FlexVPN مادختساب ISE ةيعضو نيوكت

تايوتحملا

<u>ةمدق مل ا</u> <u>ةيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>ةيساساً تامولعم</u> <u>نىوك</u>تلا <u>ةكبشلل يطيطختلا مسرلا</u> <u>DNS مداخ نیوكت</u> <u>IOS XE ىلوألا نىوكتلا</u> <u>ةىوەلا ةداەش نيوكت</u> IKEv2 نىوكت AnyConnect ليمع في عت فلم نيوكت ISE نىوكت <u>CPP و لوؤسملا تاداەش نېوكت</u> <u>ISE ىلع يلحم مدختسم ءاشنا</u> <u>RADIUS لىمعك FlexVPN عزوم ةفاضا</u> <u>ليمعلا دادما نيوكت</u> <u>عضولا طورشو تاسايس</u> <u>ليمعلا ريفوت لخدم نيوكت</u> <u>جەنلاو لىوختلا تافىصوت نىوكت</u> <u>ةحصلا نم ققحتلا</u> اهحالصاو ءاطخألا فاشكتسا

ەمدقملا

دعب نع لوصولل IOS XE ثـبلاو لـابـقتسالاا ةدحو نيوكت ةيفيكل الـاثم دنتسملاا اذه مدقي و EAP-Message Digest 5 (EAP-MD5).

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- IOS XE ىلع FlexVPN (RA) ىلإ دعب نع لوصولل VPN نيوكت •
- AnyConnect (AC) ليمع نيوكت •
- Posture Flow درال اتارادص ال او 2.2 Identity Service Engine (ISE) یلع Identity Service ا
- ISE ىلع عضولا تانوكم نيوكت •
- كالم Server 2008 R2 مداخ نيوكت Windows Server 2008 R2

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Cisco CSR1000V لغشي يذلا IOS XE 16.8 [Fuji]
- AnyConnect Client ليغشتلا ماظن يلع لمعي يذلا 4.5.03040 رادص لل
- Cisco ISE 2.3
- Windows 2008 R2 مداخ

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رماً يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

ةيساسأ تامولعم

كل حيتي ،ةلاعفو ةبسانم ةضورفملا ةكبشلا نامأ ريبادت لظت نأ نامضل نم .ةيمحملا ةكبشلا ذفني ليمع زاهج يأ ىلع اهتنايصو نامألا تاناكمإ ةحص نم ققحتلا تاقيبطتلا وأ نامألا تادادعا ثدحاً رفوت نامضل ةممصملاا عضولا تاسايس مادختسإ لالخ ىلا لصي ليمع زاهج يأ نأ نم دكأتلا Cisco ISE لوؤسمل نكمي ،ليمعلا ةزهجأ ىلع ةينمألا امب يفي لازي الو قسسؤملا ةكبش ىل لوصولل ةددحملا نامألا ريياعمب يفي ةكبشلا يف ليمعلا زاهجل قفاوتلا يوتسم نم قطقل Cisco ISE ل عضولا عضولا عم يا ترويا رفوس من نكمي من ما ترويا المالا

:ةيسيئر رصانع ةثالثب عضولا ليثمت نكمي

- موقت ISE ىلع لوؤسملا روظنم نم .ةسايسلا نيوكتل ريرقتو عيزوت ةطقنك 1. ISE ةمالع عضول اهؤافيتسا بجي يتلا ةددحملا طورشلا يه ام) عضولا تاسايس نيوكتب يذلا ليكولا جمانربلا وه ام) ليمعلا دادمإ تاسايسو (ةكرشلا عم قفاوتمك زاهجلا ىلع متي نأ بجي يتلا تانوذألا عون ام) ليوختلا جهنو (ةزهجألا نم عون يأ ىلع هتيبثت بجي .(اهعضو ةلاح ىلع دمتعت ىلإ اهنييعت
- ملتسي .يئاهنلا مدختسملا عم لعافتلاو تانايبلا عمجل ةطقنك ليكولا جمانرب .3 قلعتي اميف ISE ىلإ اريرقت رفويو ISE نم عضولا تابلطتم لوح تامولعم ليكولا مدحو ىلإ دنتسملا اذه دنتسي .ءارشلا تابلط قلاحب .هيجوتلا ةداعإ نود لماك لكشب عضولا معدت يتلا ةديحولا ةيطمنلا ةدحولا نوكت يتلا

<u>ISE طمن ةنراقم</u> ةداملا يف ادج ديج لكشب هيجوتلا ةداعإ نود عضولا قفدت قيثوت مت ISE 2.2". يف عضولا قفدت" مسقلا ،"<u>pre and Post 2.2 طمن ةنراقم) Posture</u>

نيتقيرطب FlexVPN مادختساب AnyConnect ISE Posture Module ةدحو دادمإ ءارجإ نكمي نيتفلتخم: • قمزح نم ليمعلا لمع ىلع ايودي ةيطمنلا قدحولا تيبثت متي - ايودي AnyConnect جمارب ليزنت لخدم ىلع قحاتملا https://software.cisco.com/download/home/283000185.

ةدجو ريفوت عم عضولا يف لمعلل ةيلاتلا طورشلا ءافيتسا بجي ISE Posture Module ةيوديلا:

1. لماكلاب لهؤملا لاجملا مسا لحب (DNS) لجملا مسا مداخ موقي نأ بجي enroll.cisco.com ال المال المن المراب المال ا المال الم المال الم المال المالمال المال المالي المال المالي المالي المالي المالي المالي الم

2. حامسلا بجي TCP دنيم TCP دنيم PSN IPs. دفن عضول ارمي 300 PSN دفن عن 2. ويرانيس اذه يف.

ةيامح متي .**SAN لقح** يف PSN **login.cisco.com** دقع ىلع **لوؤسملا قدامشل** نوكي نأ بجي .3 لوؤسملا قدامش ربع 8905 TCP ربع PSN قدقعو VPN قكبش مدختسم نيب لاصتالا "login.cisco.com" مسالا اذه دوجو مدع قلاح يف قدامشلاب ريذحت ىلع مدختسملا لصحيسو PSN.

ةداەشل اقفو :**ةظحالم** RFC6125، قداەشل اقفو :**ةظحالم** لقح يف لوؤسملا ةداەشل CN ةفاضإ ىلإ اضيأ ةجاحب اننأ ينعي اذه .(SAN) نيزختلا SAN.

اهتيبثتو ةيطمنلا ةدحولا ليزنت متي - (CPP) ليمعلا دادما ةباوب ربع يئاقلتلا دادمإلا • لخدملاب صاخلا FQDN ربع ةرشابم CPP ىلإ لوصولا لالخ نم ISE ماظن نم. ISE Posture Module ةدحو ريفوت عم عضولا يف لمعلل ةيلاتلا طورشلاب ءافولا بجي ةيئاقلتلا

. PSNs) IPs) ةسايسلا ةمدخ دقع ىلإ **CPP ب صاخلا FQDN** لحب DNS موقي نأ بجي .1

2. تاكبشل **(يضارتفا لكشب CPP (8443 فنمو 443 و 30 TCP ذفانمب** حامسلا بجي SN IPs. يما متيس) HTTP ربع ةرشابم CPP FQDN حتف ىلإ ليمعلا جاتحي HTTP وأ (HTTPS لكشب 8443) HTTPS ذفنم ىلإ بلطلا اذه هيجوت ةداعإ متيسو ،HTTPS وأ يذفنمل كلذ ربع ةلاحلا لقتنت مث (يضارتفا

متت .**SAN لقح** يف **CPP FQDN يلع** PSN دقع ىلع **CPP و Admin تاداەش** يوتحت نأ بجي .3 ةداەش ةطساوب 443 TCP ربع PSN ةدقعو VPN ةكبش مدختسم نيب لاصتالا ةيامح قداەش ةطساوب CPP ذفنم ىلع لاصتالا ةيامح متيو لوؤسملا

ةداەشل اقفو :**ةظحالم** مقطنم ةكبش ميق ديدحت مت اذإ CN لەاجت بجي ،<u>RFC6125</u> ةداەشل اقفو :**ةظحالم** يف CPP و ةرادإلا تاداەش نم CN ةفاضإ ىلإ اضيأ ةجاحب اننأ ينعي اذه .(SAN) نيزختلا .قلباقملا تاداەشلا نم SAN لقح

وأ <u>عضول ا</u>لمعي نلف ،<u>CSCvj76466</u> ل حالصإ ىلع يوتحي ISE جمانرب نكي مل اذإ :**قظحالم** تمت يذلا هسفن PSN ىلع ليمعلا دادمإ وأ رباختلا ريفوت مت اذإ الإ ليمعلا دادمإ ميلع ليمعلا ةقداصم.

:ةيلاتلا تاوطخلا قفدتلا نمضتي ،FlexVPN مادختساب عضولا ةلاح يف

AnyConnect. ليمع مادختساب FlexVPN عزومب مدختسملا لصتي .1

2. لوصولا يف مكحتلا ةمئاق مساب FlexVPN روحم ىلإ لوصولا لوبق ISE لسري (ACL) لوصولا ديءقتل اهقيبطت مزلي يتلا.

3a. الا تامدخ كرحم ةيعضو) ISE Posture قدحو أدبت - يوديلا دادمإلاب لوألا لاصتالا 3a. (ISE فنم ربع enroll.cisco.com ىلإ رابسملا لسري يذلا جهنلا مداخ فاشتكا يف (ISE) قدحوب قصاخلا تاليزنتلاب صاخلا عضولا فيرعت فلم نيوكت مت ،ةعجان ةجيتنك .8905 ليمعلا بناج يلع ةيطمنلا قفاوتلا قدحو ثيدحتو عضولا.

تامدخ كرحم ةيعضو) ISE Posture قدحو مدختست فوس ،ةيلاتلا لاصتالا تالواحم ءانثأ فيرعت فلمل "لزنملاب لاصتالا ةمئاق" يف ةددحملا IPs و ءامسألا اضيأ (ISE) ةيوهلا جەنلا مداخ فاشتكال عضولا.

ليزنت متي .FQDN ربع CPP حتفب ليمعلا موقي - يئاقلتلا دادمإلاب لوألا لاصتالا . ليزنتب موقي مث ،ليمعلا لمع ةطحم ىلع ةججان ةجيتنك "ةكبشلا دادعإ دعاسم" عضولا فيرعت زجومو ISE Posture قفاوت ةدحوو ةيطمنلا ISE Posture قدحو تيبثتو

(ISE) ةيوەلا تامدخ كرحم ةيعضو ةدحو مدختست فوس ،ةيلاتلا لاصتالا تالواحم ءانثأ مداخ فاشتكال عضولا فيرعت فلمل "لزنملاب لاصتالا" ةمئاق يف ةددحملا IPs و ءامسأ جەنلا

. ISE ىلإ ققحتلا جئاتن لسرتو لاثتمالا نم ققحتلا تايلمع عضولا ةدحو أدبت .4

روحم ىلإ Access-Accept لاسراب ISE موقي ذئدنعف ،ةقڧفاوتم ليمعلا ةلاح تناك اذإ .5 ليمعلا ىلع اەقيبطت متي يكل (ACL) لوصولا يف مكحتلا ةمئاق مساب FlexVPN. قڧاوتملا

، ةكبشلا ىل لوصولا قح ىلع ليمعلا لصحي.

<u>قنراقم</u> دنتسملا يف اهيلع روثعلا كنكمي يتلا عضولا ةيلمع لوح ليصافتلا نم ديزم <u>و Post 2.2 طمن ةنراقم) ISE Posture طمن الا الحمن العمن ا</u>

نيوكتلا

ةكبشلل يطيطختلا مسرلا



ةكبش مدختسم لصحيس VPN قال المان المراجل المان المراجبي المراجبي المراجبي المراجبي المراجبي المراجبي المراجبي ال المان المراجبي المراجب

DNS مداخ نيوكت

. مداخك DNS مادختسإ متي ،دنتسملا اذه يف DNS.

:**IP J PSN ل ال** يلإ ريشي **Iogin.cisco.com ل (A) فيضمل**ا لجس ةفاضإ .1 ةوطخلا

File Action Wew Help Server Manager (PUSTVUSO-OC-1) Active Directory Certificate Services Active Directory Certificate Service Active Directory Certificate Services Acti
Image: Public Product Image: Public Produ
 Active Directory Continues Sparent folder) Photo Server Conditional Forwarders Conditional Forwarders Storage

اذه يف مدختسملا لجس ةفاضإ .2 ةوطخلا (A) فيضملا لجس ةفاضإ .2 ةوطخلا ل جس ةفاضإ .2 قوطخلا (لان مرك العن مرك العن العن المرك العن المرك العن المرك العن المرك المرك المرك المرك المرك ا

🛼 Server Manager				
File Action View Help				
🗢 🔿 🗡 📰 💥 🖼 🗟 🚺 📑 📑 👘				
Server Manager (PUSTVUGO-DC-1) Active Directory Certificate Services Active Directory Domain Services DHCP Server DNS Server DNS PUSTVUGO-DC-1 Global Logs Forward Lookup Zones Comparison	example.com 6 record(s) Name (same as parent folder) (Type Start of Authority (SOA) Name Server (N5) Host (A) Host (A) Host (A) Host (A)	Data [13], pustyugo-dc-1 10.48.30.127 10.48.30.127 10.48.30.128	cpp Properties ? × Host (A) Security Host (uses parent domain if left blank):
C example.com C example.com C exercise Lookup Zones C exercise Look				Image: Second

IOS XE يلوألا نيوكتلا

ةيوەلا ةداەش نيوكت

صيخرت نوكي نأ بجي .AnyConnect ليمع ىلع ەسفن ةقداصمل ةداەشلا ەجوملا مدختسيس ءانثأ ةداەشلا ريذحت بنجتل مدختسملاب صاخلا ليغشتلا ماظن لبق نم ەب اقوثوم ەجوملا لاصتالا سيسأت ةلحرم.

ةيلاتلا قرطلا ىدحإب ةيوەلا ةداەش ميدقت نكمي:

الKEv2 FlexVPN عم موعدم ريغ ايتاذ ةعقوملا تاداهشلا مادختسإ :**ةظحالم**

ەجوملا ىلع (CA) قدصملا عجرملا مداخ نيوكت - 1 رايخلا

متي ،ةلاقملا هذه يف .رخآ هجوم وأ هسفن IOS هجوم ىلع CA مداخ ءاشنا ٍ نكمي :**ةظحالم** هسفن هجوملا ىلع CA ءاشناٍ.

.CA مداخ نيكمت نم نكمتال لبق NTP مداخ عم تقولا ةنمازم ىلإ جاتحت :**قظحالم**

،ةداەشلا ەذە ةحص نم ققحتلا نم نكمتي نل مدختسملا نأ ةظحالم ىجري :**قظحالم** نم ققحتلا مت اذإ الإ ليخدلا تامجە دض ةيمحم مدختسملا تانايب نوكت نل يلاتلابو سيسأت لبق مدختسملا زاەج ىلإ اەداريتسإ متو ايودي قدصملا عجرملا ةداەش لااصتالا

CA: مداخل RSA حيتافم ءاشنإ .1 ةوطخلا

FlexVPN-HUB(config)# crypto key generate rsa label ROOT-CA modulus 2048 حيتافم عاشنإ .2 ةوطخلا RSA تيوەلا قداەشل

FlexVPN-HUB(config)# crypto key generate rsa label FLEX-1 modulus 2048 قوحتلا:

FlexVPN-HUB# show crypto key mypubkey rsa

---- output truncated -----Key name: ROOT-CA Key type: RSA KEYS Storage Device: private-config Usage: General Purpose Key Key is not exportable. Redundancy enabled. Key Data: 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C01F04 E0AF3AB8 97CED516 3B31152A 5C3678A0 829A0D0D 2F46D86C 2CBC9175 ----- output truncated ----- output truncated ----- Key name: FLEX-1 Key type: RSA KEYS Storage Device: private-config Usage: General Purpose Key Key is not exportable. Redundancy enabled. Key Data: 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 009091AE 4185DC96 4F561F7E 506D56E8 240606D0 CC16CC5E E4E24EEB 1664E42C ----- output truncated

:قدصملا عجرملا نيوكتب مق .3 ةوطخلا

ip http server crypto pki server ROOT-CA issuer-name cn=ROOT-CA.example.com hash sha256 lifetime certificate 1095 lifetime ca-certificate 3650 eku server-auth no shutdown ققرحتال:

FlexVPN-HUB# show crypto pki server Certificate Server ROOT-CA: Status: enabled State: enabled Server's configuration is locked (enter "shut" to unlock it) Issuer name: cn=ROOT-CA.example.com CA cert fingerprint: A5522AAB 1410E645 667F0D70 49AADA45 Granting mode is: auto Last certificate issued serial number (hex): 3 CA certificate expiration timer: 18:12:07 UTC Mar 26 2021 CRL NextUpdate timer: 21:52:55 UTC May 21 2018 Current primary storage dir: nvram: Database Level: Minimum - no cert data written to storage IJZOT TrustPoint: interface loopback 0
ip address 10.10.10.10 255.255.255.255
crypto pki trustpoint FLEX-TP-1
enrollment url http://10.10.10.10.80
fqdn none
subject-name cn=flexvpn-hub.example.com
revocation-check none
rsakeypair FLEX-1

:قدصملا عجرملا ةقداصم .5 ةوطخلا

FlexVPN-HUB(config)#crypto pki authenticate FLEX-TP-1
Certificate has the following attributes:
 Fingerprint MD5: A5522AAB 1410E645 667F0D70 49AADA45
 Fingerprint SHA1: F52EAB1A D39642E7 D8EAB804 0EB30973 7647A860

% Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted.

:CA ىلٍ ەجوملا ليجست .6 ةوطخلا

FlexVPN-HUB(config)#crypto pki enroll FLEX-TP-1 % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Re-enter password: % The subject name in the certificate will include: cn=flexvpn-hub.example.com % The fully-qualified domain name will not be included in the certificate % Include the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose FLEX-TP-1' commandwill show the fingerprint. May 21 16:16:55.922: CRYPTO_PKI: Certificate Request Fingerprint MD5: 80B1FAFD 35346D0F D23F6648 F83F039B May 21 16:16:55.924: CRYPTO_PKI: Certificate Request Fingerprint SHA1: A8401EDE 35EE4AF8 46C4D619 8D653BFD 079C44F7 :عبصإلا ةمصب ةقباطم نم دكأتو قدصملا عجرملا ىلع ةقلعملا تاداهشلا تابلط نم ققحت FlexVPN-HUB#show crypto pki server ROOT-CA requests Enrollment Request Database: Subordinate CA certificate requests:

 ReqID
 State
 Fingerprint
 SubjectName

 RA
 certificate requests:

 ReqID
 State
 Fingerprint
 SubjectName

Router certificates requests:

ReqID	State	Fingerprint	SubjectName
1	pending	80B1FAFD35346D0FD23F6648F83F039B	cn=flexvpn-hub.example.com

```
:بسانملا ReqID مادختساب ةداهشلا حنم .7 ةوطخلا
```

FlexVPN-HUB#crypto pki server ROOT-CA grant 1 تارم 10 ققحتال متيس نيوكتال اذهل اقفو) ىرخأ ةرم ةداهشال هجومال بالطي ىتح رظتنا قراسر نع ثحبا .(ققيقدا يف قدحاو قرم

May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority ةذاهشلا تىبثت نم قىقرت:

```
FlexVPN-HUB#show crypto pki certificates FLEX-TP-1
Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
  cn=ROOT-CA.example.com
Subject:
  Name: flexvpn-hub.example.com
  cn=flexvpn-hub.example.com
Validity Date:
   start date: 16:18:16 UTC May 21 2018
   end date: 18:12:07 UTC Mar 26 2021
Associated Trustpoints: FLEX-TP-1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
  cn=ROOT-CA.example.com
Subject:
  cn=ROOT-CA.example.com
Validity Date:
  start date: 18:12:07 UTC Mar 27 2018
   end date: 18:12:07 UTC Mar 26 2021
Associated Trustpoints: FLEX-TP-1 ROOT-CA
 Storage: nvram:ROOT-CAexamp#1CA.cer
```

ايجراخ ةعقوم ةداەش داريتسإ - 2 رايخلا

FlexVPN-HUB(config)# crypto pki import FLEX-TP-2 pkcs12 ftp://cisco:cisco@10.48.30.130/ password cisco123 % Importing pkcs12... Address or name of remote host [10.48.30.130]? Source filename [FLEX-TP-2]? flexvpn-hub.example.com.p12 Reading file from ftp://cisco@10.48.30.130/flexvpn-hub.example.com.p12! [OK - 4416/4096 bytes] % The CA cert is not self-signed. % Do you also want to create trustpoints for CAs higher in % the hierarchy? [yes/no]: May 21 16:55:26.344: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named FLEX-TP-2 has been generated or imported yes CRYPTO_PKI: Imported PKCS12 file successfully. FlexVPN-HUB(config)# May 21 16:55:34.396: %PKI-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully Imported. FlexVPN-HUB(config)#

IKEv2 نيوكت

:COa و RADIUS مداخ نيوكت .1 ةوطخلا

aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.48.30.127 key Cisco123
server-private 10.48.30.128 key Cisco123

aaa server radius dynamic-author client 10.48.30.127 server-key Ciscol23 client 10.48.30.128 server-key Ciscol23 server-key Ciscol23 auth-type any ضيوفتلاو ةقداصملا مئاوق نيوكت. 2 قوطخلا

aaa new-model aaa authentication login FlexVPN-AuthC-List-1 group FlexVPN-AuthC-Server-Group-1 aaa authorization network FlexVPN-AuthZ-List-1 local aaa accounting update newinfo aaa accounting network FlexVPN-Accounting-List-1 start-stop group FlexVPN-AuthC-Server-Group-1 IKEv2:

crypto ikev2 authorization policy FlexVPN-Local-Policy-1 pool FlexVPN-Pool-1 dns 10.48.30.104 netmask 255.255.255.0 def-domain example.com

:IKEv2 فيرعت فلم ءاشنإ .4 ةوطخلا

crypto ikev2 profile FlexVPN-IKEv2-Profile-1 match identity remote key-id example.com identity local dn authentication local rsa-sig authentication remote eap query-identity pki trustpoint FLEX-TP-2 dpd 60 2 on-demand aaa authentication eap FlexVPN-AuthC-List-1 aaa authorization group eap list FlexVPN-AuthZ-List-1 FlexVPN-Local-Policy-1 aaa authorization user eap cached aaa accounting eap FlexVPN-Accounting-List-1 virtual-template 10

:IPSec فيرعت فلمو ليوحت ةعومجم ءاشنإ .5 ةوطخلا

crypto ipsec transform-set FlexVPN-TS-1 esp-aes esp-sha-hmac mode tunnel crypto ipsec profile FlexVPN-IPsec-Profile-1 set transform-set FlexVPN-TS-1 set ikev2-profile FlexVPN-IKEv2-Profile-1 یرہاظ بلاق ۃہجاو ءاشنا .6 ۃوطخلا:

```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet3
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
یل جم عمجت عاش ن!. 7 ةوط خل
```

```
ip local pool FlexVPN-Pool-1 10.20.30.100 10.20.30.200
ريغ ءالمعلا لوصو دييقتل (ACL) لوصولا يف مكحت ةمئاق ءاشنإب مق 8 ةوطخلا
لوألاا ىلع تانوذألا هذه ريفوت بجي ،فورعملا ريغ عضولا ةلاح ءانثاً .نيقفاوتملاً
```

- DNS رورم ةكرح •
- 8905 و 443 و 80 ذفانملا ربع ISE PSNs ىلإ رورملا ةكرح •
- CPP FQDN لخدم اهيلإ ريشي يتلا ISE PSNs ىلإ رورملا ةكرح •
- رمألاا مزل اذإ حالصإلاا مداوخ ىلإ تانايبلا رورم ةكرح •

ضفرلا ةفاضإ متت ،حالصإلا مداوخ نودب (ACL) لوصولاا يف مكحتلا ةمئاق ىلع لاثم اذه ةياهن يف "deny ip any any" ينمض دجوي امك ،ةيؤرلا ةيناكمإل 10.0.0/24 ةكبشل حيرصلا لوصولا يف مكحتلا ةمئاق:

```
:نيقفاوتملا
```

ip access-list extended PERMIT_ALL permit ip any any ا(يرايتخإ) مسقنملا قفنلا نيوكت .10 ةوطخلا

يضارتفا لكشب ،يضارتفا لكشب كيمج هيجوت متيس ،يضارتفا لكشب ليوخت keV2 لا يف مه تنيع عيطتسي تنأ ،ةددحملا تاكبشلا ىل طقف رورم ةكرح قفنأ قيسايقلا لوصولا ةمئاق مادختسإ وأ ةددعتم تارابع ةفاضإ نكمملا نم .مسق ةسايس.

crypto ikev2 authorization policy FlexVPN-Local-Policy-1 route set remote ipv4 10.0.0.0 255.0.0.0

(يرايتخإ) ةديعبلا ةليمعلا ةزهجالل تنرتنإلا ىلٍ لوصولاً .11 ةوطخلاً

in order to نأ تنرتنإلا يف فيضملا ىل إنوبز ذفنم ديعب لا نم ةرداصلا تال اصتالا تلكش in order to نأ تنرتنإلا يف يوكي NAT-ed ا، ديدخت جاحسملا نم ناونع ip يملاعلا ىل ip access-list extended NAT
 permit ip 10.20.30.0 0.0.0.255 any

ip nat inside source list NAT interface GigabitEthernet1 overload extended

interface GigabitEthernet1
ip nat outside

interface Virtual-Template 10
ip nat inside

AnyConnect ليمع فيرعت فلم نيوكت

ظفح متي AnyConnect. فيرعت فلم ررحم مادختساب ليمعلا فيرعت فلم نيوكتب مق يف 10 و Windows 7 ىلع AnyConnect Security Mobile Client فيرعت تافلم ProgramData:\Cisco AnyConnect Secure Mobility Client\Profile.

ةحول ىلع HTTP مداخ ليطعت متي مل اذإ ."ةديقملا ةباوبلا فشك" ةزيم ليطعت .1 ةوطخلا لصو AnyConnect ل ةديقملا ةباوبلا فاشتكا ةزيم ببستتسف ،FlexVPN لصو HTTP مداخ نودب لمعي نل CA مداخ نأ ةظحالم ءاجرلا. لاصتالا

🍒 AnyConnect Profile Editor -	VPN					
File Help						
VPN	Preferences (Part 1)					
Preferences (Part 1) Preferences (Part 2) Backup Servers Certificate Pinning	Profile:\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml					
	🔲 Use Start Before Logon	☑ User Controllable				
Certificate Matching	Show Pre-Connect Message					
Mobile Policy	Certificate Store					
Server List	Windows All	•				
	macOS All	▼				
	Certificate Store Override					
	📄 Auto Connect On Start	User Controllable				
	💟 Minimize On Connect	User Controllable				
	🔲 Local Lan Access	✓ User Controllable				
	Disable Captive Portal Detection	User Controllable				
	V Auto Reconnect	User Controllable				
	Auto Reconnect Behavior	User Controllable				
	ReconnectAfterResume					

مداوخلا ةمئاق نيوكت .2 ةوطخلا:

AnyConnect Profile Editor - File Help	- VPN	
VPN Preferences (Part 1) Vreferences (Part 2)	Server List Profile:\Cisco AnyConnect Secure Mobility Client\Profile\FLEXVPN.xml	
Gertificate Pinning Certificate Pinning Certificate Pinning Certificate Enrollment Mobile Policy Server List	Server List Entry Server Lead Balancing Servers Server Lead Balancing Servers Server Lead Balancing Servers a. Display Name (required) FQDN or IP Address User Group Method During IKE Negotiation FQDN or IP Address User Group Method During IKE Negotiation Group URL Backup Servers Host Address Host Address Add Move Up Move Down Delete	▲
	OK Cancel	

- . ضرعلا مسا لخدأ •
- انم ناونع ip دم تاونع FQDN تالخد.
- . يساسأ لوكوتوربك IPsec ددح •
- ةيوه لخدأ .ةقداصم ةقيرطك EAP-MD5 ددحو "ASA ةرابع" رايتخالاا ةناخ ديدحت ءاغلإب مق اذه يف) FlexVPN لصو ةحول ىلع IKEv2 فيرعت فلم نيوكت يف لاحلا وه امك امامت IKE match identity remote key-id فيرعت فلم نيوكت متي ،لاتملا example.com تيوهك IKE).

ا قوطخلا 3. توطخلا 20 كا ProgramData:\Cisco\Cisco AnyConnect Secure Mobility ددرتمل ا رايتل ليغشت دعأو Client\Profile

فيرعتلا فلمل XML فدارم:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
```

```
<CertificateStoreOverride>false</CertificateStoreOverride>
       <ProxySettings>Native</ProxySettings>
       <AllowLocalProxyConnections>false</AllowLocalProxyConnections>
       <AuthenticationTimeout>12</AuthenticationTimeout>
       <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
       <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
       <LocalLanAccess UserControllable="true">false</LocalLanAccess>
       <DisableCaptivePortalDetection
UserControllable="false">true</DisableCaptivePortalDetection>
       <ClearSmartcardPin UserControllable="true">false</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>LocalUsersOnly</WindowsVPNEstablishment>
       <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
       <PPPExclusion UserControllable="false">Automatic
           <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
       </PPPExclusion>
       <EnableScripting UserControllable="false">false</EnableScripting>
       <EnableAutomaticServerSelection UserControllable="true">false
           <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
           <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
       </EnableAutomaticServerSelection>
       <RetainVpnOnLogoff>false
       </RetainVpnOnLogoff>
       <AllowManualHostInput>true</AllowManualHostInput>
   </ClientInitialization>
   <ServerList>
       <HostEntry>
           <HostName>FLEXVPN</HostName>
           <HostAddress>flexvpn-hub.example.com</HostAddress>
           <PrimaryProtocol>IPsec
               <StandardAuthenticationOnly>true
                   <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
                   <IKEIdentity>example.com</IKEIdentity>
               </StandardAuthenticationOnly>
           </PrimaryProtocol>
       </HostEntry>
   </ServerList>
</AnyConnectProfile>
```

ISE نيوكت

CPP و لوؤسملا تاداەش نيوكت

رييغت مت يتلاا ةدقعلا ليغشت ةداعإ ىلإ لوؤسملا ةداەش رييغت يدؤيس :**ةظحالم** اەيلع قداەشلا.

ىلع رقنا ،**تاداەشلا عيقوت تابلط <- تاداەشلا <- ماظنلا <- ةرادالا</mark> ىلإ لقتنا .1 ةوطخلا تاداە<mark>شلا عيقوت تابلط ءاشنا (CSR):</mark>**

dentity Services Engine	Home	Operations Policy		enters		
System Identity Management	Network Resources	rtal Management pxGrid S	Services Feed Service Th	nreat Centric NAC		
Deployment Licensing - Certificates	s Logging Maintenance	Upgrade Backup & Res	tore Admin Access Settin	ngs		
G						
▼ Certificate Management	Certificate Signing Reques	its				
System Certificates	Generate Certificate Signing Requ	uests (CSR)				
Trusted Certificates	A Certificate Signing Requests (CS	SRs) must be sent to and sig	ned by an external authority. Click '	"export" to downloa	d one or more CSR	s so that they may be
OCSP Client Profile	bind to bind the request to the sig	gried certificate issued by the	at autionty. Once a CSR is bound,	it will be removed if	om uns ist.	
Certificate Signing Requests	🔎 View 🚯 Export 🔀 Delete	Bind Certificate				
Certificate Periodic Check Setti	Friendly Name	C	ertificate Subject	Key Length	Portal group tag	Timestamp
Certificate Authority				No data	available	

ةيرورضلا لوقحلا ةئبعتب مقو ،ةيرورضلا PSN ةدقع ددح ةحوتفملا ةحفصلا يف .2 ةوطخلا SAN لوقح يف ةدقعلل IP ناونعو enroll.cisco.com، cpp.example.com ،ةدقعلل FQDN ةفاضإو :**ءاشنا** رقناو

dentity Services Engine	Home ► Context Visibility ► Ope	erations Policy Administrat	tion Vork Centers	
System Identity Management	Network Resources	lanagement pxGrid Services + Fe	ed Service Threat Centric NAC	
Deployment Licensing - Certificates	Logging Maintenance Upgra	ade Backup & Restore Admin	Access > Settings	
G	Usage			
▼ Certificate Management	Certificate(s) will be used for	1ulti-Use	You can use a single certificate for multiple services, but	
System Certificates			should obtain individual certificates specifically for each service (for example, one certificate each for Guest	
Trusted Certificates	Allow Wildcard Cartificates	1 @	Portals, EAP, and pxGrid).	
OCSP Client Profile				
Certificate Signing Requests	Node(s)			
Certificate Periodic Check Setti	Generate CSR's for these Nodes	r.		
Certificate Authority	Node	CSR Friendly	Name	
	✓ pustyugo-ise23-1	pustyugo-ise23	J-1#Multi-Use	
	pustyugo-ise23-2	pustyugo-ise23	i-2#Multi-Use	
	Subject			
	Common Name (CN)	FQDN\$	()	
	Organizational Unit (OU)	AC	1	
	Organization (O)	Ĵisco	()	
	City (L)			
	State (ST)			
	· · · · · · · ·			
	Country (C)			

Subject Alternative Name (SAN)	DNS Name	pustyugo-ise23-1.example.com	_	÷	
	DNS Name	enroll.cisco.com	_	+	
	DNS Name	cpp.example.com	_	+	
	IP Address 🔹	10.48.30.127		+	i
* Key type	RSA 💌 🗊				
* Key Length	2048 💌 🕡				
* Digest to Sign With	SHA-256				
Certificate Policies					
	Generate Cancel				

سفن مادختسإ كنكميف ،ةوطخلا هذه يف **ددعتم مادختسإ** ديدحتب تمق اذإ :**ةظحالم** اضيأ لخدملل ةداهشلا.

:ةيلحملا لمعلا ةطحم ىلإ pem قيسنتب CSR ظفحل **ريدصت** قوف رقنا ،رهاظلا راطإلا يف

Successfully generated CSR(s)

Certificate Signing request(s) generated:

pustyugo-ise23-1#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen



×

ةفاضإلاب CA لا نم صيخرتلا فلم ىلع لصحيو هب قوثوم CA عم CSR لا ينغي .3 ةوطخلا (طيسولاو رذجلا) CA تاداهش نم ةلماكلا ةلسلسلا ىل

قوف رقنا ،**اەب قوثوملا تاداەشلا <- تاداەشلا <- ماظنلا <- قرادالا</mark> ىلإ لقتنا .4 ةوطخلا مق ،رذجلا CA ص**يخرت فلم ددحو **فلم رايتخإ قوف رقنا ةيلاتلا قشاشلا يف .داريتسإ** قوف رقناو **اەب قوثوملا تارايخلا** يرورض ددحو ،رمألا مزل اذإ فولأملا فصولاو مسالاا ةئبعتب **لاسرا:**



يأ كانه ناك اذإ ةلسلسلا يف ةطسوتملا تاداهشلا عيمجل ةوطخلا هذه ررك.

مزاللاا CSR ددح **،تاداەشلا عيقوت تابلط <- تاداەشلا <- ماظنلا <- قرادالا</mark> ىلا عوجر .5 ةوطخلا :قداەشلا طبر** قوف رقناو



همالتسإ مت يذلا ةداهشلا فلم ددح ،فلم رايتخإ قوف رقنا ةحوتفملا ةحفصلا يف .6 ةوطخلا **:مادختسإ) لوؤسم :مادختسإ** ددح مث ،رمألا مزل اذإ فولأم مسا لاخداب مق مث ،قدصملا عجرملا نم قوف رقناو (**مادختسالا ددعتم** مادختساب CSR ءاشنإ مت اذإ انه هديدحت نكمي اضيأ **لخدم** :**لاسرا**

dentity Services Engine	Home ► Context Visibility ► Ope	ations ▶ Policy ▼Administration ▶ Work Centers
▼System ► Identity Management	Network Resources Device Portal M	nagement pxGrid Service > Feed Service > Threat Centric NAC
Deployment Licensing - Certificate	es ►Logging ► Maintenance Upgr	de Backup & Restore Admin Access Settings
Certificate Management	Bind CA Signed Certificate	
System Certificates	* Certificate File	hoose File Signed CSR.cer
Trusted Certificates		
OCSP Client Profile	Friendly Name	styugo-ise23-1 Admin
Certificate Signing Requests	Validate Certificate Extensions	
Certificate Periodic Check Setti		
Certificate Authority	Usage	
		Admin: Use certificate to authenticate the ISE Admin Portal
		EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
		RADIUS DTLS: Use certificate for the RADSec server
		pxGrid: Use certificate for the pxGrid Controller
		Portal: Use for portal
		ubmit Cancel

ليغشت ةداعإ متيس .داريتسالا ءاەنإل **معن** قوف رقنا ،قثبنملا ريذحتلا يف .7 ةوطخلا لوؤسملا ةداەش رييغتب ةرثأتملا ةدقعلا:

vice F	artal	Management pyCrid Capilage & Food Capilage & Threat Captric NAC	
ince		Enabling Admin role for this certificate will cause an application server restart on the selected node.	
icat		Note: Make sure required Certificate Chain is imported under Trusted Certificates	
icate	_	No Yes	

ددح 6 ةوطخلا يف .لخدملل ةلصفنم ةداهش مادختسإ تررق اذإ CPP ةداهش رييغت تاوطخ ررك **لاسرا** قوف رقناو **لخدم :مادختسإ:**



.ISE رشن يف PSN تاكبش عيمجل تاوطخلا ررك

ISE ىلع يلحم مدختسم ءاشنإ

.ISE ىلع طقف نييلحملا نيمدختسملا معد متي ،EAP-MD5 بولساً مادختساب :**ةظحالم**

قوف رقنا ،**نومدختسملا <- تايوهلا <- لقتسملا نايكلا ةرادا <- قرادالا** ىلا لقتنا .1 ةوطخلا ق**فاضا**.

dentity Services Engine	Home • Conte	ext Visibility	► Policy	Administratio	n 🔹 Work Ce	enters			
► System - Identity Management	Network Resources	Device Portal Manageme	nt pxGrid Service	es 🕨 Feed	Service + Thr	eat Centric NAC			
✓Identities Groups External Identi	ty Sources Identity	Source Sequences	gs						
0									
Users	Network Acces	ss users							
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 🔹 🕼	port 🛛 🕞 Export 👻	XDelete					
	Status	Name	 Description 		First Name	Last Name	Email Address	User Identity Groups	Admin
							No	data available	

ةيرورضلا تامولعملاو رورملا ةملكو مدختسملا مسا لخدأ ةحوتفملا ةحفصلا يف .2 ةوطخلا ل**اسرا** ىلع رقناو ىرخألا.

dentity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers
► System - Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
◄ Identities Groups External Identit	/ Sources Identity Source Sequences
G	Notwork Accore Lines New Network Accore Lines
Users	
Latest Manual Network Scan Results	
	* Name vpnuser
	Status Enabled -
	Email
	▼ Passwords
	Password Type: Internal Users 🔹
	Password Re-Enter Password
	* Login Password Generate Password (
	Enable Password Generate Password ()
	▼ User Information
	First Name
	▼ Account Options
	Description
	Change password on next login
	▼ Account Disable Policy
	Disable account if date exceeds 2018-07-27 (yyyy-mm-dd)
	▼ User Groups
	ALL_ACCOUNTS (default) 📀 — 🕂
	Submit Cancel

RADIUS ليمعك FlexVPN عزوم ةفاضإ

.**ةفاضإ** رقنا ،**ةكبشلا ةزەجأ <- عضولا <- لمعلا زكارم** ىلا لقتنا .1 ةوطخلا

cisco Identity	Services Engine	Home ► Co	ontext Visibility	Operations	▶ Policy	 Administration 	✓ Work Centers	
Network Acces	s 🔸 Guest Acces	s + TrustSec + I	BYOD Profiler	▼ Posture	Device Admir	nistration • Pas	siveID	
Overview Net	work Devices + C	lient Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports + Settings	
Naturals Davi								
Network Devi	ces							
/ Edit 🕂 Add	Duplicate	Export	Generate PAC	🗙 Delete				
Name	▲ IP/Mask	Profile Name		Location		Туре		Description
								No data available

ددح ،ىرخألاا ةيرورضلا تامولعملا ،P، ناونع ،زاهجلا مسا لخدأ ةحوتفملا ةحفصلا يف .2 ريتس لفسأ يف **لاسرا** رقناو كرتشملا رسلا لخدأ ،"RADIUS ةقداصم تادادعإ" رايتخالاا ةناخ .ةحفصلا

uluilu cisco	Identity Services Engine	Home ► Context Vis	ibility 🕨 K	Operations	▶ Policy	Administration	✓ Work Centers				
Net	work Access	TrustSec BYOD	Profiler	▼ Posture	Device Admi	nistration Pa	ssiveID				
Overv	iew Network Devices + Clie	ent Provisioning	lements Po	osture Policy	Policy Sets	Troubleshoot	Reports Setting	S			
Networ	k Devices List > New Network D ork Devices	* Name FlexVPN-HUB Description FlexVPN HUB									
11											
	IP Address ▼ * IP : 1	0.48.71.183		/ 32							
O IP	● IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected * Device Profile ditte Cisco ▼ ⊕										
	Ма	odel Name	-								
	Softwa	re Version	•								
*	Network Device Group										
	Location All Locations	Set To Default									
	IPSEC Is IPSEC Device	Set To Default									
D	evice Type All Device Types	Set To Default									
•	→ RADIUS Authentication Setting	JS									
	RADIUS UDP Settings										
		Protocol	RADIUS								
		- Snared Secret	•••••		Show						
		ose second snared secret			Show						
		CoA Port	1700		Set T	o Default					
	RADIUS DTLS Settings (i)										
		DTLS Required	(i)								
		Shared Secret	radius/dtls		(j)						
		CoA Port	2083		Set T	o Default					
	Issuer C	JA OF ISE Certificates for CoA	Select if rec	quired (optiona	al)	• (i)					
		Dino iname									
	General Settings										
		Enable KeyWrap	i								
	* ****	* Key Encryption Key			Show						
	^ Mes	Key Input Format			Show						
_		ivey input i onliat									
	TACACS Authentication Setting	gs									
	 SNMP Settings 										
	 Advanced TrustSec Settings 										
Cubr	vit Cancol										

ليمعلا دادمإ نيوكت

AnyConnect. نيوكت دادعإل تاوطخلا يه هذه

رشابملا ليزنتلل اهسفن AnyConnect ةمزح رفوتت ال AnyConnect ةمزح ليزنت .1 ةوطخلا نكمي .يصخشلا رتويبمكلا ىلع ددرتملا رايتلا رفوت نم دكأت ،عدبلا لبق كلذل ،ISE نم اذه يف .<u>http://cisco.com/go/anyconnect</u> - ددرتملا رايتلا ليزنتل طابترالا اذه مادختسإ AnyConnect-win-4.5.05030-webdeploy-k9.pkg.

ا يلا قمزح ISE، المع**لا زكارم** يل القتنا ،2. in order to upload AC يل قمزح ISE، يل قوطخلا 2. in order to upload AC جال عن العام ين المعالي القتنا ،3E، القتنا ،3E، القتنا بعن المعالي المحالي المعالي الم معالي معالي المعالي المع معالي معالي المعالي المع معالي معالي المعالي الم

cisco Identity Services Engine	Home Context Visibility	Operations Policy	► Administration		
Network Access Guest Access	TrustSec BYOD Profile	er ▼Posture ► Device Adm	ninistration PassiveID		
Overview Network Devices - Clie	nt Provisioning Policy Elements	Posture Policy Policy Sets	Troubleshoot Reports + Setting	s	
Client Provisioning Policy	Agent Resources From Local Disk Agent Resources From Lo	k > Agent Resources From Loca Ocal Disk	al Disk		
Resources					
Client Provisioning Portal	Category	Cisco Provided Packages Choose File anyconnect-	▼ (j) ploy-k9.pkg		
	-	 AnyConnect Uploaded R 	esources		
		Name	▲ Туре	Version	Description
		AnyConnectDesktopWindows 4	.5.503 AnyConnectDesktopWindows	4.5.5030.0	AnyConnect Secure Mobility Clien
	Submit Cancel				

د**يكأت** ىلع طغضاو ةمزحلا ةئزجت نم ققحت .داريتسالا ءاەنإل **لاسرا** قوف رقنا.

-- لمعلا زكارم) ةحفصلا سفن يف ISE. ىل قي طمنلا قفاوتلا قدو ليمحت بجي 3. قوطخلا يو العاري المعلية والمعلية المعلية في المعلية في المعلية الم معلم المعلية المع معلية المعلية المعلي المعلي المعلية المعلية المعلية المعلية المعلية المعلية المعلية المعلية المعلية المعلي

Dov	vnload Remote Resources		×
	Name 🔺	Description	
	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Wir .	
	AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2	
	AnyConnectComplianceModuleOSX 4.3.29.0	AnyConnect OSX Compliance Module 4.3.29.0	
	AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2	
✓	AnyConnectComplianceModuleWindows 4.3.50.0	AnyConnect Windows Compliance Module 4.3.50.0	
	CiscoTemporalAgentOSX 4.5.02036	Cisco Temporal Agent for OSX With CM: 4.2.1019.0 Works wi	
	CiscoTemporalAgentWindows 4.5.02036	Cisco Temporal Agent for Windows With CM: 4.2.1226.0 Work	
	ComplianceModule 3.6.11510.2	NACAgent ComplianceModule v3.6.11510.2 for Windows	
	MACComplianceModule 3.6.11510.2	MACAgent ComplianceModule v3.6.11510.2 for MAC OSX	
	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3	
	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12,	
	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1	
	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE	
	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE	
	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE	
	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE	-
		•	

٣

For AnyConnect software, please download from http://cisco.com/go/anyconnect. Use the "Agent resource from local disk" add option, to import into ISE

Save Cancel

وأ NAC ليكو رتخاو **ةفاضإ** ىلع رقنا .نآلا AC Posture فيرعت فلم ءاشنإ بجي .4 ةوطخلا **ميعضو فيرعت فلم** AnyConnect.

cisco Identity Services Engine	Home	Operations Policy	Administration	✓ Work Centers
Network Access Guest Access	TrustSec BYOD Profiler	▼ Posture	nistration + Pass	iveID
Overview Network Devices - Clier	t Provisioning Policy Elements	Posture Policy Policy Sets	Troubleshoot	Reports + Settings
Client Provisioning Policy	ISE Posture Agent Profile Settings	> New Profile		
Resources	Posture Agent Profile Settings			
Client Provisioning Portal	a. AnyConnect b. * Name: AC-4.5-Posture			
	Agent Behavior			

- . ويرانيسلا اذهل AnyConnect مادختسإ بجي .فيصوتلا عون رتخأ •
- فيرعتلا فلم يف **عضولا لوكوتورب** مسق ىلإ لقتنا .فيرعتلا فلم مسا ددح •

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* a .	need to be blank by default to force admin to enter a value. "#" means agent will connect to all
Call Home List	pustyugo-ise23-1.exampl b .	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

Note: It is recommended that a separate profile be created for Windows and OSX deployments

Submit Cancel	
---------------	--

- ىلع لقحلا يوتحي نأ نكمي .اغراف لقحلا اذه نوكي نأ نكمي ال ،**مداخلا مسا دعاوق** ددح ةحاسم نم PSNs ب ددرتملا رايتلا ةيعضو ةدحو لاصتا ديقي يذلا لدبلا فرحب FQDN يأب حامسلا بجي ناك اذإ ةمجن عضو .ةبسانملا مسالا
- عجار) عضولا فاشتكا نم 2 ةلحرملا ءانثأ مادختسالا ديق انه ةددحملا IPs و ءامسألا بسح ةلصفنم ءامسأ ةفاضإ كنكمي .(مسق "<u>ISE 2.2 يف عضولا قفدت</u> نم 14 ةوطخلا دعب ذفنملا مقر كلذكو COMA دعب ذفنمل مقر كلذكو FQDN/IP

ان ان مق.5 ةوطخل AC. ح**- لمعلا زكارم** ىل لقتنا AC. حاي ان عاشن إب مق.5 ةوطخل AC. حاي مق.5 قوطخل AC. مي من المعن ا مي من المعن الم



- .ددرتم رايت ةمزح ددح •
- ددرتملا رايتلا نيوكت مسا ريفوتب مق.
- ةيطمنلا قفاوتلا ةدحو رادصإ رتخأ.

.قلدسنملا ةمئاقلا نم ددرتملا رايتلا ةيعضو نيوكت فيرعت فلم ددح • يف .**ليمعلا دادمإ <- عضولا <- لمعلا زكارم** ىلإ لقتنا .ليمعلا ريفوت جەن نيوكت .6 ةوطخلا عم مدقملا جەنلا يف ةغرافلا ميقلا قئبعت كنكمي ،يلوألا نيوكتلا قلاح جەنلا ىلإ لقتنا ،دوجوملا عضولا نيوكت ىل جەن ةفاضإل ةجاحلا قلاح يف .تايضارتفالا ديدج جەن ءاشنإ نكمي امك **.ماندا راركت** وأ **مالعا راركت** رتخاو ەمادختسإ ةداعإ نكمي يذلا .

دنتسملا يف ةمدختسملا ةسايسلا ىلع لاثم اذه.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺	९ 🙆
Network Access Guest Access	TrustSec BYOD Profiler Posture Device Administration PassiveID		
Overview Network Devices Client	Provisioning + Policy Elements Posture Policy Policy Sets Troubleshoot Reports + Settings		
0			
Client Provisioning Policy	Client Provisioning Policy		
Resources	Define the Client Provisioning Policy to determine what users will receive uno login and user session initiation: Por Agent Configuration: version of agent compliance and user compliance and agent c		
Client Provisioning Portal	ron narre depisition configuration, multiple allocal multiple and social register or the rote.		
	Rule Name Identity Groups Operating Systems Other Conditions Results		
	🖋 🖉 🕶 Windows II Any 🔷 and Windows All 🔷 and Condition(s) 🔷 Iblin AnyConnect		
	Agent Configuration		*
	Agent: AnyConnect Configuration 📀		
	Native Supplicant Configuration		
	Config Witzard [Choose a Config Witzard]		
	Wizard Profile Choose a Wizard Profile 📀		-
	4) b

جئاتنلا مسق يف ددرتملا رايتلا نيوكت رتخأ.

عضولا طورشو تاسايس

مت العن العن العن الحرف مادختس العني C:\TEST.txt فلملا المرابي العن العن المربي التعامي المتي C:\TEST.txt تاوطخ نكلو اديقعت رثكاً ةيعقاولا ةايحلا تاهويرانيس نوكت دق .يفرطلا زاهجلا بناج ىلع اهسفن يه ماعلا نيوكتلا.

رصانع <- عضولا <- لمعلا زكارم يف عضولا طورش دجوت .ةلاح ءاشناب مق .1 ةوطخلا رقناو ةيرورضلا تامولعملا ددح .**ةفاضا** *رقناو عضولا طرش عون رتخاً* .**طورشلا <- ةسايسلا** فلملا دوجو نم ققحتلا بجي يذلا ةمدخلا طرشل لاثم ىلع روثعلا كنكمي ،هاندأ .**ظفح** C:\TEST.txt.

cisco Identity Services Engine	Home ► Context Vi	/isibility ► Operations	▶ Policy	Administration	✓ Work Centers
Network Access Guest Access	TrustSec BYOD	► Profiler	Device Admir	nistration 🔹 🕨 Pas	siveID
Overview Network Devices + Clie	nt Provisioning - Policy	Elements Posture Policy	Policy Sets	Troubleshoot	Reports Settings
Conditions Hardware Attributes Condition Application Firewall Condition Anti-Malware Anti-Spyware Anti-Virus Compound Dictionary Simple Dictionary Compound Disk Encryption	File Conditions List > T File Condition * Name Description * Operating System Compliance Module * File Type * File Path * File Operator Save Reset	rest_txt TEST_txt Windows All Any version FileExistence ABSOLUTE_PATH Exists	▼ (j) ▼ (j) ▼ (C:\TEST.txt	Ĩ
File					
Patch Management					
Registry					
Service					
USB					

<- جەنلا رصانع <- عضولا <- لمعلا زكارم ىلإ لقتنا .ليكشت بلطتم 2.Posture قوطخ تقلمل TEST.txt دوجو ىلع لاثم اذه .تابلطتملا



حالصإ ءارجإ ددحو ديدج بلطتم يف كب صاخلا عضولا طرش رتخأ.

كنكمي هاندأ .**عضولا جەن <- عضولا <- لمعلا زكارم** ىلإ لقتنا .عضولا جەن نيوكت .3 ةوطخلا "فلملا دوجو" بلطتم ىلع جەنلا يوتحي .دنتسملا اذەل مدختسملا جەنلل لاثم ىلع روثعلا اەنييعت مت ىرخأ طورش يأ ىلع يوتحي الو يمازلإك ەنييعت مت يذلا

- ilii CIS	dentity	Services Engir	ne Home	Context Visibility	 Operations 	▶ Policy	Administration	✓ Work Centers			
•	Network Acces	ss 🔹 🕨 Guest Ac	cess + TrustSec	+ BYOD + Profile	er v Posture	Device Adm	inistration + Pas	siveID			
0	verview Net	twork Devices	Client Provisionin	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports + Settin	19		
Po: Def	sture Policy	/ e Policy by config	uring rules based or	n operating system and/	or other conditions						
*											
	Status	Rule Name		Identity Groups	Operating Sy	stems	Compliance M	odule	Posture Type	Other Conditions	Requirements
	• •	File Policy	If [Any 🔶 a	nd Windows Al	। 🚓 and	4.x or later	▼ an	AnyConnect	and (Optional) Dictionar	↔ then File Existance

ليمعلا ريفوت لخدم نيوكت

ىلإ لقتنا .ليمعلا ريفوت لخدم نيوكت ريرحت بجي ،هيجوتلا ةداعإ نودب عضولل ةبسنلاب ةباوبلا مادختسإ كنكمي **ليمعلا دادمإ لخدم<- ليمعلا دادمإ <- عضولا <- لمعلا زكارم** كب ةصاخلا ةباوبلا ءاشنإ وأ ةيضارتفالا.

dentity Services Engine	Home	Context Visibility	 Operations 	Folicy	 Administration 	✓ Work	Centers	
Network Access Guest Access	TrustSec	BYOD Profile	er vesture	Device Ad	ministration + P	assiveID		
Overview Network Devices - Client	Provisioning	Policy Elements	Posture Policy	Policy Set	ts Troubleshoot	Reports	 Settings 	
Client Provisioning Policy Resources Client Provisioning Portal	-	Portal Settings	HTTPS	port.* 844 (8000	3			
			Allowed Interf	aces:* For PS Gig Gig Gig Gig Gig Gig	BNS Using Physical abit Ethernet 0 abit Ethernet 1 abit Ethernet 2 abit Ethernet 3 abit Ethernet 4 abit Ethernet 5	Interfaces		For PSNs with Bonded Interfaces Configured ✓ Bond 0 Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup Bond 1 Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup Bond 2 Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
		ſ	Certificate group	tag: * Defau Configu Admir Syster	It Portal Certificates ure certificates at: histration > System m Certificates ser_ID_Stores	Group ▼ n > Certifica ▼	a.	
		_		Admir Identii	histration > Identity ty Source Sequen	y Managem ces	ent >	
			C U	onfigure auth ser account wit	orized groups h Super admin privile	ge or ERS ad	min privilege w	ill have access to the portal
				Available			Chos	ien
			а а а а а а а а а а а а а а а а а а а	AD: AD: AD: AD: AD: AD: D: Employee SROUP_ACCOUN	/Builtin/Administra /Users/Domain Co /Users/Domain Co /Users/SE Admins /Users/VPN Admin /Users/VPN User JNTS (default) ITS (default)	tors mputers ers	→ ()	ACCOUNTS (default)
								× Clear all
		Fully qualified	d domain name (F	QDN): cpp	.example.com		C.	
			Idle tin	neout: 10		1	-30 (minutes)	

هيجوتلا ةداعإ مدع ويرانيسل لخدملا نيوكت يف تادادعإلا هذه ريرحت بجي

ديدحت SSO ىلع رذعت اذإ ەمادختسإ بجي يذلا ةيوەلا ردصم لسلست ددح ،ةقداصملا يف •

مدختسملا ةسلج عقوم.

- دنع .ةحاتملا تاعومجملا ةمئاق علم متي ،ةددحملا "ةيوەلا ردصم لسلست" ةمئاقل اقفو لخدملا ىلإ لوخدلا ليجستل ةدمتعملا تاعومجملا ديدحت ىلإ جاتحت ،ةطقنلا ەذە.
- هيجوت بجي .ISE PSNs IPs ىلإ اذه FQDN لح بجي .ليمعلا ديوزت لخدمل FQDN ديدحت بجي .ىلوألا لاصتالا ةلواحم ءانثأ بيولا ضرعتسم يف FQDN ديدحتل نيمدختسملا

جەنلاو ليوختلا تافيصوت نيوكت

نكمملا نمو .ةرفوتم ريغ عضولا ةلاح نوكت امدنع ليمعلل يلوألا لوصولا دييقت مزلي ةددعتم قرطب ةياغلا هذه قيقحت:

- RADIUS Filter-ID لوصولا يف مكحتلا ةمئاق نييعت نكمي ،ةمسلا هذه مادختساب (ACL) هذه نأل ارظنو .ةفورعم ريغ عضو ةلاح هيدل يذلا مدختسملل NAD ىلع ايلحم ةفرعملا يدروم عيمجل ديج لكشب جهنلا اذه لمعي نأ بجيف ،RFC لوحمل ةيسايق ةمس
- Cisco:Cisco:AV-pair = ip:interface-config ل ادج ل ثامم Radius Filter-ID، لوصول ي قمئاق نييعت نكمي (ACL) لوصول ا يف مكحتل ريغ عضول ا قلاحب مدختسملل NAD كلع ايل م قفرعمل (ACL) لوصول يف مكحتل ا :نيوكتل كلع ل اثم فورعمل Cisco-av-pair = ip:interface-config=ip access-group deny_server ي

ليوختلا فيرعت فلم نيوكت .1 ةوطخلا.

لوألاا رايخلاا يوتحي نأ بجي .ليوخت يفيصوت دوجو مزلي ،عضولل ةبسنلاب داتعم وه امك ىلع اذه فيرعتلا فلم قيبطت نكمي .ةكبشلا ىلإ لوصولا دويق عاونأ نم عون يأ ىلع فيرعت فلم يوتحي دق .قفاوتلا اهل عضولا ةلاح يواست ال يتلا ةقداصملا تايلمع ةلاحلاب لمع ةسلج ىلع هقيبطت نكميو طقف حامس تايناكمإ ىلع يناثلا ليوختلا .قفاوتلا يواست "ةيعضو"

تافلم <- جەنلا رصانع <- عضولا <- لمعلا زكارم ىلإ لقتنا ،ليوختلا فيرعت فلم ءاشنإل ليوختلا فيرعت.

RADIUS Filter-ID: مادختساب ديقملا لوصولا فيرعت فلم ىلع لاثم

cisco Identity Services Engine	Home	Operations Policy Admi	nistration Vork Centers
Network Access Guest Access	TrustSec BYOD Profiler	Posture Device Administration	n • PassiveID
Overview Network Devices + Clier	The Provisioning Policy Elements	Posture Policy Policy Sets Troub	leshoot Reports + Settings
0	Authorization Drafiles - LTHITTE		
	Authorization Profile	ACCESS	
Hardware Attributes Condition	* Name LIMI	TED_ACCESS	
Application	Description		
Firewall Condition	* Access Type Acce	SS ACCEPT ¥	
Anti-Malware	- Acc	JJ_NGGET	
Anti-Spyware	Network Device Profile	isco 🔻 🕀	
Anti-Virus	Service Template		
Compound	Track Movement		
Dictionary Simple	Passive Identity Tracking		
Dictionary Compound			
Disk Encryption			
File	- Common Tacks		
Patch Management	· common rusks		
Registry	DACL Name		
Service			
USB	ACL (Filter-ID)	DENY_SERVER	.in
Remediations	_		
Requirements	Security Group		
Allowed Protocols			
Authorization Profiles			
Downloadable ACLs			
	Advanced Attributes Set	tings	
	· Advanced Attributes Set	lings	
	Select an item		⊘ +
	 Attributes Details 		
	Access Type = ACCESS_ACCEPT		
	Filter-ID = DENY_SERVER.in		

:Cisco-AV ةزهجأ جوز مادختساب ديقملا لوصولا فيرعت فلم ىلع لاثم

alialia cisco	Iden	tity Ser	vices Eng	jine	Home	 Context Visibil 	ity	 Operations 	Policy	Administration	→ Wor	k Centers		
► Net	work A	ccess	Guest A	Access	TrustSec	+ BYOD +	Profiler	✓ Posture	Device Admi	nistration + Pa	ssiveID			
Overv	view	Networ	k Devices	Clier	nt Provisioning	- Policy Elen	nents	Posture Policy	Policy Sets	Troubleshoot	Reports	 Settings 	3	
				G										
- Cond	litions				Authorizatio	on Profiles > LIN	1ITED_A	ACCESS						
Hard	dware A	Attribute	s Condition		Autionz	* Name	TIMIT	TED ACCESS						
Appl	lication					Description		LD_ACCESS						
Fire	wall Co	ndition				* Access Type								11
Anti-	Malwa	re				Access Type	ACCES	SS_ACCEPT	Ŧ					
Anti-	Spywa	re			Network I	Device Profile	dette Ci	isco 🔻 🕀						
Anti-	Virus				s	ervice Template								
Com	pound				т	Frack Movement								
Dicti	ionary \$	Simple			Passive I	dentity Tracking								
Dicti	onary (Compou	nd			,	U U							
Disk	Encry	otion												
File														
Patc	h Man	agemen	t		▼ Comr	non Tasks								
Reg	istry					L Name								
Serv	rice													
USB	3				AC	L (Filter-ID)								
▶ Reme	ediatio	ns												
Require	ments				Sec Sec	urity Group								
Allowed	I Proto	ols			_									
Authoria	zation F	Profiles				AN								
Downlo	adable	ACLs												
					▼ Advar	nced Attribute	es Sett	ings						
						-1					1			
					II CISCO:0	cisco-av-pair		= lip:in	iterrace-config=	ip access-g 🥹]- +			
					▼ Attrib	outes Details								
					Access T	ype = ACCESS_	ACCEPT							
					cisco-av-	-pair = ip:interfa	ce-config	g=ip access-gro	up DENY_SERVE	ER in				

:RADIUS ةيفصت لماع فرعم عم دودحملا ريغ لوصولا صيصخت فلم ىلع لاثم

alialia cisco	Identity Se	rvices Eng	jine	Home	Context Visibility	Operations	▶ Policy	Administration	- Work	Centers	
Net	work Access	Guest A	Access	TrustSec	BYOD Profiler	✓ Posture	Device Adm	inistration + Pa	assiveID		
Overv	iew Networ	k Devices	Clier	nt Provisioning		Posture Polic	y Policy Sets	Troubleshoot	Reports	 Settings 	}
			G		* Name UNL	IMITED_ACCES	5				
- Cond	itions				Description						1.
Hard	ware Attribute	s Condition			* Access Type ACC	ESS_ACCEPT	*				
Appli	ication			Network	Device Profile 📷 🤇	Cisco 🔻 🕀					
Firev	vall Condition				ancies Templete						
Anti-	Malware				ervice remplate						
Anti-	Spyware			1	rack Movement						
Anti-	Virus			Passive I	dentity Tracking 🔲 👔						
Com	pound										
Dictio	onary Simple										
Dictio	onary Compou	ind		▼ Comr	non Tasks						
Disk	Encryption				Nome						
File				U DAG	L Name						
Patcl	h Managemen	t		AC	L (Filter-ID)	PE	RMIT ALL		in		
Regi	stry				- (,		_				
Serv	ice			Sec	urity Group						
USB											
Reme	diations				AN .						
Require	ments										
Allowed	Protocols										
Authoriz	ation Profiles			▼ Adva	nced Attributes Set	tings					
Downloa	adable ACLs										
				Select	an item	=			9-+		
				▼ Attrit	outes Details	_					
				Access T Filter-ID	ype = ACCESS_ACCEP = PERMIT_ALL.in	Т					

:Cisco-AV ذفانم جوز مادختساب دودحملا ريغ لوصولا فيرعت فلم ىلع لاثم

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access	
Overview Network Devices + Clie	nt Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
9	* Name UNLIMITED_ACCESS
	Description
Hardware Attributes Condition	* Access Type ACCESS_ACCEPT -
Application	Network Device Profile data Cisco V
Firewall Condition	
Anti-Malware	Service Template
Anti-Spyware	Track Movement
Anti-Virus	Passive Identity Tracking
Compound	
Dictionary Simple	
Dictionary Compound	▼ Common Tasks
Disk Encryption	
File	DACL Name
Patch Management	
Registry	
Service	Security Group
USB	
Remediations	VLAN VLAN
Requirements	
Allowed Protocols	
Authorization Profiles	▼ Advanced Attributes Settings
Downloadable ACLs	
	Cisco:cisco-av-pair 📀 = ip:interface-config=ip access-g 📀 — 🕂
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT cisco-av-pair = ip:interface-config=ip access-group PERMIT ALL in
	errer han dennes rend ik ordere groek i we kr_nes n

لوألاا .نينثإ ليوخت جەن ءاشنإ بجي ةوطخلا ەذە ءانثأ .ليوختلا جەن نيوكت .2 ةوطخلا لوصولا نييعتل يناثلاو فورعملا ريغ عضولا ةلاح عم يلوألا ةقداصملا بلط ةقباطمل حجانلا عضولا ةيلمع دعب لماكلا.

ةلاحلا هذهل ةطيسبلا ليوختلا تاسايس ىلع لاثم هنإ:

✓ Authorization Policy (12)											
					Results	Results					
•	Status	Rule Name	Condit	ns	Profiles	Security Groups	Hits	Actions			
Search											
	Ø	Unknown Compliance Redirect	AND	Network_Access_Authentication_Passed	× LIMITED ACCESS	Select from list	65	ò			
	Ŭ			Compliance_Unknown_Devices							
	0	NonCompliant_Devices_Redirect	AND	Network_Access_Authentication_Passed		Select from list		~			
	U			Non_Compliant_Devices	- LIMITED_HOCE35		3	*			
	0	Compliant Davison Assocs		Network_Access_Authentication_Passed		Salact from list		~			
	9	Compliant_Devices_Access	AND	Compliant_Devices	NOCEDD		30	*			

نأ رابتعالا يف عضت نأ بجي نكلو دنتسملا اذه نم اعزج سيل ةقداصملا جهن نيوكت ليوختلا جهن ةجلاعم عدب لبق ةحجان نوكت نأ بجي ةقداصملا.

ةحصلا نم ققحتلا

ةيسيئر تاوطخ ثالث نم قفدتلا نم يساسألا ققحتلا فلأتي دقو:

:FlexVPN لصو ةحول ىلع RA VPN لمع ةسلج نم ققحتايا .1 ةوطخلا

show crypto session username vpnuser 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 Interface: Virtual-Access1 Profile: FlexVPN-IKEv2-Profile-1 Uptime: 00:04:40 Session status: UP-ACTIVE Peer: 7.7.7.7 port 60644 fvrf: (none) ivrf: (none) Phase1_id: example.com Desc: (none) Session ID: 20 IKEv2 SA: local 5.5.5.5/4500 remote 7.7.7.7/60644 Active Capabilities:DNX connid:1 lifetime:23:55:20 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.30.107 Active SAs: 2, origin: crypto map Inbound: #pkts dec'ed 499 drop 0 life (KB/Sec) 4607933/3320 Outbound: #pkts enc'ed 185 drop 0 life (KB/Sec) 4607945/3320 show crypto ikev2 sa detail IPv4 Crypto IKEv2 SA Tunnel-id Local Remote fvrf/ivrf Status 1 5.5.5.5/4500 7.7.7.7/60644 none/none READY Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth verify: EAP Life/Active Time: 86400/393 sec CE id: 1010, Session-id: 8 Status Description: Negotiation done Local spi: 54EC006180B502D8 Remote spi: C3B92D79A86B0DF8 Local id: cn=flexvpn-hub.example.com Remote id: example.com Remote EAP id: vpnuser Local req msg id: 0 Remote req msg id: 19 Local next msg id: 0 Remote next msg id: 19 Local req queued: 0 Remote req queued: 19 Local window: 5 Remote window: 1 DPD configured for 60 seconds, retry 2 Fragmentation not configured. Dynamic Route Update: disabled Extended Authentication configured. NAT-T is detected outside Cisco Trust Security SGT is disabled

IPv6 Crypto IKEv2 SA

Initiator of SA : No

الجس) ةقداصملا قفدت نم ققحتلاً .2 ةوطخلا RADIUS (ةرشابملاً:

Assigned host addr: 10.20.30.107

	Time	Status	Details	Identity	Posture Status	Endpoint ID	Authentication P	Authorization Policy	Authorization Profiles	IP Address
×				Identity	Posture Status	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
3.	Jun 07, 2018 07:40:01.378 PM		ò		Compliant	7.7.7.7			UNLIMITED_ACCESS	
2.	Jun 07, 2018 07:39:59.345 PM	0	ò	vpnuser	Compliant	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	10.20.30.112
1.	Jun 07, 2018 07:39:22.414 PM	~	0	vpnuser	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

- فيرعت فلم نم ققحتلاب امتهم نوكت دق ،ةوطخلا هذهل ةبسنلاب .ةيلوألا ةقداصملا .1 ىجري ،عقوتم ريغ ليوخت فيرعت فلم قيبطت ةلاح يف .هقيبطت مت يذلا ليوختلا قوف رقنلاب ريرقتلا اذه حتف كنكمي .يليصفتلا ةقداصملا ريرقت نم ققحتلا ةقداصملا ريرقت يف تامسلا ةنراقم كنكمي ."ليصافت" دومع يف "جاجزلا ريبكت" .
- 2. نم لمعلا ةسلج ةلاح تريغت نيعملا لاثملا اذه يف ،لمعلا ةسلج تانايب رييغت NotApplicable يل Compliant.
- عفدل ةحجان هذه COA ةيلمع نوكت نأ بجي .ةكبشلا ىل لوصولا زاهج ىل 3. COA ةلاح يف .ISE بناج نم ةديدج ليوخت ةسايس نييعتو NAD بناج نم ةديدجلا ةقداصملا رثكأ نوكت نأ نكمي .ببسلا نم ققحتلل لصفم ريرقت حتف كنكمي ،COA لشف لااسراب ماق يذلا PSN نأ امإ قلاحلا هذه يف - COA قلهم :يه واكاكلل اعويش اياضقلا ناكم يف COA بلط طاقسا مت وأ .NAD بناج ىلع COA ليمعك هنيوكت متي مل بلطلا لبق نم همالتسا مت دق واكاكلا نأ ىل ريشي - واكاكلل بلاسل ماك مي ماك بلطا ريرق نام مال تسار مت واكاكلا اغري ما يا من يول الالالالا كان موال دام العام المال المال

ةدهاشم كنكمي ال ،لااثملاا اذه ىلع NAD مجومك IOS XE ىلإ دنتسملا مجوملا مادختسال ارظن لقنلاب عفدلا ةزيم مدختسي ISE نأل ارظن ثدحي اذهو .مدختسملل قحال ةقداصم بلط يأ اذه يفو .VPN ةمدخ ليغشت بنجي يذلا IOS XE ليغشتلا ماظنل COA ليغشتلا ماظنل ىل ةجاح كانه نوكت ال كلذل ،ةديدج ليوخت تاملعم ىلع مسفن COA يوتحي ،ويرانيسلا قداعإ

ا قوطخلا 3.Posture report verify - ىلإ لقتنا Operations -> Reports -> Reports -> Endpoint and Users -> Posture Assessment by Endpoint.

dentity Services Engine	Home	Context	Visibility	Operations	Policy Adm	inistration	\$	License Warning 🔺	९ ० ०
RADIUS Threat-Centric NAC Live	Logs	TACACS	Troubleshoot	Adaptive Network	vork Control Reg	ports			
▼ Reports	Post	ure Assessn	nent by End	lpoint 🕄				+ My Reports Z E	xport To 👻 🕓 Schedule
▶ Audit	From	2018-06-07 00:	:00:00.0 to 201	8-06-07 19:52:48.0					
Device Administration	Repo	rts exported in la	ast 7 days 0						
Diagnostics								Y Filter	 CRefresh T
✓ Endpoints and Users		Logged At		Status	Details	PRA Action	 Identity 	C Endpoint ID	IP Address
Authentication Summary	×	Today	* ×				Identity	Endpoint ID	
Client Provisioning		2018-06-07	19:39:59.345	~	Q	N/A	vpnuser	50:00:00:03:00:00	10.20.30.112
Current Active Sessions		2018-06-07	19:38:14.053	~	<u>o</u>	N/A	vpn	50:00:03:00:00	10.20.30.111
External Mobile Device M		2018-06-07	19:35:03.172	0	0	N/A	vpnuser	50:00:00:03:00:00	10.20.30.110
Manual Certificate Provisi		2018-06-07	19:29:38.761		Q	N/A	vpn	50:00:00:03:00:00	10.20.30.109
PassiveID		2018-06-07	19:26:52.657		ò	N/A	vpnuser	50:00:00:03:00:00	10.20.30.108
Posture Assessment by C		2018-06-07	19:17:17.906		l.o	N/A	vpnuser	50:00:00:03:00:00	10.20.30.107
Posture Assessment by E	4								+
Profiled Endpoints Summ								Rows/Page 6 v I d	6 Total Rows

فرعم نم لاثملا ليبس ىلع ققحتلل نيعم ثدح لكل انه نم لصفم ريرقت حتف كنكمي نم اهديدحت مت ةددحملا عضولا تابلطتم يأ ،ريرقتلا اذه هيلإ يمتني يذلا لمعلا ةسلج بلطتم لك ةلاح كلذكو ةياهنلا ةطقنل ISE لبق.

اهحالصإو ءاطخألا فاشكتسا

المحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمي تامولعم مسقلا اذه رفوي.

:ثبلاو لابقتسالا ةدحو نم عيمجتلل IKEv2 ءاطخأ حيحصت

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 internal
debug crypto ikev2 error
```

2. تامسلا نييعت ىلع عالطالل (AAA) ةبساحملاو ضيوفتلاو ةقداصملا ءاطخأ حيحصت ةديعبلا وأ/و ةيلحملا:

debug aaa authorization debug aaa authentication debug aaa accounting debug aaa coa debug radius authentication debug radius accounting

- 3. DART ليمع نم AnyConnect.
- 4. حيحصت يف هذه ISE تانوكم نيكمت بجي ،امحالصإو عضولا ةيلمع ءاطخأ فاشكتسال نوكملا - ISE نوكملا - client-webApp:عضولا ةيلمع ثدحت نأ نكمي ثيح - guest.log فدهلا لجسلا تافلم .ليكولا ريفوت نع لوؤسملا يتأي امدنع) ةسلجلا كلام نع ثحبلاو ليمعلا ديوزت لخدم نوكم نع لوؤسملا نوكملا نع لوؤسملا نوكملا - دادمإلI.guest.log فدهلا لجسلا فلم .(ئطاخ PSN يل عيمج - (ةيعضو) guest.log فدملا لجسلا فلم .ليمعلا ريفوت قساير العلا عيمج - (قيعضو) jse-post.log.Posture - فدملا لجسلا فلم .

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما