ةدحو AnyConnect و يلحم CA مداخك ASA نيوكت ثٻلاو لاابقتسالا

تايوتحملا

<u>قمدقملا</u> .

<u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>قي ساساً تامولعم</u> <u>نىوكتلا</u> <u>ةكېشلل يطيطختلا مسرلا</u> <u>ىلحم CA مداخك ASA</u> <u>ASA يالع ەنىيكەتو يالحمالا CA مداخ نىيوكت 1. قوطخالا</u> <u>ASA تانايب ةدعاق يالا مەتفاضاو نېمدختسم ءاش.نا .2 ةوطخلا</u> <u>WAN ةەجاو ىلع WebVPN نىكمت .3 ةوطخلا</u> <u>ليمعالا زامج يالع قدامشالا داريتسا 4 قوطخاا</u> AnyConnect عالمعل SSL متاويك ANYConnect ASDM AnyConnect نېوكت چلاعم <u>CLI ک AnyConnect</u> در <u>قحصابا نم ققحتايا</u> <u>امحالصاو ءاطخألا فاشكتسا</u> <u>ةلص تاذ تامولعم</u>

ەمدقملا

(CA) تاداهش عجرم مداخك Cisco نم (ASA) ئياهم نامأ زاهج دادعا ةيفيك دنتسملا اذه فصي .Cisco AnyConnect Secure Mobility ءالمعل (SSL) ةنمآلا ليصوتلا ذخآم ةقبط ةباوبكو

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- 9.1.x ةغيص ةيجمرب ضكري نأ ليكشت ASA يساسأ
 - ىلعأ وأ ASDM 7.3

ةمدختسملا تانوكملا

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

- (6) 6: ةغيص ةيجمرب ضكري نأ Cisco 5500 Series ASA
- Windows ل 4.x رادص إل Windows في الدص الما Windows في الما ك
- . <u>قفاوت ا ططخم</u> لكل موعدم ليغشت ماظن ليغشت موقي يذلا رتوي مكل زاهج
 - Cisco Adaptive Security Device Manager (ASDM)، رادصإلاا 7.3 •

<u>جمارب ليزنت</u> نم AnyConnect VPN (AnyConnect-win*.pkg) ليمع ةمزح ليزنت :ةظحالم ASA flash، ةركاذ ىلإ AnyConnect VPN ليمع خسنا .(طقف نيلجسملا <u>عالمعلل</u>) Cisco SSL VPN لاصتا ءاشنإل ةديعبلا مدختسملا رتويبمك ةزهجأ ىلإ اهليزنت بجي يتلاو ديزم ىلع لوصحلل ASA نيوكت ليلد نم <u>AnyConnect ليمع تيبثت</u> مسق عجار .ASA عم .تامولعملا نم

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

ةيساسأ تامولعم

:فئاظولا ەذە ةبساحملا بتكم يف تاداەشلا ةئيە رفوتو

- ASA يف ةيساسألا ةداهشلا عجرم ةيلمع جمدي
 - . تاداهشلا رشنب موقي
- . ةرداصلا تاداهشلل لاطبإلل نمآلا صحفلا رفوي
- ىلإ ةدنتسملا VPN SSL تالاصتإ عم مادختسالل ASA ىلع صيخرت عجرم رفوي (AnyConnect) ليمعلا ىلإ ةدنتسملا SSL تالاصتاو (WebVPN) ضرعتسملا
- صيخرت ىلع دامتعالا ىل قجاحلا نودب ،نيمدختسملل اهب قوثوم ةيمقر تاداهش رفوي
 يجراخلا تاداهشلا
- نع رشابمل مدختسمل لي جست رفويو ةداهشل ققداصمل قنم آقيل خاد قطلس رفوي بيول عقوم ىل لوخدل لي جست قيرط.

دويقلاو ةيەيجوتلا ئدابملا

- . فافشلاو هجوملا ةيامحلا رادج عضو يف موعدم
- ASA ىلع ةرم لك يف طقف دحاو يلحم CA مداخ ةماقإ نكمي
- لشفلا زواجت دادعإ يف يلحم CA مداخك ASA ةزيم معد متي ال
- .SHA1 تاداهش ءاشنإ الإ ،يلحم CA مداخك لمعي يذلاو ،ايلاح ASA معدي ال
- ضرعتسملا ىلا ةدنتسملا SSL VPN تالاصتال يلحملا CA مداخ مادختسإ نكمي IPSec. ل ايلاح موعدم ريغ .ليمعلاو
 - .يلحملا CA ل VPN لمح ةنزاوم معدي ال
- الإلمعي نأ نكمي الو .رخآ قدصم عجرم اعبات يلحملا قدصملا عجرملا نوكي نأ نكمي ال يرذجلا قدصملا عجرملا هفصوب
 - . ةيوەلا قداەشل يلحمل CA مداخ ىل ليجستلا ايلاح ASA ىلع رذعتي
- جوز ىلع يوتحي PKCS12 فلم نيزختب ASA موقي ،ةداەشلا ليجست لامتكا دنع تيابوليك 2 يلاوح بلطتي ام وهو ،تاداەشلا ةلسلسو مدختسملاب صاخلا حيتافملا ةحاسمل يلعفلا رادقملا دمتعي ليجست لكل صرقلا ىلع ةحاسم وأ شالفلا ةركاذ نم

يەيجوتلا أدبملا اذه عض .ةداەشلا لوقحو ەنيوكت مت يذلا RSA حاتفم مجح ىلع صرقلا عم ASA ىلع ةقلعملا ةداەشلا ليجست تايلمع نم ريبك ددع ةفاضإ دنع كينيع بصن ةركاذ يف اەنيزخت متي ەذە PKCS12 تافلم نأل ،ةحاتملا Flash ةركاذ نم دودحم رادقم .اەنيوكت مت يتلا ليجستلا دادرتسإ ةلەم ةدم لاوط شالفلا

نيوكتلا

.يلحم CA مداخك Cisco ASA نيوكت ةيفيك مسقلا اذه فصي

نم ديزم ىلع لوصحلل (طقف <mark>نيلجسمل</mark>ا ءالمعلل) <u>رماوألا ثحب ةاداً</u> مدختسأ :ةظحالم .مسقلا اذه يف ةمدختسملا رماوألا لوح تامولعملا

ةكبشلل يطيطختلا مسرلا



ASA Configured as a Local CA server and AnyConnect Headend

Client machine with AnyConnect

يلحم CA مداخك ASA

ASA ىلع ەنيكمتو يلحملا CA مداخ نيوكت .1 ةوطخلا

- عجرملا < تاداەشلا ةرادإ < (دعب نع لوصولا) Remote Access VPN < نيوكتلا ىلإ لقتنا قدصملا عجرملا مداخ نيكمت رايخ نم ققحت .CA مداخ < تاداەشلل يلحملا.
 - مدختست فورح ةعبس ،ىندأ ادح رورملا ةرابع نوكت نأ بجي .رورملا ةرابع نيوكتب مق موقت .حيتافملا جوزو ةيلحملا CA قداهش نمضتي يذلا PKCS12 فلم ظفحو زيمرتل
 .حيتافملا جوز وأ CA قداهش دقف ةلاح يف PKCS12 فيشرأ نيمأت ءاغلإب رورملا قرابع
 - كلذ ديدحت نكميو .رذجلا ةداهشل CN ك لقحلا اذه رهظيس .ردصملا مسا نيوكتب مق لم ،ةمظنملا (س) ،(قيميظنتلا قدحولا) OU ،(عئاشلا مسالا) CN :يلاتلا قيسنتلاب .(دلبلا) C و (قيالولا) S ،(قيلحملا ققطنملا).
 - نامضل ينورتكلإلا ديربلا مداخو SMTP مداخ تادادعإ نيوكتب مق :يرايتخالا نيوكتلا
 ليجستلا لامكإل ديربلا ربع نييئاهنلا ءالمعلل OTP لوكوتورب يقلت ةيناكمإ

.يلحملا SMTP/ينورتكلإلا ديربلا مداخل IP ناونع وأ فيضملا مسا نيوكت كنكمي مملتسيس يذلا ينورتكلإلا ديربلل عوضوملاو ناونعلا نم لقح نيوكت اضيأ كنكمي عوضوملاو admin@<ASA hostname>.nul وه "نم" ناونع نوكي ،يضارتفا لكشب .ءالمعلا .ةداهشلا ليجست ةوعد وه

مجحو ليمعلا حاتفم مجح لثم ةيرايتخالا تاملعملا نيوكت كنكمي :يرايتخالا نيوكتلا
 اضيأ ليمعلا قداهش رمعو CA قداهش رمعو CA مداخ حاتفم

Device List 🗗 🕂 🛠	Configuration > Remote Access VP	N > Certificate Management > Local Certificate Authority > CA Server
Add Delete Connect Ind: Go	Configure the Local Certificate Author	ty. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority.
(10.105.130.69:4443	Passphrase:	
	Confirm Passphrase:	•••••••• Specify the Passphrase
	Issuer Name:	CN=ASA.local Specify the CN which will show as Issuer name
	CA Server Key Size:	1024 - Specify the Server/Client key size to
	Client Key Size:	1024 - be used
	CA Certificate Lifetime:	1095 days
		O The CA certificate lifetime change will take effect after existing CA certs expire.
Remote Access VPN 🗗 🖗	Client Certificate Lifetime:	365 days
? Introduction	SMTP Server & Email Settings	
Clientless SSL VPN Access	Server Name/IP Address:	
🗄 📷 AAA/Local Users		
Host Scan Image	From Address:	admin@ciscoasa.null
Secure Desktop Manager	Subject:	Certificate Enrollment Invitation
Cartificates		
Identity Certificates	More Options	
Trusted Certificate Pool		
Local Certificate Authority		
CA Server		
Manage User Database		
······论编 manage user Certificates		

:(CLI) رماوألا رطس ةەجاو ئڧاكم

ASA(config)# crypto ca server ASA(config-ca-server)# issuer-name CN=ASA.local ASA(config-ca-server)# subject-name-default CN=ASA.local ASA(config-ca-server)# lifetime certificate 365 ASA(config-ca-server)# lifetime ca-certificate 1095 ASA(config-ca-server)# passphrase cisco123 ASA(config-ca-server)# no shutdown % Some server settings cannot be changed after CA certificate generation. Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete

.يلحملا CA مداخ نيوكت نمض اەنيوكت نكمي ةيفاضإ لوقح ەذەو

.ASA ىلع CRL عقوم وہ اذہ	URL ناونع
نكلو <u>http://hostname.domain/+CSCOCA+/asa_ca.crl</u> وه يضارتفالا عقوملا	ةطقنل
.URL ناونع ليدعت نكمي	CRL عيزوت

ئفنملا ەمجاولاو Publish-CRL	-publish ةەجاو رتخأ ،نينيعم ذفنمو ةەجاو ىلع HTTP ليزنتل CRL ريفوتل يأ نوكي نأ نكمي يذلاو ،ذفنملا مقر لخدأ مث .ةلدسنملا ةمئاقلا نم CRL .80 ءانېم TCP مقر عانېم ريض قتليا .165535 1 نم ذفنم مقر
CRL رمع	اهيف متي ةرم لك يف هتداعإو CRL ثيدحتب يلحملا قدصملا عجرملا موقي يف تارييغت ثدحت مل اذا نكلو ،اهلاطبا ءاغلإ وأ مدختسملا ةداهش لاطبا ةرتفلا يهو ،CRL ءاقب ةدم لك ةرم ايئاقلت CRL رادصا ةداعا متت ،لاطبالا .يلحملا CA نيوكت ءانثأ ةايحلا ىدم crl رمألا مادختساب اهددحت يتلا ةينمزلا يه ةيضارتفالا ةينمزلا ةرتفلا نإف ،CRL ءاقب ةدم ديدحتب مقت مل اذا .تاعاس تس
نيزخت عقوم ندعاق تانايبلا	مئاوقو ةرداصلا تاداەشلاو مدختسملا تامولعم ىلإ لوصولاب ASA موقي تانايبلا ةدعاق دجوت .ةيلحم CA تانايب ةدعاق مادختساب اەذيفنتو لاطبإلا متيل اەنيوكت نكمي وأ ،يضارتفا لكشب ةيلحملا Flash ةركاذ يف ەذە نم ەيلإ لوصولا ةيناكمإو ەليمحت متي يجراخ تافلم ماظن ىلع اەتيبثت ASA. لبق
	تاداهشلا يف مدختسم مسا قاحلإل (DN ةلسلس) ايضارتفا اعوضوم لخدأ :ةمئاقلا هذه يف اهب حومسملا DN تامس ريفوت متي .ةرداصلا
	(ةلئاعلا مسا) SN(عئاشلا مسالا) CN [.]
	(ةسسۇم⊔ا مسا) O
مسا	(ةيلحم) L.
عوضوملا يضارتفالا	(ةلودلا) C·
	(ةيميظنتلا ةدحولا) OU [.]
	(ينورتكلإلا ديربلا ناونع) EA·
	(ةعطاقملا/ةيالولا) ST [.]
	(ناونعLI) T·
	دادرتسإ اهلالخ مدختسملل نكمي يتلا تاعاسلاب ليجستلا تقو دح نييعت ASA. نم PKCS12 فلم
ەرتف پېچىرىتلا	.ةعاس 24 يه ةيضارتڧالا ةميقلا
	PKCS12 فلم مدختسملا عجرتسي نأ لبق ليجستلا ةرتف تەتنا اذإ :ﷺ لم ليجستلاب حمسي ال ،مدختسملا ةداەش نمضتي يذلا
ءاەتنا فيحالص فرم رورم ةملك فدحاو	ليجستل احلاص OTP هيف نوكي يذلا تاعاسلاب تقولا رادقم ددحي ليجستلاب مدختسملل حمسي امدنع ةينمزلا ةرتفلا هذه أدبت .مدختسملا .ةعاس 72 يه كيكفتلا ةميق

ريكذت لاسرا اهيف متي يتلا ةداهشلا ةيحالص ءاهتنا لبق مايألا ددع ديدحت تاداهشلا يكلام ىلإ ليجستلا ةداعإل يلوأ.

ASA تانايب ةدعاق ىلإ مەتڧاضإو نيمدختسم ءاشنإ .2 ةوطخلا

• Certificate < (دعب نع لوصولا) Remote Access VPN < (نيوكتلا) Configuration كلإ لقتنا < (يلحملا تاداەشلا عجرم) Local Certificate Authority < (تاداەشلا قرادإ) Management Add.

Device List c	57 F ×	Configuration > Remote A	ccess VPN > Certificate Mana	<u>ement</u> > <u>Local Certificate Authority</u> >	 Manage User Database 	L
🖗 Add 📋 Delete 🚿 Connect		Manage the users in the use	r database for Local Certificate Au	hority Server.		
nd: Go		Username	Ema	1	Subject Name	Add
······································						Edit
						Delete
						Allow Enrollment
						Email OTP
						View/Re-generate OTP
Remote Access VPN	87 P					
Introduction Network (Client) Access						
Clientless SSL VPN Access						
Host Scan Image						
Secure Desktop Manager Certificate Management						
- 2 CA Certificates						
2 Trusted Certificate Pool						
Local Certificate Authority						

مساو ينورتكلإلا ديربلا فرعمو مدختسملا مسا لثم مدختسملا ليصافت ددح
 . قروصلا هذه يف حضوم وه امك ،عوضوملا

\overline 🔤 Add User		×
Username:	user 1	
Email ID:	user 1@cisco.com	
Subject (DN String):	CN=user1,OU=TAC	Select
Allow enrollment		
	Add User Cancel Help	

- . ةداەشلل ليجستلاب كل حمسي ثيحب ليجستلاب حامسلان م قرقحتلان م دكأت
 - مدختسملانيوكت لامكإل مدختسم ةفاضإ قوف رقنا

:(CLI) رماوألا رطس ةەجاو ئڧاكم

ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com

 ليجستان قالح ضرع متي ،"مدختسمان تانايب قدعاق" ىل مدختسمان قفاض دعب ليجستان فب حومسمك

Configuration > Rem	ote Access VPN > Certificate Management > Loca	l Certificate Authority > Manag	e User Database		
Manage the users in t	he user database for Local Certificate Authority Server.				
Username	Email	Subject Name	Enrollment Status	Certificate Holder	Add
user1	user1@cisco.com	CN=user1,OU=TAC	allowed	yes	Edit
					Delete
					Allow Enrollment
					Email OTP
					View/Re-generate OTP

:مدختسملا ةلاح نم ققحتلل CLI

<#root>

ASA# show crypto ca server user-db

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status:

Allowed to Enroll

ةرمل رورم ةملك ريفوت نكمي ،مدختسمل تان ايب ةدعاق ىل مدختسمل قفاض دعب
 تنيرمأل هذه نم يأ مادختساب ليجستل لامك ل مدختسمل (OTP) قدحاول

متيل ينورتكلإلا ديربلا تادادعإو SMTP مداخ بلطتي) ةدحاولا ةرملا رورم ةملك لسرأ .(CA مداخ نيوكت نمض اەنيوكت

وأ

ءاشنإ ةداعإ/ضرع قوف رقنلاب مدختسملا عم ەتكراشمو ةرشابم OTP لوكوتورب ضرع .(OTP) ةعرفتملا ةرجشلا لوكوتورب نيوكت ةداعإل اضيأ اذه مادختسإ نكمي .OTP لوكوتورب

nfiguration > Remote Access VPI > Certificate Management > Local Certificate Authority > Manage User Database						
Manage the us	ers in the user database for	Local Certificate Authority Server	r.			
Username	Email	Subject Name	Enrollment Status	Certificate Holder		Add
user 1	user 1@gmail.com	CN=user1,OU=TAC	allowed	yes		Edit
						Delete
						Allow Enrollment
						Email OTP
						View/Re-generate OTP

:(CLI) رماوألا رطس ةەجاو ئڧاكم

WAN ةەجاو ىلع WebVPN نيكمت .3 ةوطخلا

• .ليجستال بالطل ءالمعلال ASA اليجستال بالطل عالمعال المعال المعال المعال المعال المعال المعال المعال المعال ال

!! Enable web-access on the "Internet" interface of the ASA ASA(config)# webvpn ASA(config-webvpn)#enable Internet

ليمعلا زاهج ىلع ةداەشلا داريتسإ .4 ةوطخلا

- ليجستال المكإل طابترال على لقتناو ضرعتسم حتفا ،ةليمعال لمعل قطحم علع.
- متي يتلا ةەجاولاب صاخلا IP وە طابترالا اذە يف مدختسملا IP/FQDN نوكي نأ بجي تنرتنإلا ةەجاو يە يتلاو ،ةوطخلا كلت يف اەيلع webVPN نيكمت.

	<#root>
	https://
	 >
-	IP/FQDN>/+CSCOCA+/enroll.html
	

<u>نع تدوز ناك يأ OTP لاو (a رايخ ،2 قوطخ تحت ASA لا على لكشي) username لا تلخد</u>
 <u>ايودي وأ ينورتكل ديرب قيرط</u>

ABA - Local Certificate Authority
ASA - Local Certificate Authority Username Username One-time Password Enter the User-Name and OTP provided Username Username
 Restart the SSL VPN connection . قرش ابم ASA نم قاق ل تم ل اليمع ل اقداهش تي بثت ل حتف عل ع رق نا ماليه على عنها ماليه مع المالية منها منها مع المالية منها منها منها منها منها منها منها منها
Do you want to open or save this file? Name: user1.p12
Type: Personal Information Exchange From: 10.105.130.214
Open Save Cancel Open Save While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or

Certificate Import Wizard



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

< Back	Next >	Cancel

<u>يلاتا رقناو يضارتفاك راسملا كرتاً</u>

Certificate Import Wizard
File to Import
Specify the file you want to import.
File name: s\Temporary Internet Files\Content.IE5\SQT1AUGH\user1[1].p12 Browse
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< Back Next > Cancel

- <u>.لاجم ةملكلا يف OTP لا تلخد</u>
- <u>نكمي متح حاتفملا اذه ملع رمدصتلل لباق ةمالع عضول رامخلا دمدحت كنكمي</u> رمال بلطت اذا لبقتسمل مف لمعل اقطحم نم حاتفملا رمدصت
 - <u>يلاتا قوف رقنا</u>

Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

- <u>رجتملا راتختل اەكرت وأ نيعم تاداەش نزخم يف ايودي ةداەشلا تيبثت كنكمي</u> <u>.ايئاقلت</u>
 - <u>.(يُلاتَل</u>ا) Next قوف رقنا

Certificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store: Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel

• <u>.تيبثتاا تمتأ in order to زاجنا ققطقط</u>

Certificate Import Wizard



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected Content	Automatically determined by t PFX
File Name	C: \Users \mrsethi \AppData \Lo
•	- F
< Back	Finish Cancel

х



- <u>اەتحص نم ققحتاا كنكمي ،حاجنب قداەشاا تىبثت درجمب</u>
 - <u>.تنرتنإلا تارايخ < تاودأ يل لقتناو E حتفا</u>



. <u>قروص ا مذه يف حض وم وه امك ،تاداه أ قوف رقن او يوتحم بيوبت ا قمال عن ا لقتنا</u>

Internet Options
General Security Privacy Content Connections Programs Advanced
Parental Controls Control the Internet content that can Parental Controls be viewed.
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.
Certificates Use certificates for encrypted connections and identification.
Clear SSL state Certificates Publishers
AutoComplete
AutoComplete stores previous entries Settings on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
OK Cancel Apply

• ASA. لا نم اممالتسا مت قدامشلا عرت نأ كنكمي ،يصخشلا رجتملا تحت

Certificates			×
Intended purpose:	<all></all>		
Personal Other Peop	e Intermediate Certification	Authorities Tru	sted Root Certification
Issued To	Issued By	Expiratio	Friendly Name
Juser 1	asa.local	1/8/2017	ou=TAC,cn=user1
Import Exp Certificate intended pu	ort Remove		Advanced
Learn more about <u>certif</u>	icates		Close

AnyConnect ءالمعل SSL مالمعل

ASDM AnyConnect نيوكت جلاعم

AnyConnect Secure Mobility Client. نيوكتل AnyConnect/CLI نيوكت جلاعم مادختسإ نكمي لبق ASA ةيامح رادج صرق/ةتقؤملا ةركاذلا ىلإ AnyConnect ليمع ةمزح ليمحت نم دكأت .ةعباتملا

نيوكتلا جلاعم ربع AnyConnect Secure Mobility Client نيوكتل تاوطخلا هذه لمكأ:

يل الوخدلا ليجستب مق AnyConnect VPN1. جلاعم كل القتناو ASDM كل الوخدلا ليجستب مق يلاتال قوف رقناو نيوكتال جلاعم ءدبال.

🔄 AnyConnect VPN Connecti	on Setup Wizard	23
AnyConnect VPN Connection	Introduction Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the user's device when a VPN connection is established. VPN Remote Access	end
[< Back Next > Cancel He	elp

ةمئاقلا نم اهيلع VPN ءاهنإ متيس يتلا ةهجاولا رتخاو ،لاصتالا فيرعت فلم مسا لخدأ .2 .يلاتلا قوف رقناو ،VPN ةكبش ىلإ لوصولا ةهجاول ةلدسنملا

anyConnect VPN Connect	tion Setup Wizard	
Steps	Connection Profile Identification	
1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN	
2. Connection Profile	connections.	
Identification	Connection Profile Name: SSL_GRP	
3. VPN Protocols		
4. Client Images	VPN Access Interface: Internet	
Authentication Methods		
Client Address Assignme		
 Network Name Resolutio Servers 		
8. NAT Exempt		
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel Help	

ةداهش نوكت نأ نكمي .(SSL) ةنمآلا ليصوتلا ذخآم ةقبط نيكمتل SSL رايتخالا ةناخ ددح .3 ةداهش وأ ،(Entrust وأ Verisign لثم) اهب قوثوم ةيجراخ ةهج نع ةرداص ةداهش نع قرابع زاهجلا ةمئاقلا لالخ نم اهرايتخا نكميف ،ASA ىلع لعفلاب ةتبثم ةداهشلا تناك اذإ .أيتاذ ةعقوم 1 لبق نم اهميدقت متيس يتلا مداخلا بناج نم ةداهشلا يه ةداهشلا هذه :ةظحالم. بجي امم ASA ىلع ايلاح ةتبثم مداخ تاداهش كانه نكت مل اذا .SSL ءالمع ىلإ ASA ةرادإ ىلع كلذ دعب رقناف ،ايتاذ ةعقوم ةداهش ءاشنإ.

<u>تيبثت Cisco ASA 8.x</u> دنتسم يف ةحضوملا تاوطخلا لمكأ ،ةيجراخ ةمج ةدامش تيبثتل .WebVPN <u>نيوكت جذومن عم مادختسال أيودي ةيجراخ ةمج نم نيعئاب تادامش</u>

- .زاهجلا ةداهشو VPN تالوكوتورب نيكمتب مق
 - .(يلاتلا) Next قوف رقنا

AnyConnect VPN Connect	tion Setup Wizard
Steps	VPN Protocols
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support. SSL IPSec Device Certificate Device Certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA. Device Certificate:None Manage
	< Back Next > Cancel Help

نم وأ يلحملا صارقألاا كرحم نم AnyConnect (.pkg file) ليمع ةمزح ةفاضإل ةفاضإ قوف رقنا .4 .ASA ب ةصاخلاا Flash/disk ةركاذ

Flash صارقأ كرحم نم ةروصلا ةفاضإل (ةتقؤملا ةركاذلا) Flash ةركاذ ضارعتسإ قوف رقنا زاهجلل يلحملا صارقألا كرحم نم ةروصلا ةفاضإل ليمحت قوف رقنا وأ ،(ةتقؤملا ةركاذلا) .فيضملا

The AnyConnect VPN Connect	ion Setup Wizard	X	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.		
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.		
3. VPN Protocols			
4. Client Images			
5. Authentication Methods	Add Replace Delete 🕈 🕹		
6. Client Address Assignme	Image	Regular expression to match user-agent	
7. Network Name Resolutio Servers			
8. NAT Exempt			
9. AnyConnect Client Deployment			
10. Summary			
	You can download ApyConnect Client packages for	m Giere by contribut 'Any-Connect VON Giere' or click here	
Tou can download AnyConnect Client packages from <u>Cisco</u> by searching AnyConnect VPN Client or <u>dick here</u> .			
	< Back Next >	Cancel Help	
L			

- ةدوجوم ةمزحلا تناك اذإ) ASA Flash/Disk قركاذ نم امإ AnyConnect.pkg فلم ليمحت كنكمي .يلحملا صارقألا كرحم نم وأ (لعفلاب
- . صَارَقُأْلِا/ةَتقَوْمِلِا ASA ةركاذ نمّ AnyConnect ةمزح ديدحتل ةتقَوْمِلا ةركاذلا ضارعتسا
 - . فيضمل زاهج ل يلحمل كرحمل نم AnyConnect ةمزح ديد حتل ليم حتل .
 - .OK قوف رقناو

Add AnyConnect	Client Image	22
AnyConnect Image:	disk0:/anyconnect-win-4.2.00096-k9.pkg	Browse Flash
		Upload
Regular expression	to match user-agent	*
	OK Cancel Help	

• .(يلاتلا) Next قوف رقنا

AnyConnect VPN Connect	ion Setup Wizard	×	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the dient device when it accesses the enterprise network.		
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image.		
3. VPN Protocols	the top of the list.		
4. Client Images			
5. Authentication Methods	🗣 Add 🏼 Replace 🛄 Delete 🛧 🔸		
6. Client Address Assignme	Image	Regular expression to match user-agent	
 Network Name Resolutio Servers 	disk0:/anyconnect-win-4.2.00096-k9.pkg		
8. NAT Exempt			
9. AnyConnect Client Deployment			
10. Summary			
	You can download AnyConnect Client packages from <u>Cisco</u> by searching	'AnyConnect VPN Client' or <u>click here</u> ,	
< Back Next > Cancel Help			

ةبساحملاو ضيوفتلاو ةقداصملا مداوخ تاعومجم ربع مدختسملا ةقداصم لامكإ نكمي .5 مق الإو .يلاتل قوف رقناو يلحم رتخأف ،لعفلاب نيمدختسملا نيوكت مت اذإ .(AAA) .يلاتلا قوف رقناو ةيلحملا مدختسملا تانايب ةدعاق ىلإ مدختسم ةفاضإب

مادختسا متيس ەنأ ينعي امم ،ةيلحملا ةقداصملا نيوكت متي ،لاثملا اذه يف :ةظحالم .ةقداصملل ASA ىلع يلحملا مدختسملا تانايب ةدعاق

AnyConnect VPN Connect	ion Setup Wizard	23
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods	Authentication Methods This step lets you specify the location of the authentication server. You can dick on the "New" button to create a new server group. AAA Server Group: LOCAL New Local User Database Details cisco	
 Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	User to be Added Username: user1 Add >> Password: ••••• Delete Confirm Password: •••••	
	< Back Next > Cancel He	elp

مقف ،لعفلاب IP عمجت نيوكت مت اذإ .VPN ءالمعل نيوانعلا عمجت نيوكت نم دكأت .6 .نيوكتلل ديدج قوف رقناف ،ةحاسم كانه نكت مل اذإو .ةلدسنملا ةمئاقلا نم هديدحتب .كلذ دعب ،متي نإ ام تقطقط

AnyConnect VPN Connect	tion Setup Wizard
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool:
	< Back Next > Cancel Help

Carl Add IPv4 Pool		
Name:	VPN_Pool	
Starting IP Address:	10.10.10.1	
Ending IP Address:	10.10.200	
Subnet Mask:	255.255.2 ▼	
ОК	Cancel Help	

• .(يلاتلا) Next قوف رقنا

DNS يلقح يف DN تاكبشو (DNS) لاجملا مسا ماظن مداوخ نيوكتب مق ،يرايتخإ لكشب .7 .يلاتلا قوف رقنا مث ،لاجملا مساو

anyConnect VPN Connec	tion Setup Wizard	
Steps	Network Name Resolution Servers	
1. Introduction	This step lets you specify how domain names are resolved for the remote user when accessing the internal network.	
2. Connection Profile Identification	DNS Servers:	
3. VPN Protocols	WINS Servers:	
4. Client Images	Domain Name:	
5. Authentication Methods		
6. Client Address Assignme		
7. Network Name Resolution Servers		
8. NAT Exempt		
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel Help)

ةيلخادلا ةيعرفلا ةكبشلاو ليمعلا نيب تانايبلا رورم ةكرح ءانثتسإ بجي هنأ نم دكأت .8 ناونع ةكبش نم رورم ةكرح يفعم VPN لا تنكم .ةيكيمانيد (NAT) ةكبش ناونع ةمجرت يأ نم ةكبشلا ددح ،اضيأ .ءافعإلل تلمعتسا نوكي نأ نراق LAN لا لكشيو قيقدت ةمجرت .يلاتلا قوف رقناو اهؤافعإ بجي يتلا ةيلحملا

Connect VPN Connect	a AnyConnect VPN Connection Setup Wizard						
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols	NAT Exempt If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. Image: Second S						
 Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	Inside Interface: Inside Local Network is the network address(es) of the internal network that client can access. Local Network: 192.168.10.0/24 The traffic between AnyConnect client and internal network will be exempt from network address translation.						
	< Back Next > Cancel Help	,					

.يلاتال قوف رقنا .9

anyConnect VPN Connect	tion Setup Wizard	23
Steps	AnyConnect Client Deployment	
1. Introduction	AnyConnect client program can be installed to a client device by one of the following two methods:	
2. Connection Profile Identification	 Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed Pre-deployment - Manually install the AnyConnect client package. 	;
3. VPN Protocols		
4. Client Images		
5. Authentication Methods		
6. Client Address Assignme		
7. Network Name Resolutio Servers		
8. NAT Exempt		
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel He	lp

دادعإلا لامكإل ءاهنإ قوف رقنا ،صخلملا ةريخألا ةوطخلا ضرعت .10.

a AnyConnect VPN Connection Setup Wizard					
VPN Wizard	Summary				
Branch	Here is the summary of the configuration.				
TEN T	Name	Value			
T ISP	Summary				
TORU	Name/Alias of the Connection Profile	SSL_GRP			
Home	VPN Access Interface	Internet			
otato	Device Digital Certificate	none			
Network	VPN Protocols Enabled	SSL only			
	AnyConnect Client Images	1 package			
GLADA IS	Authentication Server Group	LOCAL			
	Address Pool for the Client	10.10.10.1 - 10.10.10.200			
	DNS	Server: Domain Name:			
	Network Address Translation	The protected traffic is not subjected to network address translation			
	< Back Finish	Cancel Help			

،نيوكتلا جلاعم ربع AnyConnect نيوكت دنع ،كلذ عمو .نآلا AnyConnect ليمع نيوكت لمتكا لكشب (AAA) ةبساحملاو ضيوفتلاو ةقداصملاك ةقداصملا بولسأ نيوكتب موقي هنإف نيوكت بجي ،رورملا ةملك/مدختسملا مساو تاداهشلا ربع ءالمعلا ةقداصمل .يضارتفا .ةقداصملل ةقيرطك AAA و تاداهشلا مادختسال (لاصتالا فيرعت فلم) قفنلا ةعومجم

- ةكبشلا ىلإ لوصولا < (دعب نع لوصولا) Remote Access VPN < نيوكتلا ىلإ لقتنا AnyConnect. ليصوت تافيصوت < (ليمعلا)
 - جردملا SSL_GRP ديدجلا فاضملا لاصتالا فيرعت فلم يرت نأ بجي

Device List 🗇 🕀 🗡	Configuration >	Remote Access VP	N > Network (Client	Access > AnyConne	ect Connection Profiles				
Add 📋 Delete 🖋 Connect	The security app tunnel with Data	liance automatically de gram Transport Layer	ploys the Cisco AnyCo Security (DTLS) tunnel	nnect VPN Client to rem ing options.	note users upon connection. Th	e initial client deployment	t requires end-user administrative right	s. The Cisco AnyConnect VPN Client supports I	/Psec (IKEv2) tunnel as well as SSL
Remote Access VPN Introduction G AnyCorrect Contraction Profile G AnyCorrect Contraction Profile G AnyCorrect Contraction Profile G AnyCorrect Contraction Profile G AnyCorrect Clent Software G AnyCorrect G AnyCorrect Clent Software G AnyCorrect G AnyCorrec	Access Interfaces Image: Class State Class State Interface Interface Internet Outside Image: State State Internet Outside State Internet Outside State Image: State State Image: State State State	AnyConnect VPN Clier be enabled if you allow SSL Access Allow Access I I I I I I I I I I I I I I I I I I I	nt access on the interfa w AnyConnect client to Enable DTLS UP Sound VPN sessions policy always apply to	the traffic.	le below wser (Web Launch) . Enable Client Services	Device Cer	tificate		
Group Policies Group Reserve Connection Profiles Group Secure Mobility Solution Group Address Assignment	Image: Way with the select connection profile on the login page. Image: Shutdown portal login page.								
- 평, Advanced Advanced AnyConnect Essentials - 평, AnyConnect Custom Attributes 단 문 Endpoint Security 관 - 탁 IPsec	Connection prof	ile (tunnel group) spec dit <u> Delete</u> Find	ifies how user is authe	nticated and other para	meters. You can configure the Case	mapping from certificate	to connection profile <u>here</u> ,		
ACL Manager	Name		SSL Enabled	IPs	ec Enabled	Aliases	Authenticatio	on Method Group	p Policy
Connection Profiles	DefaultRAGroup DefaultWEBVPN	Group			 ✓ 		AAA(LOCAL) AAA(LOCAL)	DfitGr	pPolicy rpPolicy
Portal VDL Access	ssl-grp					ssl-grp	AAA(LOCAL)	DfitGr	pPolicy
0	SSL_GRP		V			SSL_GRP	AAA(LOCAL)	Group	Policy_SSL_GRP

- . ريرجت قوف رقناو SSL_GRP لاصتالا فيرعت فلم ددح ،ةداهشلا ققداصمو AAA ديدجتل
 - .الك ددح ،ةقداصملا بولسأ تحت

	Edit AnyConnect Connection Profile: SSL_GRP						
Γ	: <mark>Basic</mark>	Name:	SSL GRP				
	⊕ - Advanced	Aliases:	SSL GRP				
L		A . Ih an Kan Kan					
L		Method:					
L		AAA Server Crever					
L		AAA Server Group:	EUCAL V	Manage			
L			Use LOCAL if Server Group fails				
		Client Address Assignment –					
L		DHCP Servers:					
L			None O DHCP Link O DHCP Subnet				
		Client Address Pools:	VPN_Pool	Select			
		Client IPv6 Address Pools:		Select			
L		Default Group Policy					
L		Group Policy:	GroupPolicy_SSL_GRP	Manage			
		(Following field is an attribu	ute of the group policy selected above.)				
		Enable SSL VPN dien	t protocol				
		Enable IPsec(IKEv2)	client protocol				
		DNS Servers:					
		WINS Servers:					
L		Domain Name:					
L							
L							
L							
L							
	Find:	Ne	xt 🔘 Previous				
L		OK	Cancel Help				

AnyConnect ل CLI نيوكت

<#root>

!! *****Configure the VPN Pool*****
ip local pool VPN_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0
!! *****Configure Address Objects for VPN Pool and Local Network*****
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0

```
object network NETWORK_OBJ_192.168.10.0_24
                             subnet 192.168.10.0 255.255.255.0
                                                           exit
                                 !! *****Configure WebVPN*****
                                                        webvpn
                                               enable Internet
    anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
                                             anyconnect enable
                                      tunnel-group-list enable
                                                          exit
                                   !! *****Configure User*****
username user1 password mb02jYs13AX1IAGa encrypted privilege 2
                           !! *****Configure Group-Policy*****
                     group-policy GroupPolicy_SSL_GRP internal
                   group-policy GroupPolicy_SSL_GRP attributes
                                vpn-tunnel-protocol ssl-client
                                               dns-server none
                                              wins-server none
                                           default-domain none
                                                           exit
                           !! *****Configure Tunnel-Group*****
                       tunnel-group SSL_GRP type remote-access
                       tunnel-group SSL_GRP general-attributes
                             authentication-server-group LOCAL
                      default-group-policy GroupPolicy_SSL_GRP
                                        address-pool VPN_Pool
                        tunnel-group SSL_GRP webvpn-attributes
                                authentication aaa certificate
                                    group-alias SSL_GRP enable
                                                          exit
                      !! *****Configure NAT-Exempt Policy*****
```

nat (Inside, Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24 destinati

ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

مدختسا .show رماوأ ضعب (طقف <u>نول جسملا ءالمعلا) چارخالا مجرتم ةادأ معدت</u> :ةظحالم .show رمألا جَرخُمل ليلحت ضرعل "جارخإلا مجرتم ةادأ"

.CA مداخ نيكمت نم دكأت

show crypto ca server

<#root>

ASA(config)# show crypto ca server Certificate Server LOCAL-CA-SERVER:

Status: enabled

State: enabled Server's configuration is locked (enter "shutdown" to unlock it)

Issuer name: CN=ASA.local

CA certificate fingerprint/thumbprint: (MD5) 32e868b9 351a1b07 4b59cce5 704d6615 CA certificate fingerprint/thumbprint: (SHA1) 6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d Last certificate issued serial number: 0x1 CA certificate expiration timer: 19:25:42 UTC Jan 8 2019 CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016 Current primary storage dir: flash:/LOCAL-CA-SERVER/

> Auto-Rollover configured, overlap period 30 days Autorollover timer: 19:25:42 UTC Dec 9 2018

WARNING: Configuration has been modified and needs to be saved!!

ةفاضإ دعب ليجستلاب مدختسملل حامسلا نم دكأت:

<#root>

*****Before Enrollment****

ASA#

show crypto ca server user-db

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll

>>> Shows the status "Allowed to Enroll"

```
*****After Enrollment****
```

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:05:14 UTC Thu Jan 14 2016 notified: 1 times

enrollment status: Enrolled

, Certificate valid until 19:18:30 UTC Tue Jan 10 2017, Renewal: Allowed

.ASDM وأ CLI ربع امإ AnyConnect لاصتا ليصافت نم ققحتاا كنكمي

Via CLI

show vpn-sessionDB detail AnyConnect

<#root>

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : user1 Index : 1 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Essentials : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Encryption Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 13822 Bytes Rx : 13299 : 10 Pkts Tx Pkts Rx : 137 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_SSL_GRP Tunnel Group : SSL_GRP Login Time : 19:19:10 UTC Mon Jan 11 2016 Duration : 0h:00m:47s Inactivity : 0h:00m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 1.1 Public IP : 10.142.189.181 Encryption : none Hashing : none TCP Src Port : 52442 TCP Dst Port : 443 : Certificate and userPassword Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Client Ver Bytes Tx : 6911 Bytes Rx : 768 Pkts Tx : 5 Pkts Rx : 1

Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 1.2 : 10.142.189.181 Assigned IP : 10.10.10.1 Public IP Hashing : SHA1 Encryption : RC4 Encapsulation: TLSv1.0 TCP Src Port : 52443 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 : 6911 Bytes Tx Bytes Rx : 152 Pkts Tx : 5 Pkts Rx : 2 Pkts Rx Drop : 0 Pkts Tx Drop : 0 DTLS-Tunnel: Tunnel ID : 1.3 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Encryption : AES128 Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 59167 UDP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Bytes Tx : 0 Bytes Rx : 12907 Pkts Tx : 0 Pkts Rx : 142 Pkts Tx Drop : 0 Pkts Rx Drop : 0 NAC: Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds SQ Int (T) : 0 Seconds EoU Age(T) : 51 Seconds Hold Left (T): 0 Seconds Posture Token: Redirect URL :

ASDM ربع

- .لمعلا تاسلج < VPN تايئاصحإ < VPN < ةبقارم ىلإ لقتنا
 - لماكلاب دعب نع لوصولا ةطساوب ةيفصتلا لماع رتخاً
 - . ددحملا AnyConnect ليمعل نئارجإلا نم يأ ذيفنت كنكمي.

لمعلا ةسلج لوح تامولعملا نم ديزم ريفوت -ليصافتلا

ثبلاو لابقتسالا ةدحو نم ايودي مدختسملا جورخ ليجستل -جورخلا ليجست

ثبلاو لابقتسالا ةدحو نم AnyConnect ليمع لاصتا رابتخال - لاصتالا رابتخإ

Filter By: All Remote A	ccess 🗸 🗸	All Sessions	• Filt	ter	
Username	Group Policy	Public IP Address	Protocol	Login Time	Bytes Tx
	Connection Profile	Assigned IP Address	Encryption	Duration	Bytes Rx
user 1	ssl-pol	10, 142, 189,80	AnyConnect-Parent SSL-Tunnel DTLS	14:39:08 UTC Mo	10998
	ssl-grp	192, 168, 1, 1	AnyConnect-Parent: (1)none SSL-Tu	0h:00m:33s	885

اهحالصإو ءاطخألا فاشكتسا

.اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمي تامولعم مسقلا اذه رفوي

.debug رماوأ مادختسإ لبق <u>حيحصتا رماوأ لوح قمهم تامولعم</u> ىلإ عجرا :ةظحالم

مادختسا متي ؛ةفلتخم ءاطخأ حيحصت تايوتسم نييعت كنكمي ،ASA ىلع :ەيبنت ةجرد ديازتت دقف ،ءاطخألا حيحصت ىوتسم رييغتب تمق اذإ .اًيضارتفا لوألا ىوتسملا .جاتنإلا تائيب يف ًةصاخو ،رذحب كلذب مق .ءاطخألا حيحصت عسوت

- debug crypto ca ·
- debug crypto ca مداخ
- debug crypto ca messages •
- crypto ca تاكرح ءاطخأ حيحصت
 - debug webVPN AnyConnect •

.no shutdown رمألا مادختساب CA مداخ نيكمت متي امدنع اذه ءاطخألاا حيحصت جارخإ رهظي

<#root>

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255 CRYPTO_CS: input signal enqueued: no shut >>>> Command issued to Enable the CA server Crypto CS thread wakes up! CRYPTO_CS: enter FSM: input state disabled, input signal no shut CRYPTO_CS: starting enabling checks CRYPTO_CS: found existing serial file. CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019 CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: DB version 1 CRYPTO_CS: last issued serial number is 0x4 CRYPTO_CS: closed ser file CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists. CRYPTO_CS: Read 220 bytes from crl file. CRYPTO_CS: closed crl file CRYPTO_PKI: Storage context locked by thread Crypto CA Server CRYPTO_PKI: inserting CRL CRYPTO_PKI: set CRL update timer with delay: 20250 CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016 CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016 CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016 CRYPTO_PKI: CRL cache delay being set to: 20250000 CRYPTO_PKI: Storage context released by thread Crypto CA Server

CRYPTO_CS: Inserted Local CA CRL into cache!

CRYPTO_CS: shadow not configured; look for shadow cert CRYPTO_CS: failed to find shadow cert in the db CRYPTO_CS: set shadow generation timer CRYPTO_CS: shadow generation timer has been set CRYPTO_CS: Enabled CS. CRYPTO_CS: exit FSM: new state enabled CRYPTO_CS: cs config has been locked.

Crypto CS thread sleeps!

ليمعلا ليجست اذه ءاطخألا حيحصت جارخإ رهظي

<#root>

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255

CRYPTO_CS: writing serial number 0x2. CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: Writing 32 bytes to ser file CRYPTO_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

:طورشلا هذه بجومب ليمعلا ليجست لشفي دق

لوألا ويرانيسلا.

ليجستال نذإ نودب CA مداخ تانايب ةدعاق يف مدختسمال ءاشنإ متي

亏 Add User		— X
Username:	user 1	
Email ID:	user 1@cisco.com	
Subject (DN String):	Select	
Allow enrollment		
	Add User Cancel Help	

:(CLI) رماوألا رطس ةەجاو ئڧاكم

<#root>

ASA(config)# show crypto ca server user-db

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: <not allowed> notified: 0 times

enrollment status: Not Allowed to Enroll

قلواحم موقت ،ليجستلاب هل حومسم ريغ مدختسملا اهيف نوكي يتلا قلاحلا يف
 .هذه أطخلا قلاسر ءاشنإب مدختسملل OTP علا ينورتكلا ديرب لاسرا/ءاشنا

Error	X	
	OTP exists only if the user is allowed to enroll. Please ensure that the selected user is allowed to enroll.	
	ОК	

- .2 ويرانيسلا
- show run رمألا مادختساب ليجستلا لخدم اهيلع رفوتي يتلا قهجاولاو ذفنملا نم ققحت هليدعت نكمي نكلو 443 وه يضارتفالا ذفنملا.
 - قەجاولاب صاخلا IP ناونع ىل قەكبشلا ىل لوصولا قىناكم ۋى دىل لىم على نا نم دى أت لخدم ىل حاجنب لوصول مدختسملا دفنمل ىل اوى والا webVPN نىكمت متى يتلا
 لىجستل

:تالاحلا هذه يف ASA ليجست لخدم ىلإ لوصولا يف ليمعلا لشفي دق

- ASA1. ب صاخلا IP webVPN ىلإ ليمعلا نم ةدراولا تالاصتالا رظحب طيسو زاهج يأ ماق اذإ ددحملا ذفنملا ىلع
 - .2.اەيلع WebVPN نيكمت متي يتلا ةەجاولا ةلاح فاقيإ مت
 - ىلع تنرتنإلا ةەجاوب صاخل IP ناونع ىلع حاتم ليجستل لخدم نأ جارخإلا اذه حضوي 4433.
 4433.

<#root>

ASA(config)# show run webvpn

```
enable Internet
```

```
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

```
.3 ويرانيسلا
```

- ل (ةتقۇملا ةركاذلا) Flash قركاذ وه CA Server Database Storage ل يضارتڧالا عضوملا ASA.
- عانثأ مدختسملل هظفحو PKCS12 فلم ءاشنإل ةرح قحاسم اهب Flash قركاذ نأ نم دكأت ليجستلا
- ، (ةتُوَوْملا ةركاذلا) Flash قركاذل ةيفاك قرح قحاسم اهيف رفوتت ال يتلا قلاحلا يف عاطخألا حيحصت تالجس ءاشنإب موقيو ليمعلا ليجست ةيلمع لامكإ يف ASA لشفي :هذه

<#root>

ASA(config)# debug crypto ca 255 ASA(config)# debug crypto ca server 255 ASA(config)# debug crypto ca message 255 ASA(config)# debug crypto ca transaction 255 ASA(config)# debug crypto ca trustpool 255

CRYPTO_CS: writing serial number 0x2. CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: Writing 32 bytes to ser file CRYPTO_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

- CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.
 - CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.
 - CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1

ةلص تاذ تامولعم

- Cisco ASA 5500 Series Adaptive Security Appliances
- <u>ةعئاش لا تالكش ملا المحال صاو AnyConnect VPN Client لى مع عاطخاً فاش كتس الى لد</u>
 - <u>امحالصاو امئاطخاً فاشكتساو امتبقارمو AnyConnect لمع تاسلج ةرادا</u>
 - <u>Cisco Systems تادنتسملاو ينقتلا معدلا</u>

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