SSL AnyConnect met lokale verificatie op FTD beheerde door FMC configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Configuraties Stap 1. Controleer de licenties Stap 2. Upload AnyConnect met FMC Stap 3. Een zelfondertekend certificaat genereren Stap 4. Lokaal antwoord op FMC maken Stap 5. Het configureren van SSL AnyConnect Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u Cisco AnyConnect met lokale verificatie kunt configureren op een Cisco Firepower Threat Defense (FTD) die wordt beheerd door Cisco Firepower Management Center (FMC). In het voorbeeld onder Secure Socket Layer (SSL) wordt gebruikt om Virtual Private Network (VPN) tussen FTD en een Windows 10-client te maken.

Bijgedragen door Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SSL AnyConnect-configuratie via FMC
- Configuratie van FireSIGHT-objecten via FMC
- SSL-certificaten op Firepower

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

• Cisco FTD versie 7.0.0 (gebouwd 94)

- Cisco FMC versie 7.0.0 (gebouwd 94)
- Cisco AnyConnect beveiligde mobiliteit-client 4.10.01075

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Vanaf release 7.0.0 ondersteunt FTD die wordt beheerd door FMC lokale authenticatie voor AnyConnect-klanten. Dit kan worden gedefinieerd als de primaire authenticatiemethode of als reserve voor het geval de primaire methode faalt. In dit voorbeeld wordt lokale authenticatie ingesteld als de primaire authenticatie.

Voor deze softwareversie was AnyConnect lokale verificatie op FTD alleen beschikbaar op Cisco Firepower Apparaatbeheer (FDM).

Configureren

Configuraties

Stap 1. Controleer de licenties

Voordat u AnyConnect kunt configureren moet de FMC worden geregistreerd en in overeenstemming zijn met Smart Licensing Portal. U kunt AnyConnect niet implementeren als FTD geen geldige Plus-, Apex- of VPN-licentie heeft.

Navigeer naar **Systeem > Licenties > Smart Licenties** om het FMC te valideren en is deze compatibel met Smart Licensing Portal.

Overview Analysis Policies	Devices Objects AMP Intelligence							🔍 De	ploy System	Help 🔻 d	perezve v .
	Confi	guration Users	Domains	Integration	SecureX	Updates	Licenses + Smart Licenses	Logging •	Health 🔻	Monitoring •	Tools •
Smart License Status		<u>Cisco Smart Softwa</u>	e Manager	e 9							
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 🕕										
Cisco Support Diagnostics:	Disabled ()										

Scroll-down op dezelfde pagina, onder in het schema van **slimme licenties**, u kunt de verschillende soorten AnyConnect-licenties zien die beschikbaar zijn en de apparaten die op elke licentie zijn geabonneerd. De geldigheid van de FTD in kwestie is geregistreerd onder één van deze categorieën.

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)	٥			
> 💋 Malware (2)	0			
> 💋 Threat (2)	0			
> 💋 URL Filtering (2)	0			
a 💋 AnyConnect Apex (2)	0			
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	٢	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)				
Note: Container Instances of same blade share feature licenses			Activate Win Go to System in	dows Control Panel to activate Windows.
st login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				

Stap 2. Upload AnyConnect met FMC

Download het AnyConnect Head-end implementatiepakket voor Windows van cisco.com.

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 Γ ⁴	21-May-2021	0.05 MB	±₩

Als u de AnyConnect-afbeelding wilt uploaden, navigeer dan naar **Objecten > Objectbeheer** en selecteer **AnyConnect File** onder de **VPN-**categorie in de inhoudsopgave.



Selecteer de knop Add AnyConnect File. In het venster Add AnyConnect File toewijzen u een naam voor het object en selecteert u Bladeren. Om het AnyConnect-pakket te kiezen en uiteindelijk AnyConnect-clientafbeelding als het bestandstype in het vervolgkeuzemenu te kiezen.

Overview Analysis Polici	es Devices Objects AMP Intelligen	ce		. I 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 AnyConnect Client Profile and AnyConnect Client Image files.		Add AnyConnect File
IPv6 Prefix List	Name		Value	Туре
Route Map Security Intelligence DNS Lists and Feeds		No records to display Add AnyConnect File	? X	
Network Lists and Feeds URL Lists and Feeds URL Lists and Feeds Lists and Fee		Name:" AnyConnect_Win_4.10 File Name:" anyConnect win-4.10.01073-webdeploy-k0.p Browse File Type:" AnyConnect Client Image Description: Save Ca)) Hncet	
Last login on Friday, 2021-09-03 at 12	246:00 PM from 192.168.13.2			No data to display (< Page 1 of 1 >) C

Selecteer de knop Opslaan en het object moet aan de lijst met objecten worden toegevoegd.



Stap 3. Een zelfondertekend certificaat genereren

SSL AnyConnect vereist dat één geldig certificaat in de SSL-handdruk tussen VPN-head-end en - client wordt gebruikt.

Opmerking: In dit voorbeeld wordt hiervoor een zelfondertekend certificaat gegenereerd. Naast de zelf ondertekende certificaten is het echter mogelijk om een certificaat te uploaden dat is ondertekend door een interne certificeringsinstantie (CA) of een bekende CA.

Om het zelf-ondertekende certificaat te maken, navigeer naar Apparaten > Certificaten.

Overview Analysis	Policies Devi	ces O	bjects	AMP Ir	ntelligence			🍳 Deploy System Help 🕶 di	perezve 🔻
Device Management	Device Upgrade	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates		

Selecteer de knop Add en kies vervolgens de FTD die in het vervolgkeuzemenu Apparaat in het venster Add New Certificate (Nieuw certificaat toevoegen) wordt gebruikt.

Device Management Device Upgrade NAT VPN • QoS Platform Settings FlexConfig Certificates Mame Domain Enrollment Type States No certificates Add New Certificate Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate Device*: Enrollment*: Select a certificate entrollment object	Overview Analysis Policies Devices Objects AMP Intelli	gence	0, Deploy System Help ▼ dperezve ▼
No certificates ? × Add a new certificate to the device using cert enrollment object which is used to generate CA and identify cretificate. ? × Device*: ftdyh-dperetyt Cert Enrollment*: Select a certificate entrollment object ** 0	Device Management Device Upgrade NAT VPN V QoS Pla	tform Settings FlexConfig Certificates	
No Enrollment Type Staus No certificates Add Certificates Add New Certificate ? × Add a new certificate to the device using cert enrollment object which is used to generate CA and identity certificate. Device*: Edvha-dperezve Cert Enrollment*: Select a certificate entrollment object			Add
Add New Certificates Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. Device*: Edvha-dparezve Cert Enrollment*: Select a certificate entrollment object	Name Domain	Enrollment Type Status	
Add New Certificate ? × Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. Pevice*: Device*: Pdvha-dperezve Cert Enrollment*: Select a certificate entrollment object		No certificates Add Certificates	
Add New Certificate ? × Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. Device*: Pdvha-dperezve Cert Enrollment*: Select a certificate entrollment object			
Add New Certificate ? × Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. Device*: Itdvha-dperezve Cert Enrollment*: Select a certificate entrollment object Add Cancel			
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. Device*: Ttdvha-dperezve Cert Enrollment*: Select a certificate entrollment object Add Cancel		Add New Certificate ? ×	
Device*: rtdvha-dperezve Cert Enrollment*: Select a certificate entrollment object Add Cancel		Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.	
Cert Enrollment*: Select a certificate entrollment object V O		Device*: ttdvha-dperezve	
Add Cancel		Cert Enrollment*: Select a certificate entrollment object	
		Add Cancel	
Activate Windows			Activate Windows
	Last Jude an Catavday 2021-00-04 at 14/26/07 04 from 102-168-12-2		attatta

Selecteer de knop **Toegang toevoegen** (groen + symbool) om een nieuw inschrijvingsobject te maken. Nu, in het venster **Add Cert Enrollment**, geef een naam voor het object toe en kies

Zelfgetekend Certificaat in het vervolgkeuzemenu Invoertype.

Overview Analysis Policies Devices Objects AMP	Intelligence		. I Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN ¥ Qo	S Platform Settings FlexConfig Certificates		
	Add Cert Enrollment	? ×	O Add
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 config CN, please navigate to 'Certificate Parameters' tab.	ure	
	Allow Overrides		
	Save	incel	A chusto Mindour
1			Go to System in Control Panel to activate Windows
			cisco

Ten slotte is het voor zelf ondertekende certificaten verplicht een gemeenschappelijke naam (GN) te hebben. Navigeer naar het tabblad **certificaatparameters** om een GN te definiëren.

Overview Analysis Policies Devices Objects AM	P Intelligence			. ● Deploy System Help v dperezve v
Device Management Device Upgrade NAT VPN • Q	oS Platform Settings Fl	exConfig Certificates		
	Add Cert Enrollment		? ×	C Add
Name Domain	Name*	SSL_SelfSigned	_	
	Description			
	CA Information Cert	ificate Parameters Key Revocation		
	Include FQDN:	Don't use FQDN in certificate		
	Include Device's IP Addres	s:		
	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 N	lumber		
	Allow Overrides	0		
		Save	Cancel	Activate Windows
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				Go to System in Control Panel to activate Windows

Selecteer de knoppen **Opslaan** en **Toevoegen** na een paar seconden. Het nieuwe certificaat moet aan de certificaatlijst worden toegevoegd.

Overview Analysis	Policies Devices	Objects AMP	Intelligence		0 ₄ Deploy System	Help 🔻	dperezve v
Device Management	Device Upgrade NAT	VPN VQ05	S Platform Settings FlexConfig	Certificates			
						0	Add
Name		Domain	Enrollment Type	Status			
4 🗐 ftdvha-dperezve							
SSL_SelfSigned		Global	Self-Signed	O CA ID		±₽¢	8

Stap 4. Lokaal antwoord op FMC maken

De lokale gebruikersdatabase en de respectievelijke wachtwoorden worden in een lokaal veld opgeslagen. Om het lokale rijk te maken navigeer naar **Systeem > Integratie > Realms**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence									🔍 Dej	ploy System	n Help 🔻 dp	erezve v
								Configuration	Users	Domains	Integration	SecureX	Updates	Licenses •	Logging •	Health 🔻	Monitoring •	Tools v
Cloud S	ervices	Realms	Identity	y Sources	High	Availability	eStreame	er Host Inp	ut Client	Smart So	ftware Manager	On-Prem						
Realn	ns Rea	lm Sequen	ces Sy	nc Results														

Selecteer de knop **Opnieuw toevoegen**. In het venster **Add New** Realm toewijzen een naam en selecteer **LOCAL** optie in het vervolgkeuzemenu **Type**.

Overview Analysis Policies Devices Objects	AMP I	ntelligence			🔍 Dep	oy System	n Help ∓ dp	erezve 🔻
		Add New Realm	θ×	Licenses *	Logging •	Health *	Monitoring •	Tools v
Cloud Services Realms Identity Sources	High Av	Name" Description AnyConnect-Local-Auth Type						
Realms Realm Sequences Sync Results		LOCAL						
		Local User Configuration Vername Password Confirm Password				Compar	e Realms Add	Realm
	The	Add another local steet		ne.				
Last Jooln on Diday, 2021-00-02 at 12:46:00 DM from 100-168-12-2		Cancel	Save		Go to System in (ontrol Panel t	o activate Window	սիսիս
Last logit of 190ay, 2021 09 03 at 12.40.00 PM field 192.108.13.2								cisco

Gebruikersrekeningen en wachtwoorden die in het gedeelte Local User Configuration zijn gemaakt.

Opmerking: Wachtwoorden moeten ten minste één hoofdletter, één kleine letter, één nummer en één speciaal teken hebben.

Overview Analysis Policies Devices Objects AMP	Intelligence			. ● Deploy System Help * dperezve *
	Add New Realm		• × Licenses •	Logging Health Monitoring Tools
Cloud Services Realms Identity Sources High / Realms Realm Sequences Sync Results	Add New Realm Name* AnyConnect-Local-Auth Type LOCAL V Local User Configuration Adversive Username Derrave Desename Add another local user	Confirm Password	•× Licenses •	Logging • Health • Monitoring • Tools •
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2		Cancel	Save	

Veranderingen opslaan en een nieuw gebied moeten aan de lijst met bestaande gebieden worden toegevoegd.

Overview Anal	ysis Policies	Devices Objects	AMP Intelligence										₿ ₄ De	ploy Syster	n Help v d	perezve v
						Configuration	Users	Domains	Integration	SecureX	Updates	Licenses •	Logging •	Health •	Monitoring •	Tools •
Cloud Service	s Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Ma	nager Or	n-Prem								
Realms	Realm Sequen	ces Sync Results														
														Compa	re Realms A	dd Realm
Name 👻	Descri	ption	Тут	xe	Domain	AD Primary	Domain		B	ase DN				State		
AnyConnect-Loc	al-Auth		LO	CAL	Global									ඟ Enable	id 🛨	· 5 🗑

Stap 5. Het configureren van SSL AnyConnect

Om SSL AnyConnect te configureren **navigeer** naar **Apparaten > VPN > Externe toegang**.

Overview Analysis	Policies Device	es Ob	ojects AMP Intelliger	nce				📙 Deploy	System	Help 🔻	dperezve v
Device Management	Device Upgrade	NAT	VPN Remote Access	QoS	Platform Settings	FlexConfig	Certificates				

Selecteer de knop **Toevoegen** om een nieuw VPN-beleid te maken. Defineer een naam voor het verbindingsprofiel, selecteer SSL selectieteken en kies de FTD in hand als het beoogde apparaat, alles moet in de sectie **Beleidstoewijzing** in de **wizard Afstandsbeleid van VPN** worden geconfigureerd.



Selecteer Volgende om naar de configuratie van het verbindingsprofiel te gaan. Defineer een naam voor het verbindingsprofiel en selecteer AAA Alleen als de authenticatiemethode, en selecteer vervolgens in het vervolgkeuzemenu Verificatieserver LOCAL en selecteer vervolgens het lokale veld dat is gemaakt in Stap 4 in het vervolgkeuzemenu Local Real.



Scroll-down op dezelfde pagina, selecteer vervolgens het potlood pictogram in het gedeelte IPv4adresgroep om de IP pool te definiëren die door AnyConnect-klanten wordt gebruikt.

Overview Analysis Policies Devices Objects AMP Inte	lligence	🍳 Deploy System Help 🔻 dperezve 🔻
Device Management Device Upgrade NAT VPN > Remote Acc	ess QoS Platform Settings FlexConfig Certificates	
Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 Any	Connect > ④ Access & Certificate > ⑤ Summary	
Authent	ication Server:* LOCAL V (LOCAL or Realm or RADIUS)	
	Address Pools ? ×	
Author	Available IPv4 Pools C O Selected IPv4 Pools	
Client Addre	Q Search ₩4 ftdv-dperezve-pool	
Client IP addre assignment is	dress ddress	
Use		
Use	Add	
Group Policy		
A group policy or create a Gr	ed. Select	
Group		
	OK Cancel	
		Back Next Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		-iliuliu cisco

Selecteer **Volgende** om naar het gedeelte **AnyConnect** te gaan. Selecteer nu de AnyConnectafbeelding die in Stap 2 is geüpload.

Overview Analysis Policies Devices Objects AMP Intelligence	0, Deploy S	System Help 🔻	dperezve v
Device Management Device Upgrade NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates			
Remote Access VPN Policy Wizard			
1 Policy Assignment 2 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 S Summary			
Remote User AnyConnect Client Outside User Corporate Resources			ĺ
AnyConnect Client Image			
The VMV gateway Can automatically download the latest Anyconnect package to the client device when the VMV connection is initiated. Himiting connection setup time by choosing the appropriate CS for the selected package.			
Download AnyConnect Client packages from <u>Cisco Software Download Center</u> . Show Bundler buttons			
AnyConnect File Object Name AnyConnect Client Package Name Operating System			
AnyConnect_Win_4.10 anyconnect-win-4.10.01075-webdeploy-k9.pkg Windows			
	to system como	Next	Cancel
Last Jooin on Saturday. 2021-00-04 at 14:26:07 PM from 192.168.13.2			aludo

Selecteer Volgende om naar het gedeelte Toegang en certificaat te gaan. Selecteer in het vervolgkeuzemenu Interfacegroep/Security Zone de interface waar AnyConnect moet worden ingeschakeld en selecteer vervolgens in het vervolgkeuzemenu certificaatinschrijving het certificaat dat in Stap 3 is gemaakt.

Overvlew 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		ĺ
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 connections.		
Interface group/Security Zone:* VLAN232		
☑ Enable DTLS on member interfaces		
Au the devices must have interfaces as part or 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 Windows	
	Go to System in Control Panel to	activate Windows
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		-ili-ili- cisco

Selecteer ten slotte Volgende om een samenvatting van de AnyConnect-configuratie te zien.



Als alle instellingen correct zijn, selecteert u Voltooien en implementeert u wijzigingen in FTD.

Over	view	Analysis Policies Devices Objects AMP Intelliger	ice					0	Deploy System Help +	dperezve *
									Deployment Deplo	yment History
									1 device selecte	d Deploy
T	Q,	Search using device name, user name, type, group or status							Deploy time: counter	
		Device	Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status	
>		ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 PM	8	Pending	
								A ctivato MG		
								Go to System in	Control Panel to activate Wind	iows.
Last lo	ain on S	aturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2								սիսիս

Verifiëren

Nadat de implementatie met succes is voltooid, kunt u een AnyConnect-verbinding van Windows client naar FTD starten. De gebruikersnaam en het wachtwoord die gebruikt worden in de authenticatie-prompt moeten hetzelfde zijn als in Stap 4.

	VPN:
	S Cisco AnyConnect 10.31.124.25
	Group: SSL_AnyConnect_LocalAuth ~
\$ (i)	Username: dperezve
	Password: *******
	OK Cancel

Zodra de aanmeldingsgegevens door FTD zijn goedgekeurd, moet AnyConnect-app de aangesloten status weergeven.

Cisco AnyC	Connect Secure Mobility Client		-		Х
	VPN: Connected to 10.31.124.25. 10.31.124.25	~	Di	sconnect	t
00:00:49					IPv4
Ö					ahaha

Vanaf FTD kunt u **show vpn-sessiondb uitvoeren** om de opdracht **aan te sluiten** om de AnyConnect-sessies weer te geven die momenteel actief zijn in de Firewall.

Assigned IP : 172.16.13.1 Public IP : 10.31.124.34 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 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 : 0000000000000000000137dcc9 Security Grp : none Tunnel Zone : 0

Problemen oplossen

Start **debug webVPN anyconnect** 255 opdracht op FTD om SSL-verbindingsstroom op FTD te zien.

firepower# debug webvpn anyconnect 255

Naast AnyConnect debugs kan ook de verbindingsstroom met TCP-pakketvastlegging worden waargenomen. Hieronder zie je een voorbeeld van een succesvolle verbinding. Er wordt een regelmatige drie handdruk tussen Windows client en FTD voltooid, gevolgd door een SSL-handdruk die wordt gebruikt om ciphers goed te keuren.

*Ethernet1						- a ×
File Edit View	Go Capture Analyze St	atistics Telephony Wirele	iss Tools Help			
🛋 III 🧟 🕒 📙	🖸 🗙 🖸 🤇 🗢 👳 🕯	s 🕴 🕴 🛄 🖬 🗗 🕯	l @ <u>!!</u>			
p.addr == 10.31.1	24.25					+ • 🖂
No. No.	C	Contraction (and the second			^
13 3.33162	2 10.31.124.34	10.31.124.25	TCP 66 51300 →	443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		
14 3.33273	3 10.31.124.25	10.31.124.34	TCP 60 443 + 51	1300 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460		
15 3.33283	3 10.31.124.34	10.31.124.25	TCP 54 51300 →	443 [ACK] Seg=1 Ack=1 Win=64240 Len=0		
16 3.33866	5 10.31.124.34	10.31.124.25	TLSv1.2 247 Client H	Hello		
17 3.34196	3 10.31.124.25	10.31.124.34	TCP 60 443 + 51	1300 [ACK] Seq=1 Ack=194 Win=32768 Len=0		
18 3.34196	3 10.31.124.25	10.31.124.34	TLSv1.2 1171 Server H	Hello, Certificate, Server Key Exchange, Server Hello Done		
21 3.39886	4 10.31.124.34	10.31.124.25	TCP 54 51300 +	443 [ACK] Seq=194 Ack=1118 Win=63123 Len=0		
29 5.49497	10.31.124.34	10.31.124.25	TISVI 2 147 Client K	Key Exchange, Change Cipher Spec, Encrypted Handshake Hessag	e	
31 5 49748	2 10.31.124.34	10.31.124.25	TISVI.2 1299 Apolicat	tion Data		
32 5,49806	10.31.124.25	10.31.124.34	TCP 60 443 + 51	1300 [ACK] Sep=1169 Ack=1532 Win=32768 Len=0		
33 5,50005	4 10.31.124.25	10.31.124.34	TLSv1.2 594 Apolicat	tion Data		
34 5,50005	4 10.31.124.25	10.31.124.34	TLSv1.2 797 Applicat	tion Data		
35 5.500054	4 10.31.124.25	10.31.124.34	TLSv1.2 90 Applicat	tion Data		
36 5.50015	10.31.124.34	10.31.124.25	TCP 54 51300 →	443 [ACK] Seq=1532 Ack=2488 Win=64240 Len=0		
66 12.2550	10.31.124.34	10.31.124.25	TLSv1.2 1524 Applicat	tion Data		
67 12.2692	07 10.31.124.25	10.31.124.34	TCP 60 443 → 51	1300 [ACK] Seq=2488 Ack=2992 Win=32768 Len=0		
68 12.2692	97 10.31.124.25	10.31.124.34	TCP 68 443 → 51	1300 [ACK] Seq=2488 Ack=3002 Win=32768 Len=0		
69 12.2692	97 10.31.124.25	10.31.124.34	TLSv1.2 594 Applicat	tion Data		
70 12.2692	97 10.31.124.25	10.31.124.34	TLSv1.2 1431 Applicat	tion Data		
71 12.2692	97 10.31.124.25	10.31.124.34	TLSv1.2 1433 Applicat	tion Data		
72 12.2695	18 10.31.124.34	10.31.124.25	TCP 54 51300 +	443 [ACK] Seq=3002 ACK=5784 Win=64240 Len=0		
75 12.2704	73 10.31.124.25	10.31.124.34	TLSVI.2 1514 Applicat	tion bata [T/B cannot of a case cashlad DNI]		
75 12 2784	73 10.31.124.25	10.31.124.34	TISUL 2 1271 Applicat	tion Data		
A frame the dd b	when on when /ENR blac) of hoter cashood i	EXP bits) on interface \De	with the fact and all short these successes on the a		
> Frame 13: 60 0	ytes on wire (520 bits	a), 60 bytes captured (0)50(56)(6)(6)(6)(8)) Dot	S28 Dits) on interface (De	evice(NPF_{0L14AL43-0A01-4ALC-A05E-04CFC2FFC0C9), 10 0		
> Internet Proto	col Version 4. Src: 18	.31.124.34. Dst: 10.31	124.25			
> Transmission (Control Protocol, Src P	ort: 51300, Dst Port:	443, Seo: 0, Len: 0			
0000 00 50 56 b	3 84 a7 00 50 56 96 c	6 e8 08 00 45 00 ·Pv	····P V····E·			
0010 00 34 70 8	f 40 00 80 06 00 00 0.	a 1f 7c 22 0a 1f -4p	·			
0020 7c 19 c8 6	4 01 bb 94 5b 21 b4 0	0 00 00 00 80 02	d[]			
0030 Ta 10 0c a	0 00 00 02 04 05 54 0	1 03 03 08 01 01				

Nadat de protocol handtekeningen zijn gemaakt, moet FTD geloofsbrieven valideren met informatie die in lokaal gebied is opgeslagen.

Verzamel de DART-bundel en neem contact op met Cisco TAC voor verder onderzoek.