا certificate map نم ضرغلا. بـ ٰتبثم ٰددعتم تاداهش هـدل جوملا نـأ ٰلاح يـف، ٰـددحملـا تـامـولـعـملـا.

```
crypto pki certificate map CERT_MAP 5  
issuer-name co ca-server.cisco.com
```

c. AAA ل ئىلەملا لىوخىتلا ئەكپش نىيوكت.

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

ضيوفتل او ٽقاداص ملا لي وخت certificate map ىلإ ٽراس إلأا متت IKEv2 profile. ىف يلحملأا (AAA) ٽبساحملأاو IKEv2 profile.

RSA-SIG. نیوکت متبی اوق داصلما ټیل جمل او ټیل عېدې ټئیه.

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint FlexVPNSpoke
dpd 10 2 on-demand
aaa authorization group cert list FLEX default
```

عجلة IPsec profile و IKEv2 profile.

```
crypto ipsec profile IPSEC_FlexPROFILE  
set ikev2-profile Flex_PROFILE
```

ادانتسا ٽرصلا نم قفنلл IP ناونع يقلتل tunnel interface نيوكت مت tunnel interface. ٽيوكتب مق. و ليوختلا جئاتن ىلإ.

```
interface Tunnel0  
ip address negotiated  
tunnel source GigabitEthernet1  
tunnel destination 192.168.10.10  
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

مالكلل ٽيلحمل اٽكبشلا نع نالعإلاو EIGRP tunnel interface. نيوكتب مق. ز.

```
router eigrp 10  
network 10.20.1.0 0.0.0.255  
network 172.16.0.0
```

ٽيلخاد ٽكبش ٽاكاحمل aloopback نيوكت.

```
interface Loopback2010  
ip address 10.20.1.10 255.255.255.255
```

ISE نيوكت: 3: ٽوطخل

ٽكبش زاهج ٽفاض او تاعومجم و نيمدختسم عاشنإ 3.1: ٽوطخل

أ مداخ ىلإ لقتنا او ISE ىلإ لوطدل ليجستب مق. Administration > Network Resources > Network Devices.

Cisco ISE

What page are you looking for?

Dashboard Context Visibility Operations Policy **Administration** Work Centers

Recent Pages

- Live Logs
- Users
- Policy Sets
- External Identity Sources
- Certificate Provisioning
- Authorization Profiles

System

- Deployment
- Licensing
- Certificates
- Logging
- Maintenance
- Upgrade
- Health Checks
- Backup & Restore
- Admin Access
- Settings

Identity Management

- Identities
- Groups
- External Identity Sources
- Identity Source Sequences

Shortcuts

- Ctrl** + **[/]** - Expand menu
- esc** - Collapse menu

Network Resources

- Network Devices**
- Network Device Groups
- Network Device Profiles
- External RADIUS Servers
- RADIUS Server Sequences
- NAC Managers
- External MDM
- Location Services

pxGrid Services

- Summary
- Client Management
- Diagnostics
- Settings

Device Portal Management

- Blocked List
- BYOD
- Certificate Provisioning
- Client Provisioning
- Mobile Device Management
- My Devices
- Custom Portal Files
- Settings

Feed Service

- Profiler

Threat Centric NAC

- Third Party Vendors

Make a wish



قرادالا دراوم ۋە كېش ۋە زەجأ

لیمعک FlexVPN عزوم نیوکتل Add رقنا .ب

Network Devices

Device Profile List						Selected 0 Total 1	flex	Filter
	Name	IP/Mask	Profile Name	Location	Type	Description		
<input type="checkbox"/>	FlexVPN_Hub	 Cisco	?	All Locations	All Device Types			
Edit	+ Add	Duplicate	Import	Export	Generate PAC	Delete		

FlexVPN چومن ڈیفائلز اسے AAA میں جمع کرنا

فضأو رايتخالا ةناخ ددح RADIUS Authentication Settings مث IP ناونع يلقو ٰكبشلا زاهج مسالخ دأ. دنع اهمادختسا مت يتلا اهسفن يه نوكت نأ بجي Shared Secret. ٰكرتشملأا ٰيرسلأا رورملأا ٰقملاك رقنا FlexVPN. لص و ٰحوالي ع فـ RADIUS مـداخ ٰعومجم عاشـنـا Save

Network Devices List > FlexVPN Hub

Network Devices

Name	FlexVPN_Hub
Description	
<hr/>	
IP Address	<input type="button" value="▼"/> * IP : <input type="text" value=""/> / <input type="text" value="32"/>  

ةكبشلا زاهجل IP ناونع

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol	RADIUS
Shared Secret	*****
<input type="checkbox"/> Use Second Shared Secret <small>(i)</small>	
networkDevices.secondSharedSecret	Show
CoA Port	1700
Set To Default	

ةكبشل زاهجل كرتشملا حاتفملا

د. ایلإ لقتنا Administration > Identity Management > Identities.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar has tabs for Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), and Work Centers. The left sidebar has sections for Recent Pages (Groups, Network Devices, Live Logs, Users, Policy Sets), System (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), Identity Management (Groups, External Identity Sources, Identity Source Sequences, Settings), and Shortcuts (with keyboard shortcuts for expanding/collapsing menus). The main content area is divided into several panels: Network Resources (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), pxGrid Services (Summary, Client Management, Diagnostics, Settings), Feed Service (Profiler), Device Portal Management (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Management, My Devices, Custom Portal Files, Settings), and Threat Centric NAC (Third Party Vendors). The 'Identities' link under Identity Management is highlighted with a red box.

ةرادل اتافرع م - ةرادل ا فيرعت - ةرادل ا

م داخلل ئيلحمل ا تانايبل ا ئدعاق يف ديدج مدخلتس م عاشن إل رقنا Add.

ىلع تاداهشل ا هيلع يوتحت يذلا مسالا سفن و همدختسملا مسا Username و Login Password. اهسفن يه لوطدا ليجست رورم ئملك نوكت نأ بجي و ئداهشل ا يف ئدحولـا-ئسـسـفـمـلـاـ ئـمـيـقـ اـ فـيـرـعـتـ فـلـمـ يـفـ اـهـدـيـدـحـتـ مـتـ يـتـلـاـ Kev2.

رقنا Save

Network Access Users

Network Access Users								Selected 0 Total 2	Group	Filter
Edit	+ Add	Change Status	Import	Export	Delete	Duplicate				
Status	Username	Description	First Name	Last Name	Email Address	User Identity G...	Admin			
<input type="checkbox"/>	Enabled BLUE_GROUP									
<input type="checkbox"/>	Enabled RED_GROUP									

ةرادل ا تافرع م - ةرادل ا فېرعت - ةرادل ا

Network Access User

* Username: RED_GROUP

Status: Enabled

Email:

Passwords

Password Type: Internal Users

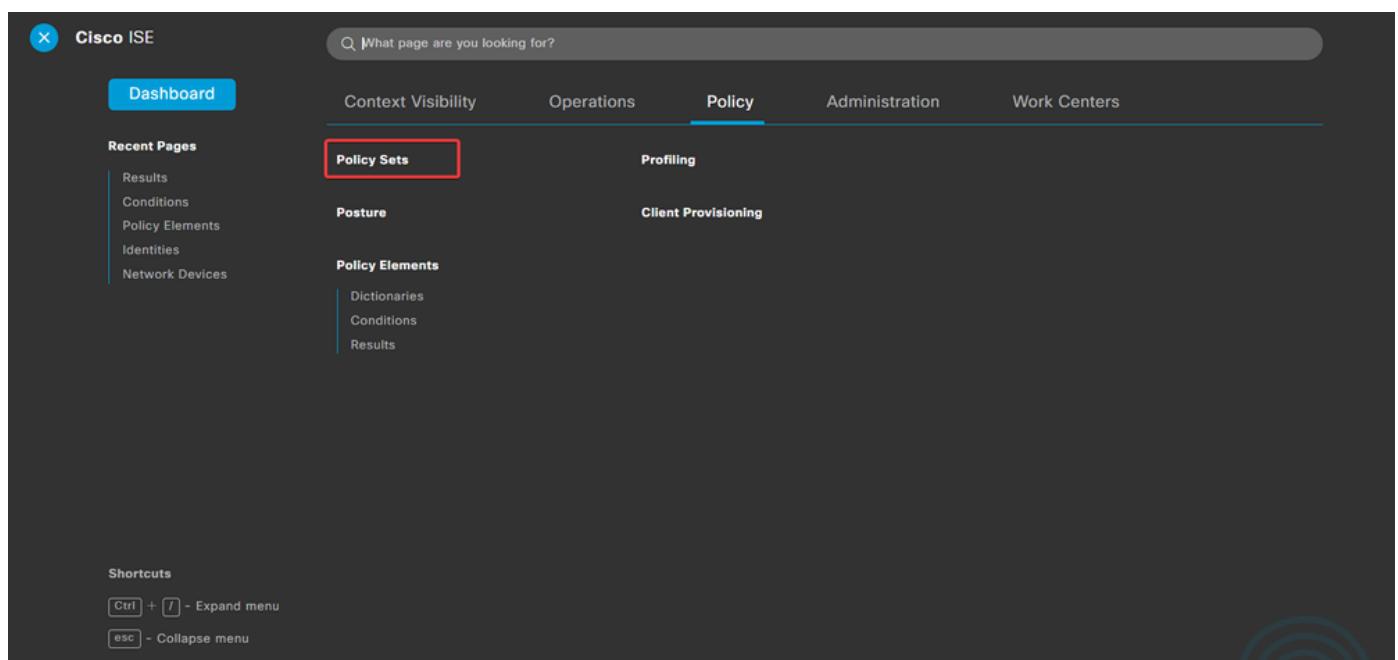
Password	Re-Enter Password
* Login Password: <input type="password"/> <input type="password"/>
<input type="button" value="Generate Password"/> (i)	
<input type="button" value="Generate Password"/> (i)	

Enable Password:

ةيمي ظنتلا ةدحولا ئەم يق سەفنب ئەعومجملا ئاشنامەت

جەنلە ئەعومجم نىوكت: 3.2: ۋەطخىل

ىلى لىقتىنالا Policy > Policy Sets.



The screenshot shows the Cisco ISE dashboard with the 'Policy' tab selected. On the left, under 'Recent Pages', 'Policy Sets' is highlighted with a red box. The main content area displays sections for 'Policy Sets', 'Posture', 'Profiling', 'Client Provisioning', and 'Policy Elements'. A sidebar on the left lists 'Dashboard', 'Context Visibility', 'Operations', 'Administration', and 'Work Centers'. A 'Shortcuts' section at the bottom provides keyboard shortcuts for expanding and collapsing menus.

تاسايسل اسلا موجم

نم نميألا بناجلالا ىلع دوجوملا مهسلا قوف رقنلاب يضارتفالا ليوختلا جهن ددح .بـ
ةـشـاشـلـا:

The screenshot shows a table titled 'Policy Sets' with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. A search bar is at the top. A single row is selected, labeled 'Default policy set'. The 'Actions' column contains a gear icon and a red-bordered arrow icon. Buttons for 'Reset', 'Save', and 'Reset Policyset Hitcounts' are at the bottom.

يضارتفالا جهـنـلـا رـيـحـتـ

ـنـوـقـيـأـلـا قـوـفـ رـقـنـا مـثـ .ـهـيـدـمـتـلـ روـاجـمـلـا ئـلـدـسـنـمـلـا ئـمـيـاقـلـا مـهـسـ قـوـفـ رـقـنـا جـ
ـهـيـدـجـ ئـدـعـاـقـ ئـفـاصـإـلـ (ـأـدـدـ)ـ (ـأـضـاـلـ).

The screenshot shows a table titled 'Authentication Policy' with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is at the top. A single row is selected, labeled 'FlexVPN_Router'. The 'Actions' column contains a gear icon and a red-bordered arrow icon. Buttons for 'Reset', 'Save', and 'Add' (+) are at the bottom. A red box highlights the 'Add' button.

ـقـدـاصـمـلـا جـهـنـ ئـفـاصـإـ

ـطـورـشـلـا دـوـمـعـ تـحـتـ (ـأـضـاـلـ)ـ زـمـرـ دـدـحـ وـ ئـدـعـاـقـلـا مـسـاـ لـخـدـأـ .ـدـ

The screenshot shows a table titled 'Authentication Policy' with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is at the top. A single row is selected, labeled 'FlexVPN_Router'. An additional row is being added, indicated by a red-bordered plus sign (+). The 'Actions' column contains a gear icon and a red-bordered arrow icon. Buttons for 'Reset', 'Save', and 'Add' (+) are at the bottom. A red box highlights the 'Add' button.

ـقـدـاصـمـ ئـسـاـيـسـ عـاـشـنـاـ

ـنـاـونـعـلـا تـلـخـدـ .ـهـيـنـوـقـيـأـلـا قـوـفـ رـقـنـاـوـ تـامـسـلـا رـحـمـ صـنـ عـبـرـمـ رـقـنـاـ ..ـهـيـصـرـصـ فـلـيـخـنـمـ FlexVPNـ .ـ

Conditions Studio

Library

Search by Name

Catalyst_Switch_Local_Web_Authentication
EAP-MSCHAPv2

Editor

Radius-NAS-IP-Address

Equals

Set to 'Is not'

Duplicate Save

NEW AND OR

Authenticate FlexVPN Hub

Authorization Policy (3)

+ Status	Rule Name	Conditions	Use	Hits	Actions
<input type="text"/> Search					
✓ FlexVPN		Radius-NAS-IP-Address EQUALS	Internal Users	12	

ڦڻڻا جهڻا جهڻا

لیوختلا جهڻن نیوکت: 3.3: ڦڻڻا جهڻا

ڦڻڻا قوف رقنا مث . دیدم تل رواجملا ڦل دس نملاء مئاقلما مهس قوف رقنا .
Authorizaion Policy add (+) .

Authorization Policy (13)

+ Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
<input type="text"/> Search							

دیدج لیوخت جهڻن عاشنإ

طورشلا دومع تتحت ڦڻڻا ددھو ڦدعاق لاما مسا لخدا . add (+) .

Authorization Policy (3)

+ Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
<input type="text"/> Search							
✓ RED-GROUP			Select from list		Select from list		

دیدج ڦدعاق عاشنإ

ڦڻڻا ددھو Network Access - UserName Subject . ڦڻڻا قوف رقنا او تام سلا ررحم صن عبرم رقنا .

The screenshot shows the Microsoft Intune interface. On the left, the 'Library' pane displays a list of device configurations, each with a preview icon and a 'Details' button. The configurations listed are: BYOD_is_Registered, Catalyst_Switch_Local_Web_Authentication, Compliance_Unknown_Devices, Compliant_Devices, EAP-MSCHAPv2, and EAP-TLS. On the right, the 'Editor' pane is open, showing the configuration details for 'Network Access-UserName'. A red box highlights the 'Network Access-UserName' section. Below it, a modal window titled 'Select attribute for condition' lists attributes under 'Dictionary' (Network Access) and 'Attribute' (AD-User-Name-Domain). A red box highlights the 'Network Access' row, which maps to the 'UserName' attribute. Other rows include 'PassiveID' mapping to 'PassiveID_Username' and 'Radius' mapping to 'User-Name'.

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
NETWORK ACCESS	AD-User-Name-Domain		
Network Access	AD-User-Join-Point		
Network Access	UserName		
PassiveID	PassiveID_Username		
Radius	User-Name	1	

مـدـخـتـسـمـلـا مـسـا - ةـكـبـشـلـا ىـلـا لـوـصـوـلـا دـيـدـحـتـ

تاداهش لـلـ ةـ دـ حـ وـ لـاـ ةـ سـ فـ مـ لـاـ ةـ مـ يـ قـ فـ ضـ أـ مـ ثـ ، لـ غـ شـ مـ كـ Contains دـ دـ حـ .

Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Editor

Network Access-UserName

Contains

Set to 'Is not'

Duplicate Save

NEW AND OR

فاضة مساحة وجمعة

رتبخ او ڦنوقی add (+) لع رقنا ، تافي صوتلا دوماع يف .. ٥ Create a New Authorization Profile.

Results							
Status	Rule Name	Conditions	Profiles	Security Groups	Hits Actions		
<input type="text"/> Search							
	RED-GROUP	Network Access-UserName CONTAINS RED_GROUP	Select from list	Select from list	122		
<table border="1"> <thead> <tr> <th>Profiles</th> </tr> </thead> <tbody> <tr> <td> </td> </tr> </tbody> </table>						Profiles	
Profiles							

ديج ليوخت فيرعت فلم ۋەفاضا

فیصل ولاد خداوند Name.

Authorization Profile

* Name FlexVPN_RED

Description

* Access Type ▼

Network Device Profile Cisco Cisco +

Service Template

Track Movement i

Agentless Posture i

Passive Identity Tracking i

ليوختلا فيرعت فلم ةيمست

ىلע ۋەلسەن مەلە ئەمئاقلە نەم ۋەمسىل Cisco-av-pair دەح، كەلذ دەعەب Advanced Attributes Settings. ىلإ لىقتىن از FlexVPN Talk ىلإ اهنىيەت مەت يېتلى ئەمسىلە فەضلۇ، رسىيەلە بىنالىجىلە.

لابهملا اذهل اهنوي عت متي س يتلا تامسلا نمضتت

- IP ناونع ىلע عورفلار اهنم لصحت يتلار ئومجملا ديدح ت.
 - ردىص مك عاجرت سالا ئەھج او نىييعت.

نۇ ئالىغا مەتى ئەل تامسلا ھەذە نو دېب ھەن ئۆل route accept any تامسلا route set interface رفوت مەزلىي امك ئەي عرفلى مادا خىلە ئىلە حىچھىص لىكش ب تاھجۇملا.

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip unnumbered loopback100
cisco-av-pair = ipsec:addr-pool=RED_POOL
cisco-av-pair = ipsec:route-accept=any
cisco-av-pair = ipsec:route-set=interface
```

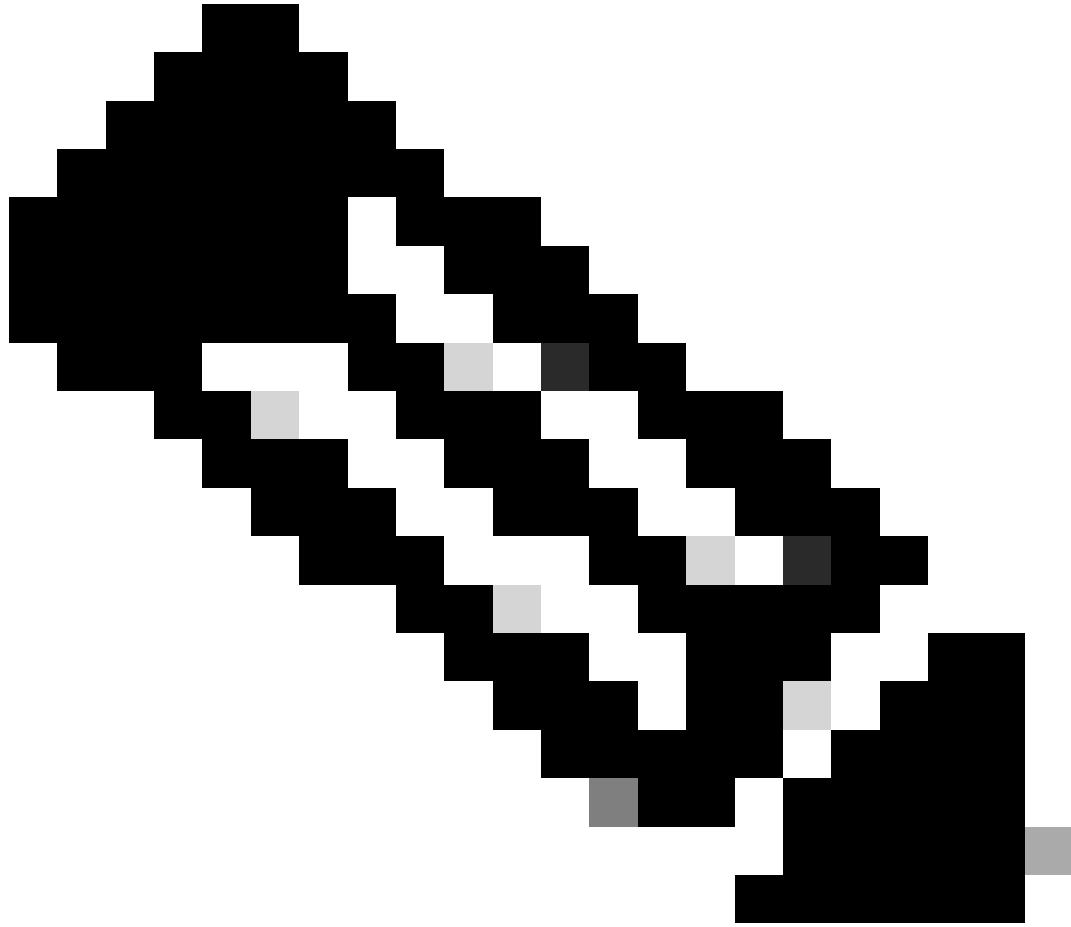
✓ Advanced Attributes Settings

Cisco:cisco-av-pair	▼	=	ip:interface-config=ip unnumbered	▼	-
Cisco:cisco-av-pair	▼	=	ipsec:addr-pool=RED_POOL	▼	-
Cisco:cisco-av-pair	▼	=	ipsec:route-accept=any	▼	-
Cisco:cisco-av-pair	▼	=	ipsec:route-set=interface	▼	- +

✓ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip unnumbered loopback100
cisco-av-pair = ipsec:addr-pool=RED_POOL
cisco-av-pair = ipsec:route-accept=any
cisco-av-pair = ipsec:route-set=interface
```

ةمدقتمل اصخل اتاددعى



امو لاثمل او فص ول او ئلمجلما عانب و مس(الا) تام سلا تافص او مل ئبس نلاب : ئظحالم FlexVPN RADIUS:

نافیصوتلا دومع یف authorization profile نییعتب مق. ح.

Authorization Policy (11)		Results					
	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
<input type="text"/> Search							
<input checked="" type="checkbox"/>	RED_GROUP		Network Access-UserName CONTAINS RED_GROUP	FlexVPN_RED	<input type="button"/> Select from list	<input type="button"/> 8	

لیختل اڈعاق

رقنا - الـ وـ Save.

ةحصـلـا نـم قـقـحتـلـا

- يـرـهـاـظـلـا لـوـصـولـا ةـلـاحـو يـرـهـاـظـلـا بـلـاقـلـا وـقـفـنـلـا ةـعـجـارـمـلـ رـمـأـلـا مـدـخـتـسـأـ.

لـكـلـ يـرـهـاـظـلـا لـوـصـولـا ئـشـنـيـوـ، ةـيـدـاعـ يـهـوـ up/down ةـلـاحـ يـرـهـاـظـلـا بـلـاقـلـا ةـقـلـتـيـ، ةـرـصـلـا ئـلـعـ Talk up/up.

<#root>

```
FlexVPN_HUB#show ip interface brief
Interface          IP-Address      OK?   Method    Status       Protocol
GigabitEthernet1   192.168.10.10  YES   NVRAM     up        up
GigabitEthernet2   192.168.0.10  YES   manual    up        up
Loopback100        10.100.100.1 YES   manual    up        up
Loopback200        10.200.200.1 YES   manual    up        up
Loopback1010       10.10.1.10  YES   manual    up        up
Loopback1020       10.10.2.1   YES   manual    up        up
virtual-Access1    10.100.100.1 YES   unset     up        up

virtual-Template2  unassigned     YES   unset     up        down
```

عـضـوـ يـدـبـيـ وـعـوـمـجـمـلـا ئـلـا نـيـعـيـ عـمـجـتـلـا نـمـ نـاـونـعـ قـفـنـلـا نـرـاقـ تـمـلـتـسـاـ، ئـلـا ئـلـعـ Talk up/up.

<#root>

```
FlexVPN_RED_SPOKE#show ip interface brief
Interface          IP-Address      OK?   Method    Status       Protocol
GigabitEthernet1   192.168.10.20  YES   NVRAM     up        up
Loopback2          10.20.1.10   YES   manual    up        up
Tunnel10           172.16.10.107 YES   manual    up        up
```

- رـمـأـلـا مـدـخـتـسـأـ show interfaces virtual-access

configuration

```
FlexVPN_HUB#show interfaces virtual-access 1 configuration
Virtual-Access1 is in use, but purpose is unknown
Derived configuration : 232 bytes
!
interface Virtual-Access1
  ip unnumbered Loopback100
  tunnel source GigabitEthernet1
  tunnel mode ipsec ipv4
  tunnel destination dynamic
  tunnel protection ipsec profile IPSEC_FlexPROFILE
```

```
no tunnel protection ipsec initiate
end
```

- تاهجوملـا نـيـب نـمـآلـا لـاصـتـالـا ءـاعـشـنـا دـيـكـأـتـلـ show crypto session رـمـآلـا مـدـخـتـسـأـ.

```
FlexVPN_HUB#show crypto session
Crypto session current status
Interface: Virtual-Access1
Profile: Flex_PROFILE
Session status: UP-ACTIVE
Peer: 192.168.10.20 port 500
Session ID: 306
IKEv2 SA: local 192.168.10.10/500 remote 192.168.10.20/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

- خـآلـا عـقـوـمـلـا عـمـ EIGRP رـوـاجـتـ ءـاعـشـنـا دـيـكـأـتـلـ show ip eigrp neighbors رـمـآلـا مـدـخـتـسـأـ.

```
FlexVPN_HUB#show ip eigrp neighbors
EIGRP-IPv4 VR(Flexvpn) Address-Family Neighbors for AS(10)
H   Address           Interface      Hold Uptime      SRTT    RT0     Q     Seq
          (sec)          (ms)          Cnt  Num
0   172.16.10.107     Vi1            10  00:14:00      8  1494   0   31
```

- مـداـوـخـلـا ىـلـا تـعـفـدـ دقـ تـارـاسـمـلـا نـأـ نـمـ قـقـحـتـلـلـ show ip route رـمـآلـا مـدـخـتـسـأـ.
 - ربـعـ رـبـكـمـلـا ىـلـعـ عـاجـرـتـسـالـا ٰهـجـاـوـ، 10.20.1.10 لـ رـاسـمـلـا ىـلـعـ فـرـعـتـلـا مـتـ EIGRP يـرـهـاـظـلـا لـوـصـوـلـا لـالـخـ نـمـ هـيـلـا لـوـصـوـلـا نـكـمـيـوـعـزـوـمـلـا لـبـقـ نـمـ

<#root>

```
FlexVPN_HUB#show ip route
<<<< Output Ommitted >>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
C       10.10.1.10 is directly connected, Loopback1010
C       10.10.2.10 is directly connected, Loopback1020
D       10.20.1.10 [90/79360000] via 172.16.10.107, 00:24:42, Virtual-Access1

C       10.100.100.1 is directly connected, Loopback100
C       10.200.200.1 is directly connected, Loopback200
      172.16.0.0/32 is subnetted, 1 subnets
S         172.16.10.107 is directly connected, Virtual-Access1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C           192.168.0.0/24 is directly connected, GigabitEthernet2
```

```
L      192.168.0.10/32 is directly connected, GigabitEthernet2
C      192.168.10.0/24 is directly connected, GigabitEthernet1
L      192.168.10.10/32 is directly connected, GigabitEthernet1
```

- اهيل ا لوصول ا نكمي و EIGRP لالخ نم 10.10.1.10 و 10.10.2.10 تاراس ملا يلع فرع تلا مت رب ع اهيل ا لوصول ا نكمي و ،(1) RED_GROUP (10.100.100.1) IP ردهم لالخ نم Tunnel0.

<#root>

```
FlexVPN_RED_SPOKE#sh ip route
<<<< Output Ommitted >>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.10.1
          10.0.0.0/32 is subnetted, 5 subnets
D        10.10.1.10 [90/26880032] via 10.100.100.1, 00:00:00

D        10.10.2.10 [90/26880032] via 10.100.100.1, 00:00:00

C        10.20.1.10 is directly connected, Loopback2
S        10.100.100.1 is directly connected, Tunnel0

D        10.200.200.1 [90/26880032] via 10.100.100.1, 00:00:00

C        172.16.0.0/32 is subnetted, 1 subnets
C          172.16.10.107 is directly connected, Tunnel0
C        192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.10.0/24 is directly connected, GigabitEthernet1
L          192.168.10.20/32 is directly connected, GigabitEthernet1
```

اهحالص او عاطخاً فاشكتس ا

رشنلا نم عونلا اذه عاطخاً فاشكتس ال اهم ادخلتس ا كنكمي تامولعم مسقل ا اذه رفوي قفنلا ضوافت ئيلمع عاطخاً حي حصتل رم اوألا هذه مدختس ا. اهحالص او:

```
debug crypto interface
```

```
debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet
```

```
debug crypto ipsec  
debug crypto ipsec error  
debug crypto ipsec message  
debug crypto ipsec states
```

ا.حالص او عورفلـا دامـتعـا ءاطـخـا فـاشـكـتـسـا يـف RADIUS وـ AAA حـيـحـصـتـ دـعـاسـيـ نـأـ نـكـمـيـ.

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

Working Scenario

..تـامـلـعـمـلـا ةـلـاحـاوـلـيـوـخـتـلـا ةـيـلـمـعـ تـالـجـسـلـا هـذـهـ ضـرـعـتـ

```
<#root>

RADIUS(000001A7): Received from id 1645/106
AAA/BIND(000001A8): Bind i/f
AAA/AUTHOR (0x1A8): Pick method list 'FLEX'
RADIUS/ENCODE(000001A8):Orig. component type = VPN IPSEC

RADIUS(000001A8): Config NAS IP: 192.168.0.10

vrfid: [65535] ipv6 tableid : [0]
idb is NULL
RADIUS(000001A8): Config NAS IPv6: ::

RADIUS/ENCODE(000001A8): acct_session_id: 4414
RADIUS(000001A8): sending
RADIUS(000001A8): Send Access-Request to 192.168.0.5:1645 id 1645/107, len 138
RADIUS: authenticator 7A B5 97 50 F2 6E F0 09 - 3D B0 54 B4 1A DB BA BA

RADIUS: User-Name          [1]   11  "RED_GROUP"
```

```
RADIUS: User-Password      [ 2 ]   18   *
RADIUS: Calling-Station-Id [ 31 ]  14  "192.168.10.20"
RADIUS: Vendor, Cisco      [ 26 ]  63
RADIUS: Cisco AVpair       [ 1 ]   57  "audit-session-id=L2L496130A2ZP2L496130A21ZI1F401F4ZM134"
RADIUS: Service-Type        [ 6 ]   6   Outbound      [ 5 ]
RADIUS: NAS-IP-Address     [ 4 ]   6   192.168.0.10
RADIUS(000001A8): Sending a IPv4 Radius Packet
```

RADIUS(000001A8): Started 5 sec timeout

RADIUS: Received from id 1645/107 192.168.0.5:1645, Access-Accept, len 248

RADIUS: authenticator BE F4 FC FF 7C 41 97 A7 - 3F 02 A7 A3 A1 96 91 38
RADIUS: User-Name [1] 11 "RED_GROUP"
RADIUS: Class [25] 69
RADIUS: 43 41 43 53 3A 4C 32 4C 34 39 36 31 33 30 41 32 [CACS:L2L496130A2]
RADIUS: 5A 50 32 4C 34 39 36 31 33 30 41 32 31 5A 49 31 [ZP2L496130A21ZI1]
RADIUS: 46 34 30 31 46 34 5A 4D 31 33 34 3A 49 53 45 42 [F401F4ZM134:ISEB]
RADIUS: 75 72 67 6F 73 2F 35 33 34 36 34 30 33 32 39 2F [urgos/534640329/]
RADIUS: 32 39 31 [291]

RADIUS: Vendor, Cisco [26] 53

RADIUS: Cisco AVpair [1] 47 "ip:interface-config=ip unnumbered loopback100"

RADIUS: Vendor, Cisco [26] 32

RADIUS: Cisco AVpair [1] 26 "ipsec:addr-pool=RED_POOL"

```
RADIUS: Vendor, Cisco      [26]  33

RADIUS: Cisco AVpair      [1]   27  "ipsec:route-set-interface"

RADIUS: Vendor, Cisco      [26]  30

RADIUS: Cisco AVpair      [1]   24  "ipsec:route-accept=any"

RADIUS(000001A8): Received from id 1645/107
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001A9): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001AA): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

AAA/BIND(000001AB): Bind i/f
RADIUS/ENCODE(000001AB): Orig. component type = VPN IPSEC
RADIUS(000001AB): Config NAS IP: 192.168.0.10
vrfid: [65535]  ipv6 tableid : [0]
fdb is NULL
RADIUS(000001AB): Config NAS IPv6: :: 
RADIUS(000001AB): Sending a IPv4 Radius Packet
RADIUS(000001AB): Started 5 sec timeout
```

RADIUS: Received from id 1646/23 192.168.0.5:1646, Accounting-response, Ten 20

%DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 172.16.10.109 (Virtual-Access1) is up: new adjacency

هـ ذـ هـ لـ وـ حـ جـ رـ تـ لـ ا

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ حـ 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).