# ةداەش ىلإ ةدنتسملا ةقداصملا نيوكت لقنتلا ءانثأ لوصولل AnyConnect

## تايوتحملا

قمدق مل ا قمدق مل ا متاب ا حاب ا حاب ا عناب ا حاب ا حاب ا حات مل ا عناب ا حاب ا حاث مل ا من المعن من المعن من المال من من من

## ەمدقملا

ةلومحملا ةزهجألاا ىلع ةداهشلا ىل قدنتسملا ةقداصملا ذيفنتل الاثم دنتسملا اذه حضوي.

## ةيساسألا تابلطتملا

يه ليلدلا يف ةمدختسملا ةزهجألاو تاودألا:

- o Cisco نم FirePOWER (FTD) ديدهت دض عافدلا
- Firepower (FMC) ةرادإ زكرم
- زامج Apple iOS (iPhone، iPad) زامج
- (CA) ةداەشلا حنم ةەج •
- o sco نم AnyConnect Client جمانرب

#### تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ةيساسأ VPN ةكبش
- SSL/TLS
- ماعلا حاتفملل ةيساسألا ةينبلا
- FMC عم ةبرجت •
- OpenSSL

Cisco AnyConnect

#### ةمدختسملا تانوكملا

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

- Cisco FTD
- Cisco FMC
- مداخ Microsoft CA
- XCA
- Cisco AnyConnect
- داب يآ لبآ

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 ،ليغشتلا ديق كتكبش.

## FTD ىلع Cisco AnyConnect نيوكت

عيمج رشن نم دكأت ،ءدبلا لبق .FMC ربع AnyConnect نيوكت تاوطخ مسقلاا اذه فصي تانيوكتلا.

#### ةكبشلل يطيطختلا مسرلا



FTD ىلإ ةداەش ةڧاضإ

رتخاو صيخرتلا < ةزهجألا ىلإ لقتنا .FMC زاهج ىلع FTD ل ةداهش ءاشنإب مق .1 ةوطخلا ةروصلا هذه يف حضوم وه امك ،ةفاضإ:

Firepower Management Center Devices / Certificates	Overview Ana	alysis Policies	Devices Objects	AMP	Intelligence	۹	Deploy	¢ 🕹	🛛 admin 🕶
	=					-		$\cdot \subset$	Add
Name	Domain	Enrollment Type	Status						
V = FTD1									
FTD	Global	Manual (CA & ID)	CA ID					G• 🖉	Ci
✓ 📾 Tcoutrie-FTD2									
ħd2	Global	PKCS12 file	CA (L)					G• 🖉	C
					How To				

ةزهجألل ةلدسنملا ةمئاقلا نم FTD زاهج رتخأ .ليصوت VPN لا ل بغر ب FTD لا 2. قوطخ ترتخأ. ةروصلا هذه يف حضوم وه امك ،ديدج ةداهش ليجست بولسأ ةفاضإل + ةنوقيأ ىلع رقنا:

← → C @ O A http	s://tcoutrie-fmc.tcoutrie-	security301.com/ddd/#P	alcerificate 🏠 😇 🐇 🕼 🖽 🔮 📟	e = 🗴 =	
Octing Started C School C Work				C Other Bookman	ks
Firepower Management Center Devices / Certificates	Overview A	nalysis Policies	Devices Objects AMP Intelligence Q Deploy 💞	🗘 🌒 admin	,
				Add	
Name	Domain	Enrollment Type	Status		
∨⇔FTD1					
FTD	Global	Manual (CA & ID)		• ₽ C ₹	
✓ 🚥 Tcoutrie-FTD2					
ftd2	Global	PKCS12 file	Add New Certificate	• ₽ C ∎	
			Add a new certificate to the device using cert enrollment object which is used to generate CA: Tootrie-FID2 Cert Enrollment*: Select a certificate entrollment object • (+) Cancel Add		
			How To		

ىلع لوصحلل ةلضفملا ةقيرطلا وه يذلا رايخلا رتخأ .زاهجلا ىلاٍ تاداەشلا فضاً .3 ةوطخلا ةئيبلا يف تاداەشلا. وه امك ،ظفح رقناو (طقف PKCS12) رورملا زمر لخدأ .FTD زاهج ىلاٍ ةداهشلا ليمحت .4 ةوطخلا ةروصلا هذه يف حضوم:

Add Cert Enrollme	ent	?
Name* ftdcert Description		
CA Information Enrollment Type: PKCS12 File*:	Certificate Parameters Key Revocation          PKCS12 File <ul> <li>Prowse PKCS12 File</li> </ul> Troutrie-ftd2 p12	_
Passphrase:	Skip Check for CA flag in basic constraints of the CA Certificate	
	Cancel	ave

ةدهاشمل .اروف ثدحت تاداهشلا رشن ةيلمع نإف ،فلملا ظفحب موقت نأ درجمب :ةظحالم 📎

## 🔌 فرعملا رتخأ ،ةداەشلا ليصافت.

#### Cisco AnyConnect نيوكت

.دعب نع لوصولا جلاعم مادختساب FMC ربع AnyConnect نيوكتب مق

AnyConnect. نيوكتل Remote Access VPN جەن جلاعم ليغشت ءدب 1. ةوطخلا

مزەجألا ىلإ لقتنا Add. رتخاو (دعب نع لوصولا) Remote Access <

cisco	Firepower Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence		٩	Deploy	¢ 😵	admin •
													Add
Name					Status				Last Modified				
RAVP	N				Targeting 1 d Up-to-date o	levices in all targeted d	levices		2021-07-09 17:10:31 Modified by "admin"		/ 1		
								How To					
								How To					

جەنلا نييعت .2 ةوطخلا.

جەنلا نييعت لامكإ: جەنلا ةيمستب مق أ.

بغر ب لوكوتورب VPN لا ترتخأ .ب.

c. نيوكتلا قيبطتل فدەتسملا زاەجلا رتخأ.

Periode Access VPN Policy Wizard           Policy Assignment         2 Connection Profile         3 AnyConnect         4 Access & Certificate         5 Summary		
Targeted Devices and Protocols     Sel      VPN Protocols:   VPI Protocols:   Targeted Devices   VPI Protocols:   Targeted Devices   VPI Protocols:	Before You Start. Before you start, ensure the following configuration elements to be in place to complete Remote Access VNN Policy. Authentication Server Configure Resin or RADIUS Server Group or SSO to authenticate VPN clients. AnyConnect Client Package Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Clicoc crederials to download it during the valued. Device Interface Interfaces should be already configured on targeted or interface group to enable VPN access.	
How To		Cancel Back Next

لاصتالا فيرعت فلم .3 ةوطخلا.

لاصتالا فيرعت فلم ةيمستب مق .أ طقف ليمعلا ةداهش ىلع ةقداصملا بولسأ نييعت .ب

ديدج ةعومجم جەن ءاشنإب مق ،رمألا مزل اذاو ،IP نيوانع عمجت نييعتب مق .ج.

(يلاتلا) Next قوف رقنا .د

Remote Access VPN Policy Wizard
1) Policy Assignment — 1 AnyConnect — 3 AnyConnect — 6 Access & Certificate — 5 Summary
Connection Profiles asset(f) the houring group publicles for a VPN connection. These publices partials to creating the benefitsed. Two shall a communicate and these addresses are assigned. They also includes user attributes, which are defined in group publices.
This name is configured as a connection alias, it can be used to connect to the VMV getensoy.
Authentication, Authorization & Accounting (AAA):
Specify the method of authentication (MAA, certificates or both), and the AAA servers that will be used for VMs conventions.
Authentication Methods Celete Device to Provide the Device of the Celeterate Device of the Celet
Username from 🐇 Map specific hold: 🔿 Use entrie DN (Distripublied Name) as sommane
Princy Flets (CK (Common Name) +
Secondry Field Nove •
Authorization Server: (Incent or 19/0.00)
Accounting Server: + +
Client Address Assignment:
Center Parkstreas can be assigned from AAA survey, CHCP and a service and P address pools, but and the address pools, but addre
□ Use AA Server (Resine #RADES only) ●
very structure overversal     test structure struct
Group Paticy:
A group policy is a collection of user-indential sension abilitybas which are assigned to client when a VPN connection is exhibiting. Select or creates a Coroup Fully values.
Group hility* (biblightiy +) +
Let Grup Palay

💊 تاسلجل مدختسملا مسا لاخدال همادختساٍ دارملا يساسألا لقحلا رتخاً :ةظحالم. ليلدلا اذه يف ةداهشلل CN مدختسي .ةقداصملا.

فوطخلا 4. AnyConnect.

رقناو AnyConnect نم لضفملا رادصإلا ليمحتب مق .زامجلا ىل AnyConnect قروص ةفاضإ يلاتا قوف.

Software.Cisco.com. مزح ليزنت نكمي :ةظحالم Software.Cisco.com.

.ةداەشلاو لوصولا .5 ةوطخلا

يف حضوم وه امك ،ةهجاولا ىوتسم ىلع AnyConnect نيكمتو ةهجاو ىلع ةداهشلا قيبطتب مق يلاتلا قوف رقناو ،ةروصلا هذه.

🗯 Firefox File Edit View History Bookmarks Tools Window Help				💲 🛤 🗢 😨 🍳 🚍 🧶 Frijul 30 10:40 AM -
Cisco Firepower Management C X +				
← → C @ ♦ https://tcoutrie-fmc.tcoutrie-security301.co	n/ddd/#RAVpnSetupWizard		û	छ 🛃 IN 🗈 😨 💭 🔤 🚏 ≡ ⊡ Other Bookmarks
CISCO Devices / VPN / Setup Wizard Overview Analysis Pr	olicies Devices Objects AMP Intelligence			९. Deploy 💕 🌣 🔕 admin 🕶
Remote Access VPN Policy Wizard				
Policy Assignment 2 Connection Profile 3 AnyConnect	Access & Certificate 5 Summary			
Bende User	Lerrerer Lierer Lierer Lierer Lierer Lierer Lerrerer Lierer Lerrererer Lerrerer Lerrerer Lerrerer Lerre	<pre>vpn baside vpn baside baside vpn baside vpn baside</pre>	Corporate Resources	
			How To	Cancel

.صخلم .6 ةوطخلا

رشنلا مث ءاەنإ قوف رقنا ،بحسلا تايلمع ةفاك بحس مت اذإ .تانيوكتلا عجار.

## ةلومحملا ةزهجألا يمدختسمل ةداهش ءاشنإ

ليصوتلا يف مدختسملا لومحملا زاهجلا ىلإ اهتفاضإل ةداهش ءاشنإ.

.XCA ةوطخلا

XCA حتف .أ

ةديدج تانايب ةدعاق ءدب .ب

.CSR ءاشنإ .2 ةوطخلا

(CSR) ةداەشلا عيقوت بلط رتخأ .أ

ديدج بلط رايتخإ .ب

ةداەشلل ةمزاللا تامولعملا لك عم ةميقلا لخدأ .ج

ديدج حاتفم ءاشنإ .د

قفاوم قوف رقنا ،ءاەتنالا دنع .ه

• • •	🛷 X Certificate a	nd Key management		
Create Certificate signing req	uest			3 Provinsk Priliden 7/11
Source	Extensions	Key usage Netscape	Advanced	
Distinguished name				
Internal name		organizationName		
countryName		organizationalUnitName		
stateOrProvinceName		commonName	Cisco_Test	
localityName		emailAddress		
Туре		Content		Add Delete
Private key Cisco_Test_1 (RSA:204	48 bit)	ᅌ 🗌 Used key	s too Generat	e a new key
			Ca	oncel OK

## 🌭 .ةداەشلاب صاخلا CN دنتسملا اذە مدختسي :ةظحالم.

.CSR لاسرإ .3 ةوطخلا

CSR ريدصت .أ

ةديدج ةداەش ىلع لوصحلل CA ىلإ CSR لاسرإ .ب

		I X	Certificate and Key manager	nent		
1		Private Keys	Certificates	Templates	Revocation lists	
	Internal name A commonName Signed					
	Cisco_Test Cisco_Test Unhandled					New Request
						Export
						Import
						Show Details
						Delete
						Insurincela
						3 Minshoo Fine
D	atabase: /Users/tcoutrie/cisco.xdb		Search			

.CSR ب صاخلا PEM قيسنت مدختساً :ةظحالم 🛇

لومحملا زاهجلا ىلع تيبثتلا

لومحملا زاهجلا ىلإ زاهجلا قداەش ةفاضإ .1 ةوطخلا. ديدج ةداەش قيبطت ةفاضإل AnyConnect قيبطت عم ةداەشلا كراش .2 ةوطخلا.

ال .قيبطتال عم ةداهشال مدختسمال كراشي نأ يوديال تيبثتال بالطتي :ريذحت 🗥 ربع اهعفد متي يتال تاداهشال يلع اذه قبطني

<b>C</b> Documents		certs		Select
Q Search				Ŷ
Cisco Test.p1	DMChain.p7b		Certificate Personal Control	Certificate
Сору	Ф	4/25/21, 1:50 1 KB	driod.p12 5/13/21, 7:04	driod_1.p12 5/13/21, 7:05
Duplicate	œ		4 KB	4 KB
Move	Ð	Contilligate	Certificate	Certificate
Delete	団	Perional	Perional	Perional
t Info	(j	Noblesse_IPA D_2.p12	Noblesse_IPh one.p12	Noblesse_IPh one_1.p12
Quick Look	۲	4/25/21, 11:18 4 KB	4/25/21, 10:31 3 KB	4/25/21, 11:01 4 KB
Tags	0			
Rename	1	Certificate Personal	Certificate Perional	Certificate Personal
Share	Û	Noblesse_MA	Noblesse_Wi	Noblesse_Wi
Compress	ē	<b>C_2.p12</b> 4/25/21, 11:19	ndows.p12 4/25/21, 12:56	ndowsIKE.p12 5/12/21, 12:42
410	4110	4 KB	3 KB	4 KB

دربم PKCS12 ل ةملك ةداهش .3 ةوطخ لخدي.

.AnyConnect ىلع ديدج لاصتا ءاشنإ .4 ةوطخلا

.VPN لاصتا ةفاضإ < تالاصتالا ؛ةديدج تالاصتإ ىلإ لقتنا .5 ةوطخلا

AnyConnect	VPN Connections	
PRIMARY VIRTUAL PRIVATE NETWORK		
AnyConnect VPN	CALO Enabled	Ð
Connections CALO >	номеіке	i
Details Disconnected >	HOMEIKE-IN	i
GENERAL	HOMESSL-IN	i)
Settings >	HomeIPEC-IN (	Ð
Diagnostics >	HomeIPSEC	Ð
About >	HomeSSL	Ð
	rtp-vpn-cluster.cisco.com	Ð
	Add VPN Connection	•
cisco		

ديدجلا لاصتالل ةمولعملا. 6 ةوطخ لخدي.

لاصتالا ةيمستب مق :فصولا

FTD ب صاخلا FQDN وأ IP ناونع :مداخلا ناونع

ةيفاضإ تانيوكت :مدقتم

مدقتم رتخأ .7 ةوطخلا.

اثيدح اەتڧاضإ تمت يتلا كتداەش رتخاو ةداەش رتخأ .8 ةوطخلا.

AnyConnect	VPN Co	VPN Connections			
PRIMARY VIRTUAL PRIVATE NETWO	RK				
AnyConnect VPN	Advanced Select Certificate		(j)		
Connections FT			(j)		
Details Disconnecte	Disabled				
Details	Selecting this option will disable certificate authentication.		í		
	Automatic		(j)		
GENERAL	This will automatically select a certificate for authentication.		•		
Settings	Noblesse_IPAD		í		
Disguastics	Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	(i)		
Diagnostics	Expiration Date: Apr 25, 2022 11:00:36	_			
About	Cisco_Test	(i) >	i		
	Expiration Date: Aug 02, 2022 08:12:47	<b>U</b>	(i)		
	Noblesse_IPAD		0		
	Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	i		
	Expiration Date: Apr 25, 2022 11:04:38				
	Noblesse_IPAD	(i) >			
	Issuer: DMSIIders-TCOUTRIE-SRV-CA	<b>U</b>			
	Expiration Date: Apr 25, 2022 00:42:05				
CISCO					

رابتخالاو تالاصتالا ىلإ ىرخأ ةرم لقتنا .9 ةوطخلا.

ةلاحلا يف الصتم ليصافتلا رەظتو ليغشتلا ديق ليدبتلا ىقبي ،ليدبتلا حاجن درجمب.



## ةحصلا نم ققحتلا

لصتملا فيضملا لوح تامولعملا عيمج show vpn-sessionDB detail AnyConnect رمألا ضرعي.

'sort' وأ 'filter' ةيساسألا تاملكلا وه رثكأ رمألا اذه حيشرتب موقي نأ رايخلا :حيملت sort' وأ 'filter' أي ساسألا تاملكلا وه رثكاً .

:لاثملا ليبس ىلع

Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect

Username : Cisco\_Test Index : 23 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel License : Anyconnect Premium, Anyconnect for Mobile Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 8627 Bytes Rx : 220 Pkts Tx : 4 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : SSL Tunnel Group : SSL Login Time : 13:03:28 UTC Mon Aug 2 2021 Duration : 0h:01m:49s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a7aa95d000170006107ed20 Security Grp : none Tunnel Zone : 0 Anyconnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 Anyconnect-Parent: Tunnel ID : 23.1 Public IP : 10.118.18.168 Encryption : none Hashing : none TCP Src Port : 64983 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : apple-ios Client OS Ver: 14.6 Client Type : Anyconnect Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 6299 Bytes Rx : 220 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 23.2 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 64985 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : SSL VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 2328 Bytes Rx : 0 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 23.3 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 51003 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : DTLS VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 0 Bytes Rx : 0 Pkts Tx : 0 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

اهحالصإو ءاطخألا فاشكتسا

#### ءاطخألا حيحصت

وه امحالصإو ةلكشملا هذه ءاطخأ فاشكتسال بولطملا حيحصتلا:

Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255

:SSL سيلو IPsec وه لاصتالا ناك اذإ

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14

:ةلومحملا ةزهجألل AnyConnect قيبطت نم تالجسلا

.تالجسلا ةكراشم < VPN ءاطخاً حيحصت تالجس < صيخشتلا ىلإ لقتنا

AnyConnect	Diagnostics
PRIMARY VIRTUAL PRIVATE NETWORK	
AnyConnect VPN	VPN Debug Logs
Connections Asa1 >	Logs
Details Disconnected >	System Information >
	Share Logs
GENERAL	Customize Debug Logs
Settings	
Diagnostics	Certificates
About >	Profile >
	Localization
CISCO	

تامولعملا لخدأ:

- ەلكشملا •
- رثاكتلل تأوطخ

.عم ةكراشم < لاسرإ ىلإ لقتنا مث

3:49 PM wed Sep 29		€ 47% ■			
AnyConnect		Diagnostics			
	DRK				
AnyConnect VPN	Cancel	Share Logs	Send		
Connections As	Please describe the following fields.	e problem and steps to r	Email logs to	>	
Details Disconnecte	PROBLEM		Administrator	>	
GENERAL	Test		Cisco		
Settings	STEPS TO REPRODU	CE	Share with	>	
Diagnostics	Test			/// · · ·	
About				>	
			1.1	>	
··i ··i ·· cisco	The data sent is for diagnostic purposes only and may contain information about configured connections, as well as server and endpoint identities, IP addresses, and username. This data will appear to come from the email address you specify and will not be used for marketing or advertising purposes.				

.تالجسلا لاسرال ينورتكلإ ديرب ليمع مادختسإ رايخ مدقي اذهو

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