ةقداصملا مادختساب نمآلا SSL ليمع نيوكت FTD ىلع ةيلحملا

تايوتحملا

قمدق مالیا تعالیا لی تعالیا لی تعالیا لی تعالیا لی تعالیا لی تعالیا تعالیا لی تعالیا تعالیا تعالیا تعالیا تعالی تعالیا تعانیول مللا تعانیول مللا تعانیول مللا تعانیول مللا تعانیول مللا تعالیول معالیا تعانیول مللا تعالیول معال می مخت معالیا معالی معالی معالی معالی معالی معالی معالیا معالیا معالیا معالیا معالیا معالیا معالیا معالیا معالی معالیا م معالیا معا

ةمدقملا

مادختساب (AnyConnect نمضتي) نمآلا Cisco ليمع نيوكت ةيفيك دنتسملا اذه فصي دامساوب اهترادإ متت يتلا Cisco FTD يلع ةيلحملا ةقداصملا ا

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ترادإ زكرم لالخ نم نمآلا SSL اليمع نيوكت FirePOWER (FMC)
- FMC لالخ نم Firepower تانئاك نيوكت •
- Firepower ىلع SSL تاداەش •

ةمدختسملا تانوكملا

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

- Cisco Firepower Threat Defense (FTD)، رادصإلاا 7.0.0 (Build 94)
- Cisco FMC، رادصإلا 7.0.0 (Build 94)
- Cisco Secure Mobility Client 4.10.01075

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 رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

ةصاخلا ةكبشلا ءاشنإل (SSL) ةنمآلا ليصوتلا ذخآم ةقبط مادختسإ متي ،لاثملا اذه يف ليمعو FTD نيب (VPN) قيرهاظلا Windows 10.

ة يلحملا ةقداصملا FMC ةطساوب هترادا متت يذلا FTD لوكوتورب معدي ،7.0.0 رادصإلا نم ةيطايتحا ةقيرطك وأ ةيساسأ ةقداصم ةقيرطك اذه فيرعت نكميو .نينمآلا Cisco ءالمعل ةيلحملا ةقداصملا نيوكت متي ،لاثملا اذه يف .ةيساسألا ةقيرطلا لشف ةلاح يف ةيلحملا م

طقف احاتم FTD ىلع Cisco Secure Client Local Authentication اذه جمانربلا رادصإ نوكي نأ لبق ىلع Cisco Firepower Device Manager (FDM).

نيوكتلا

تانيوكتلا

صيخرتلا نم ققحتلا .1 ةوطخلا

صيخرتلا لخدم عم ةقڧاوتم نوكت نأو FMC ليجست بجي ،Cisco Secure Client نيوكت لبق وأ APEX وأ PLUS صيخرت FTD ل نكي مل اذإ Cisco Secure Client رشن كنكمي ال .يكذلا طقف حلاص.

عم اەقڧاوتو FMC ليجست نامضل ةيكذلا صيخارتلا < صيخارتلا < ماظنلا ىلإ لقتنا يكذلا صيخرتلا ةباوب:

Overview Analysis Policies	Devices Objects AMP Intelligence						🔍 Dep	loy System	Help 🔻 d	lperezve ▼
	Confi	uration Users	Domains In	tegration SecureX	Updates	Licenses + Smart Licenses	Logging •	Health 🔻	Monitoring •	Tools •
Smart License Status		Cisco Smart Softwar	re Manager 🛛 🌞 💲							
Usage Authorization:	Authorized (Last Synchronized On Sep 04 2021)									
Product Registration:	Registered (Last Renewed On Sep 04 2021)									
Assigned Virtual Account:	SEC TAC									
Export-Controlled Features:	Enabled									
Cisco Success Network:	Enabled (1)									
Cisco Support Diagnostics:	Disabled 🕕									

،ةيكذلا صيخارتلا ططخم نم يلفسلا ءزجلا يف .ةحفصلا سفن ىلع لفسأل ريرمتلاب مق، ةرفوتملا (AnyConnect) نمآلا Cisco ليمع صيخارت نم ةفلتخملا عاونألا ةيؤر كنكمي "(FTD) ةعرسلا قئاف لاسرإلا جمانرب" ليجست نم دكأت .اهنم لك يف ةكرتشملا ةزهجألاو" تائفلا هذه نم يأ نمض يلاحلا:

Smart Licenses		Filter Devices	× Edit i	Performance Tier Edit License
License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	٢			
🤉 🤪 Base (2)	0			
🖓 🕼 Malware (2)	0			
🖓 🕻 Threat (2)	0			
VIL Filtering (2)	0			
a 💋 AnyConnect Apex (2)	0			
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	٥	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdvha-dperezve (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMware - v7.0.0	0	Cisco Firepower Threat Defense for VMware	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				
tote: Container Instances of same blade share feature licenses			Activate Win Go to System in G	dows Control Panel to activate Windows.
login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				

FMC ىلإ Cisco Secure Client ةمزح ليمحت .2 ةوطخلا

ب ةصاخلا ثبلاو لابقتسالا ةدحو رشن ةمزح ليزنتب مق Cisco Secure Client (AnyConnect) ب قصاخلا ثبارة <u>cisco.com:</u> نم Windows ليغشتلا ماظنل

Application Programming Interface [API] (Windows) anyconnect-win-4.10.01075-vpnapi.zip Advisories	21-May-2021	141.72 MB	<u>+</u> \;
AnyConnect Headend Deployment Package (Windows) anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories 🗗	21-May-2021	77.81 MB	<u>+</u> \;
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories	21-May-2021	34.78 MB	<u>+</u> ₩
AnyConnect Headend Deployment Package (Windows 10 ARM64) anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	44.76 MB	<u>+</u> \;
Profile Editor (Windows) tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 📑	21-May-2021	10.90 MB	<u>+</u> \;
AnyConnect Installer Transforms (Windows) tools-anyconnect-win-4.10.01075-transforms.zip Advisories	21-May-2021	0.05 MB	<u>+</u> \;

ليمع ةروص ليمحتل Cisco ليمع فلم رتخاو نئاكلا ةرادإ < تانئاكلا ىل لوتنا ،نمآلا Cisco ليمع ةروص ليمحتل تايوتحملا لودج يف VPN ةئف نمض نمآلا:



مق ،نمآلا AnyConnect ليمع فلم ةفاضإ ةذفان يف AnyConnect فلم ةفاضإ رزلا رتخأ رتخأ ،اريخأو .نمآلا Cisco ليمع ةمزح رايتخال ..ضارعتسإ رتخأ مث ،نئاكلل مسا نييعتب ةلدسنملا ةمئاقلا يف فلملا عونك AnyConnect ليمع ةروص:

Overview Analysis Polici	es Devices Objects AMP Intelliger	nce			🌖 Deploy System Help 🔻	dperezve *
Object Management Intru	ision Rules					
AnyConnect File File objects represent files used in c	onfigurations, typically for remote access VPN policies.	They can contain AnyConne	ect Client Profile and AnyConnect Client Image files.		Add AnyConnect File	
IPvő Prefix List	Name			Value	Туре	
Ø Route Map						
a 🥪 Security Intelligence			No records to display			
DNS Lists and Feeds		Add AnyConnect F	ile	7 ×		
Network Lists and Feeds						
URL Lists and Feeds		Nama: 8	An Connect West 10			
Sinkhole		Norme.	AnyConnect_win_4.10			
SLA Monitor		File Name:*	anyconnect-win-4.10.01075-webdeploy-k9.p Browse			
Time Range						
👩 Time Zone		File Type:*	AnyConnect Client Image	 Image: A set of the set of the		
Tunnel Zone						
URL OF		Description:				
S Variable Set						
PLUCH Tag		-				
And And Connect File			Save	ancel		
R Certificate Man						
Custom Attribute						
Group Policy						
KEv1 IPsec Proposal						
DIKEV1 Policy						
KEv2 IPsec Proposal						
D IKEV2 Policy					No data to display < < Page 1	of 1 > > C
Last login on Friday, 2021-09-03 at 12						alah

تانئاكلا ةمئاق ىلإ نئاكلا ةفاضإ بجي .ظفح رزلا رتخأ:



ايتاذ ةعقوم ةداەش ءاشنإ .3 ةوطخلا

يف اهمادختساٍ متيل ةحلاص ةدحاو ةداهش دوجو (SSL Cisco Secure Client (AnyConnect بلطتي ليمعلاو VPN ةكبشب ةصاخلا ثبلاو لابقتسالا ةدحو نيب SSL محفاصم.

الكلذ ىلإ ةفاضإلاب .ضرغلا اذهل ايتاذ ةعقوم ةداهش ءاشنإ متي ،لاثملا اذه يف :ةظحالم لبق نم ةعقوم ةداهش ليمحت نكمملا نم ،ايتاذ ةعقوملا تاداهشلا ىلإ ةفاضإلاب اضيأ فورعم قدصم عجرم وأ ةيلخاد ةداهش ةطلس.

.تاداەش < ةزەجأ ىلإ لقتنا ،عيقوتلا ةيتاذ ةداەش ءاشنإل

 Overview
 Analysis
 Policies
 Devices
 Objects
 AMP
 Intelligence

 Device
 Management
 Device Upgrade
 NAT
 VPN •
 QoS
 Platform Settings
 FlexConfig
 Certificates

04 Deploy System Help ▼ dperezve ▼

ةفاضإ ةذفان يف زاهجلل ةلدسنملا ةمئاقلا يف دوجوملا FTD رتخأ مث .ةفاضإ رزلا رتخأ .ةديدج ةداهش

Overview Analysis Policies Devices Objects AMP Intel	igence	🔍 Deploy System	Help v dperezve v
Device Management Device Upgrade NAT VPN ▼ QoS Pl	tform Settings FlexConfig Certificates		
			Add
Name Domain	Enrollment Type Status		
	No certificates <u>Add Certificates</u>		
	Add New Certificate ? ×		
	Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.		
	Device*: rtdvha-dperezve 💌		
	Cert Enrollment*: Select a certificate entrollment object 💌 🔾		
	Add Cancel		
4			
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2			.1]1.1]1. cisco

ةذفان يف ،نآلاا مق .ديدج ليجست نئاك ءاشنإل (زمر + رضخأ) لوصولا ليجست ةفاضإ رز رتخأ ةمئاقلا يف ايتاذ ةعقوم ةداهش رتخاو نئاكلل مسا نييعتب ،رصنعلل لوخد ليجست ةفاضإ ليجستلا عون ةلدسنملا

Overview Analysis Policies Devices Objects AM	P Intelligence	🍳 Deploy System Help 🔻 dperezve 🔻
Device Management Device Upgrade NAT VPN ¥ Q	oS Platform Settings FlexConfig Certificates	
	Add Cert Enrollment	? ×
Name Domain	Name* SSL_SelfSigned	
	Description	
	CA Information Certificate Parameters Key Revocation	
	Enrollment Type: Self Signed Certificate	
	Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configur CN, please navigate to 'Certificate Parameters' tab.	re
	Allow Overrides	
	Save Cano	Antiometer Minuter
d		Go to System in Control Panel to activate Windows
		cisco

اريخاً (CN) كرتشم مسا كانه نوكي نأ ايمازلإ نوكي ،ايتاذ ةعقوملا تاداهشلل ةبسنلاب ،اريخاً (CN). فيرعتل ةداهشلا تاملعم بيوبتلا ةمالع ىلإ لقتنا

Overview Analysis Policies Devices Objects AMP	Intelligence			. Opploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN • Qot	5 Platform Settings Fle	xConfig Certificates		
	Add Cert Enrollment		? ×	Add *
Name Domain	Name*	SSL_SelfSigned		
	Description			
	CA Information Certif	icate Parameters Key Revocation		
	Include FQDN:	Don't use FQDN in certificate		
	Include Device's IP Address			
	Common Name (CN):	dperezve.local		
	Organization Unit (OU):			
	Organization (O):			
	Locality (L):			
	State (ST):			
	Country Code (C):	Comma separated country codes		
	Email (E):			
	Include Device's Serial Nu	mber		
	Allow Overrides			
		Save	Cancel	Activate Windows
Last Joain on Saturday. 2021-09-04 at 14:26:07 PM from 192.168.13.2				Go to System in Control Panel to activate Windows

:تاداەشلا ةمئاق ىلإ ةديدجلا ةداەشلا ةفاضإ بجي ،ناوث عضب دعب . ةفاضإو ظفح رارزأ رقنا

Overview Analysis	Policies Devices	Objects	AMP	Intelligence			0 ₄ Deploy System	Help 🔻	dperezve
Device Management	Device Upgrade	LAT VPN •	QoS	Platform Settings	FlexConfig	Certificates			
								0	Add
Name		De	main	Enrollment	Type :	Status			
4 🗐 ftdvha-dperezve	1							<u> </u>	
SSL_SelfSigned		GI	obal	Self-Signed		😔 CA 🔍 ID		200	8

FMC ىلع يلحم قاطن ءاشنإ .4 ةوطخلا

يلحم قاطن يف ةلباقملا رورملا تاملكو يلحملا مدختسملا تانايب ةدعاق نيزخت متي

زمير < لماكت < ماظن ىلإ لقتنا ،يلحملا لاجملا ءاشنإل



يف يلحم رايخ رتخاو مسا نييعتب مق ،ديدج قاطن ةفاضإ ةذفان يف .زيح ةفاضإ رز رتخأ عونلا ةلدسنملا ةمئاقلا:

Overview Analysis Policies Devices Objects	AMP I	ntelligence					System	Help 🔻 dj	
		Add New Realm		θ×	Licenses 🔻	Logging V	Health •	Monitoring *	Tools v
Cloud Services Realms Identity Sources Realms Realm Sequences Sync Results	High Av	Name" AnyConnect-Local-Auth Type LocaL Cocal User Configuration New Configuration	Description				Compare	Realms Ad	d Realm
		Add another local user	Confirm Password						
	The				<u>ne</u> .				
			Cancel	Save		Go to System in C	ontrol Panel to	activate Windo	ns.
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2									cisco

.يلحملا مدختسملا نيوكت مسق يف رورملا تاملكو نيمدختسملا تاباسح ءاشنإ متي

فرح فرح فرحو لڨألا ىلع دحاو ريبك فرح فرح فرح رورملا تاملكل نوكي نأ بجي :ةظحالم 🔌 دحاو صاخ فرحو دحاو مڨرو ريغص.

						_		
Overview Analysis Policies Devices Objects AMP	Intelligence					System	Help 🔻 dj	erezve 🔻
	Add New Realm		θ×	Licenses 🔻	Logging T H	lealth 🔻	Monitoring *	Tools *
Cloud Services Realmo Identity Sources High / Realms Realm Sequences Sync Results	Add New Realm Name" AnyConnect-Local-Auth Type LoCAL V Local User Configuration Add another local user	Confirm Password	e×	Licenses •	Logging • P	Compare	Realms Ad	Tools •
		Cancel	Save		Go to System in Con	trol Panel to	activate Windo	12.
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2								cisco

تالماعملا ةمئاق ىلإ ديدج قاطن ةفاضإل زيح ةفاضإ قوف رقنا مث ،تارييغتلا ظفحا

.ةدوجوملا

Overview Analysis Policies Devices Objects	AMP Intelligence									0₄ De	ploy System	Help 🔻 🕯	dperezve v
			Configuration	Users	Domains	Integration	SecureX	Updates	Licenses •	Logging •	Health 🔻	Monitoring	 Tools •
Cloud Services Realms Identity Sources	High Availability eStreamer	Host Input Client	Smart Software Ma	nager On	-Prem								
Realms Realm Sequences Sync Results													
											Compar	e Realms	dd Realm
Name - Description	Туре	Domain	AD Primary	Domain		84	ise DN				State		
AnyConnect-Local-Auth	LOCAL	Global									C Enable	d <u>↓</u> b	/ 5 🗑

SSL Cisco Secure Client نيوكت .5 ةوطخلا

دعب نع لوصولا < VPN < ةزهجألا ىلإ لقتنا ،SSL Cisco Secure Client نيوكتل



فيرعت فلمل مسا ديدحتب مق .ةسايس VPN ديدج تقلخ in order to رز add لا تقطقط بجي .فدهتسملا زاهجلا هنأ ىلع جردملا FTD رتخأ مث ،SSL رايتخإ ةناخ ددح مث ،لاصتالا دعب نع لوصولل VPN جهن جلاعم يف جهنلا نييعت مسق يف ءيش لك نيوكت:

Overview Analysis Policies Devices Objects AMP	P Intelligence	evConfin Cartificates		🍳 Deploy System H	elp 🔻 dperezve 🔻
Remote Access VPN Policy Wizard	Vos Plationin Settings II	excoming Certificates			
Policy Assignment 2 Connection Profile	3) AnyConnect 🔰 4) Access & Certifica	te S Summary			
Name:* Description: VPN Protocols: Targeted Devices:	SSL_AnyConnect_LocalAuth	Selected Devices	configuration elements to be in place to complete Nemete Access VPI Policy. Authentication server Configure (ACAL or Realm or SADUS Server Group or SSD to authenticate VPN clents. AnyConnect Client Package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard. Device Interface Device South be already configured on targeted devices so that they can be used as a security zone or Interface group to enable VPN access.		
				Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2					սիսիս

فيصوتل مسا فيرعتب مق .لاصتالا فيرعت فلم نيوكت ىلإ لقنلل يلاتلا رتخاً ،ةقداصملا مداخ ةلدسنملا ةمئاقلا يف ،مث .ةقداصم ةقيرطك طقف AAA رتخاو ليصوتلا ةلدسنملا ةمئاقلا يف 4 ةوطخلا يف ەؤاشنإ مت يذلا يلحملا قاطنلا رتخأ ،اريخأو ،يلحم رتخأ يلحملا قاطنلا

Overview Analysis Policies Devices Objects AMP Intelligence	🌒 Deploy	System Help 🔻	dperezve v
Device Management Device Upgrade NAT VPN - Remote Access QoS Platform Settings FlexConfig Certificates			
Remote Access VPN Policy Wizard			
Policy Assignment O Connection Profile AnyConnect A Access & Certificate S Summary			
Remote User AnyConnect Client Internet Outside Very Device Inside Corporate Resources			
Connection Profile:			
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.			
Connection Profile Name: * SSL_AnyConnect_LocalAuth			
Authentication, Authorization & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections. Authentication Method: AAA Only Authentication Server:* LOCAL Local Realm:* AnyConnect-Local-Auth Authorization Server: Authorization			
Accounting Server:			
	Activate Back dov	Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2			uluilu cisco

مسق يف صاصرلا ملقلا ةنوقيأ قوف رقنا مث ،ةحفصلا سفن ىلع لفسأل ريرمتلاب مق :نمآلا Cisco ءالمع لبق نم مدختسملا IP عمجت ديدحتل IPv4 نيوانع عمجت

Overview Analysis Policies Devices Objects AMP Inte		04 Deploy System Help ▼ dperezve ▼
Device Management Device upgrade NAI VPN • Remote Acc	ess Qob Platform Settings Flex.coning Certificates	
Policy Assignment Connection Profile 3 Anyi	Lonnect / 4 Access & Certificate / 5 Summary	
Authent	ICAL V (LOCAL or Realm or RADIUS)	
Author	Address Pools ? ×	
Accour	Available IPv4 Pools C Selected IPv4 Pools	
Client Addre:	Search	
Client IP addre assignment is	tdv-dperezve-pool ddress	
Use		
Use		
use Use		
Group Policy A group policy	ed. Select	
or create a Gr		
Group	OK Cancel	
		Back Next Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		-ili-ili- cisco

نمآلا Cisco ليمع ةروص ددح ،نآلاا .مسق AnyConnect ىلإ تلقن in order to كلذ دعب تقطقط 2: ةوطخلا يف اهليمحت مت يتلا

Overview Analysis Policies Devices Objects	AMP Intelligence				🔍 Deploy	System Help 🔻	dperezve v	
Device Management Device Upgrade NAT VPN •	Remote Access QoS Platf	form Settings FlexConfig Certificates						_
Remote Access VPN Policy Wizard								
1 Policy Assignment 2 2 Connection Profile	3 AnyConnect 4	Access & Certificate > 🌀 Summary						
Remote C	User AnyConnect Client	Internet Outside	VPN Device Inside	Corporate Resources				Î
Any The Initia	yConnect Client Image VPN gateway can automatically downly iated. Minimize connection setup time by	oad the latest AnyConnect package to the client choosing the appropriate OS for the selected pack	AAA device when the VPN connecti age.	ion is				
Dow	wnload AnyConnect Client packages from	Cisco Software Download Center.	Show Re-order buttons	0				
	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System					
	AnyConnect_Win_4.10	anyconnect-win-4.10.01075-webdeploy-k9.pkg	Windows					
_				_				
								+
					Activate Backdows	Next	Cancel	
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192,168,13.2							սիսիս	

ةلدسنملا ةمئاقلا يف .مسق Access & Certificate ىل تلقن in order to كلذ دعب تقطقط نيكمت مزلي يتلا ةمجاولا رتخأ ، نامألا ةقطنم/ةمجاولا ةعومجم (AnyConnect) مت يتلا ةداهشلا يف ،مث .اهيف (Access & Certificate) مت يتلا ةداهشلا رتخأ ،ةداهشلا ليجست ةلدسنملا ةمئاقلا يف ،مث .اهيف 3:

Overview Analysis Policies Devices Objects AMP Intelligence	🔍 Deploy	System Help 🔻	dperezve 🔻
Device Management Device Upgrade NAT VPN + Remote Access QoS Platform Settings FlexConfig Certificates			
Remote Access VPN Policy Wizard			
Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate S Summary			
Remote User AnyConnect Client Internet Outside User Corporate Resources			Î
AAA Network Interface for Incoming VPN Access Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN			
Interface group/Security Zone:* VLAN232			
Inable DTLS on member interfaces All the devices must have interfaces as part of the Interface Group/Security Zone selected.			
Device Certificates Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway. Certificate Enrollment:* SSL_SelfSigned			
	Activate Backdow	Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2			 cisco

لي المات المات المات المات الم الم الم الم المات ال



.FTD ىلع تارييغتلا رشنو ءاەنإ قوف رقنا ،ةحيحص تادادعإلا عيمج تناك اذإ

Overview	N .	Analysis Policies Devices Objects AMP Intelligence	e					0	Deploy System Help + dperezve	•
									Deployment Deployment Histor	y
									1 device selected Deploy time: Estimate Deploy	
۹		earch using device name, user name, type, group or status								
	9	Device	Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status	
> 0	2	ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 PM	₿.	Pending	
								Activate Wi Go to System in	ITCOWS In Control Panel to activate Windows.	
Last login or	n Sal	urday, 2021-09-04 at 14:26:07 PM from 192.168.13.2							uluulu cisco	

ةحصلا نم ققحتلا

ىل Windows ليمع نم Cisco AnyConnect Secure Mobility Client لاصتا أدبا ،رشنلا حاجن درجمب Windows ليمع نم Windows FTD. ةقداصملا رماوأ هجوم يف نيمدختسملا رورمل قملكو مدختسمل مسا نوكي نأ بجي 4:

	/PN:
	S Cisco AnyConnect 10.31.124.25 ×
	Group: SSL_AnyConnect_LocalAuth ~
¢ ()	Username: dperezve
	Password: *********

البق نم دامتعالا تانايب دامتعا درجمب FTD، قيبطت ضرعي نأ بجي Cisco AnyConnect Secure Mobility Client لالصتال المات:

🕙 Cisco AnyC	Connect Secure Mobility Client		_		Х
	VPN: Connected to 10.31.124.25.				
-	10.31.124.25	\sim	D	isconnect	
00:00:49]	[Pv4
Ö (i)					altalta cisco

cisco لا تضرع in order to رمأ vpn-sessionDB anyConnect ضرع تضكر عيطتسي تنأ ،FTD نم

```
ةيامحلا رادج ىلع ايلاح طشن ةسلج نوبز نمأي:
```

firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

: dperezve : 8 Username Index Public IP : 10.31.124.34 Assigned IP : 172.16.13.1 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel Protocol License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing Bytes Tx : 15756 Bytes Rx : 14606 Group Policy : DfltGrpPolicy Tunnel Group : SSL_AnyConnect_LocalAuth Login Time : 21:42:33 UTC Tue Sep 7 2021 Duration : 0h:00m:30s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 000000000080006137dcc9 Security Grp : none Tunnel Zone : 0

اهحالصإو ءاطخألا فاشكتسا

ىلع SSL لاصتا قڧدت ىرتل FTD ىلع SSL لاصتا قڧدت ىرتل FTD كاصتا ق FTD:

firepower# debug webvpn anyconnect 255

عم لاصتالا قفدت ةظحالم نكمي ،Cisco نم نمآلا ليمعلا ءاطخأ حيحصت ىلإ ةفاضإلاب قمزح طاقتلا قيرود ةحفاصم تايلمع ثالث لامكإ متي ،حجان لاصتا ىلع لاثم اذه .اضيأ TCP قمزح طاقتلا تايلمع ىلع ةقفاوملل مدختست SSL ةحفاصم اهعبتي ،FTD و Windows ليمع نيب ريفشتلا

*Ethernet1					- 0 3	×
File Edit View Go	Capture Analyze Str	atistics Telephony Wireles	ss Tools Help			
4 H & O						
I in add, 10.01.124.0						
H Diego substants			le con la colo			
		Particular and				1
13 3.331622	10.31.124.34	10.31.124.25	TCP 66.5	51300 + 443 [SYN] Seq+0 Hin+64240 Len+0 P55+1460 H5+256 SACK_PER*1 443 + 51300 [SYN_ACK] Seq+0 Ack+1 Hin+13268 Len+0 H55+1460		
15 3, 332833	10.31.124.34	10.31.124.25	TCP 54 5	51300 + 443 [ACK] Seg+1 Ack+1 Win+64240 Len+0		
16 3.338665	10.31.124.34	10.31.124.25	TL5v1.2 247 0	Client Hello	1 –	
17 3.341963	10.31.124.25	10.31.124.34	TCP 60 4	443 + 51300 [ACK] Seg=1 Ack=194 Win=32768 Len=0		
18 3.341963	10.31.124.25	10.31.124.34	TLSv1.2 1171 5	Server Hello, Certificate, Server Key Exchange, Server Hello Done		
21 3.390864	10.31.124.34	10.31.124.25	TCP 54 5	51300 + 443 [ACK] Seq=194 Ack=1118 Win=63123 Len=0		
29 5.494978	10.31.124.34	10.31.124.25	TLSv1.2 147 0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message		
30 5.496969	10.31.124.25	10.31.124.34	TLSv1.2 105 C	Change Cipher Spec, Encrypted Handshake Message		
31 5.497482	10.31.124.34	10.31.124.25	TLSv1.2 1299 #	Application Data		
32 5.498869	10.31.124.25	10.31.124.34	TCP 60 4	443 → 51300 [ACK] Seq=1169 Ack=1532 Win=32768 Len=0		
33 5,500054	10.31.124.25	10.31.124.34	TLSV1.2 594 A	Application Data		
34 5.500054	10.31.124.25	10.31.124.34	TLSV1.2 /9/ #	Application Data		
35 5.500054	10.31.124.25	10.31.124.34	TCP 54.5	Application Data 51300 + 443 [4/Y] Sen=1533 Ark=3488 Uin=64340 Len=0		
66 12 255001	10.31.124.34	10.31.124.25	TI Sv1.2 1524 4	Application Data		
67 12,269297	10.31.124.25	10.31.124.34	TCP 68.4	443 + 51300 [ACK] Sen+2488 Ark+2992 Win+32768 Len+0		
68 12.269297	10.31.124.25	10.31.124.34	TCP 68.4	443 + 51300 [ACK] Seg+2488 Ack+3002 Win+32768 Len+0		
69 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 594 #	Application Data		
70 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 1431 #	Application Data		
71 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 1433 #	Application Data		4
72 12.269518	10.31.124.34	10.31.124.25	TCP 54 5	51300 + 443 [ACK] Seq=3002 Ack=5784 Win=64240 Len=0		-
73 12.278473	10.31.124.25	10.31.124.34	TLSv1.2 1514 A	Application Data		
74 12.278473	10.31.124.25	10.31.124.34	TLSv1.2 1514 #	Application Data [TCP segment of a reassembled PDU]		
75 12.278473	10.31.124.25	10.31.124.34	TLSv1.2 1271 4	Application Data		Y
> Frame 13: 66 byte	es on wire (528 bits)), 66 bytes captured (!	528 bits) on interf	face \Device\NPF_{@C14AC43-8A81-4ACC-A85E-84CFC2FFC8C9}, id 0		
> Ethernet II, Src:	: Vhware_96:c6:e8 (04	0:50:56:96:c6:e8), Dst	: VMware_b3:84:a7 ((00:50:56:b3:84:a7)		
> Internet Protocol	l Version 4, Src: 10	.31.124.34, Dst: 10.31	.124.25			
Transmission Cont	trol Protocol, Src Pi	ort: 51300, Dst Port: 4	443, Seq: 0, Len: 0	0		
0000 00 50 56 b3 8	84 a7 00 50 56 96 c6	6 e8 88 88 88 45 88 · PV·	P V E			
0010 00 34 70 87 4	40 00 80 05 00 00 02 01 bb 04 55 01 b4 00	a 11 /C 22 8a 11 -4p				
0030 fa fo oc ao 0	00 00 02 04 05 54 01	1 03 03 05 01 01				
0040 04 02						

تانايب ةحص نم ققحتلاب FTD موقي نأ بجي ،لوكوتوربلاب لاصتالا ديكأت تايلمع دعب يلحملا قاطنلا يف ةنزخملا تامولعملا مادختساب دامتعالا.

.ثحبالا نم ديزمل Cisco TAC ب لصتاو DART ةمزح عمجت

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