Configuration du client sécurisé SSL avec authentification locale sur FTD

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Configurations
Étape 1. Vérifier les licences
Étape 2. Télécharger le package Cisco Secure Client vers FMC
Étape 3. Générer un certificat auto-signé
Étape 4. Créer un domaine local sur FMC
Étape 5. Configurer le client sécurisé Cisco SSL
Vérifier
Dépannage

Introduction

Ce document décrit comment configurer Cisco Secure Client (y compris Anyconnect) avec l'authentification locale sur Cisco FTD géré par Cisco FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration du client sécurisé SSL via Firepower Management Center (FMC)
- Configuration des objets Firepower via FMC
- Certificats SSL sur Firepower

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower Threat Defense (FTD) version 7.0.0 (build 94)
- Cisco FMC version 7.0.0 (build 94)
- Client Cisco Secure Mobility 4.10.01075

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans cet exemple, SSL (Secure Sockets Layer) est utilisé pour créer un réseau privé virtuel (VPN) entre FTD et un client Windows 10.

À partir de la version 7.0.0, FTD géré par FMC prend en charge l'authentification locale pour les clients sécurisés Cisco. Cette méthode peut être définie comme méthode d'authentification principale ou comme méthode de secours en cas d'échec de la méthode principale. Dans cet exemple, l'authentification locale est configurée comme authentification principale.

Avant cette version logicielle, l'authentification locale du client sécurisé Cisco sur FTD était uniquement disponible sur Cisco Firepower Device Manager (FDM).

Configurer

Configurations

Étape 1. Vérifier les licences

Avant de configurer Cisco Secure Client, le FMC doit être enregistré et conforme au portail de gestion des licences Smart. Vous ne pouvez pas déployer Cisco Secure Client si FTD ne possède pas de licence Plus, Apex ou VPN Only valide.

Accédez à System > Licenses > Smart Licenses afin de vous assurer que le FMC est enregistré et conforme à Smart Licensing Portal :

Overview Analysis Policie:	Devices Objects AMP Intelligence							🔍 De	ploy System	Help 🔻 dp	erezve *
	Co	nfiguration U	sers Domains	Integration	SecureX	Updates	Licenses + Smart Licenses	Logging •	Health 🔻	Monitoring •	Tools •
Smart License Status		Cisco Smart	Software Manager	9							
Usage Authorization:	Authorized (Last Synchronized On Sep 04 202))									
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 🕕										

Faites défiler la page vers le bas. Au bas du tableau Licences Smart, vous pouvez voir les différents types de licences Cisco Secure Client (AnyConnect) disponibles et les périphériques abonnés à chacune d'elles. Assurez-vous que le FTD disponible est enregistré dans l'une des catégories suivantes :

Smart Licenses		Filter Devices	× Edit	Performance Tier	Edit Licenses
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				
> 💋 URL Filtering (2)	٥				
a 🥩 AnyConnect Apex (2)	0				
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	0	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	٥	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 Wir Go to System in	idows Control Panel to activ	ate Windows.
it login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2					•1)• CI

Étape 2. Télécharger le package Cisco Secure Client vers FMC

Téléchargez le package de déploiement de tête de réseau Cisco Secure Client (AnyConnect) pour Windows à l'adresse <u>cisco.com</u>:

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	± ∵

Pour télécharger l'image Cisco Secure Client, accédez à Objets > Gestion d'objets et choisissez Fichier Cisco Secure Client sous la catégorie VPN dans la table des matières :



Cliquez sur le bouton Ajouter un fichier AnyConnect. Dans la fenêtre Add AnyConnect Secure Client File, attribuez un nom à l'objet, puis choisissez Browse.. pour sélectionner le package Cisco Secure Client. Enfin, choisissez AnyConnect Client Image comme type de fichier dans le menu déroulant :

Overview Analysis Policies Devi	ces Objects AMP Intelligence		● ₄ Deploy System Hel	p 🔻 dperezve 🔻
Object Management Intrusion Rules				
AnyConnect File			Add AnyConnect File	ter
File objects represent files used in configuration	is, typically for remote access VPN policies. They can contain AnyC	onnect Client Profile and AnyConnect Client Image files.		
Rende Man		Valu	е туре	
Koute Hap Security Intelligence		No secondo to disular:		
DNG Lists and Easts	Add And Conce	ino records to display		
Network Lists and Feeds	Add AnyConnec	r rie r	^	
IIRI Lists and Feeds				
Sinkhole	Name:*	AnyConnect_Win_4.10		
SLA Monitor	The Manual A			
Time Range	File Name: -	anyconnect-win-4.10.01075-webdeploy-k9.p Browse		
Time Zone	File Type: 8	In Connect Client Image		
and Tunnel Zone	the type:	Any connect chent image		
ORL .	Description:			
S Variable Set				
NLAN Tag				
A BO VPN		Save Cancel		
ManyConnect File			-	
R Certificate Map				
Custom Attribute				
Group Policy				
IKEV1 IPsec Proposal				
IKEV1 Policy				
IKEV2 IPsec Proposal			and the second	
DP IKEV2 Policy			No data to display IK K Page []) of T >> > C
				athatha

Cliquez sur le bouton Enregistrer. L'objet doit être ajouté à la liste des objets :



Étape 3. Générer un certificat auto-signé

SSL Cisco Secure Client (AnyConnect) nécessite l'utilisation d'un certificat valide dans la connexion SSL entre la tête de réseau VPN et le client.

Remarque : dans cet exemple, un certificat auto-signé est généré à cette fin. En outre, outre les certificats auto-signés, il est possible de télécharger un certificat signé par une autorité de certification interne ou par une autorité de certification bien connue.

Pour créer le certificat auto-signé, accédez à Périphériques > Certificats.

```
      Overview
      Analysis
      Policies
      Devices
      Objects
      AMP
      Intelligence
      Operezve *

      Device
      Management
      Device Upgrade
      NAT
      VPN *
      QoS
      Platform Settings
      FlexConfig
      Certificates
```

Cliquez sur le bouton Ajouter. Sélectionnez ensuite le FTD répertorié dans le menu déroulant Device de la fenêtre Add New Certificate.

Overview Analysis Policies Devices Objects AMP Intel	igence	🔒 Deploy System	Help v dperezve v
Device Management Device Upgrade NAT VPN ¥ QoS Pla	tform Settings FlexConfig Certificates		
			Add
Name Domain	Enrollment Type Status	1	
	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*: tdvha-dperezve		
	Cert Enrollment*: Select a certificate entrollment object		
	Add Cancel		
<			
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2			uluulu cisco

Cliquez sur le bouton Add Cert Enrollment (vert + symbole) pour créer un nouvel objet d'inscription. À présent, dans la fenêtre Ajouter une inscription de certificat, attribuez un nom à l'objet et choisissez Certificat auto-signé dans le menu déroulant Type d'inscription.

Overview Analysis Policies Devices Objects AM	P Intelligence			Q _i Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN ¥ Q	oS Platform Settings	FlexConfig Certificates		
	Add Cert Enrollment		? ×	e Add
Name Domain	Name*	SSL_SelfSigned		
	Description			
	CA Information	Certificate Parameters Key Revocation		
	Enrollment Type:	Self Signed Certificate		
	Common Name (CN) i CN, please navigate to	is mandatory for self-signed certificate that is used in Remote Access VPN. To confi o "Certificate Parameters" tab.	pure	
	Allow Querrides	0		
	Allow Overhues			
		Save	ancel	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

Enfin, pour les certificats auto-signés, il est obligatoire d'avoir un nom commun (NC). Accédez à l'onglet Paramètres de certificat pour définir un CN :

Overview Analysis Policies Devices Objects AMP	Intelligence			. I Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN • Qot	5 Platform Settings Flex	xConfig Certificates		
	Add Cert Enrollment		? ×	Add *
Name Domain	Name* s	SL_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 C			
		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

Cliquez sur les boutons Enregistrer et Ajouter. Après quelques secondes, le nouveau certificat doit être ajouté à la liste des certificats :

Overview Analysis	Policies Devices	Objects AMP	Intelligence		0 ₄ Deploy System Help v dperezve v
Device Management	Device Upgrade N	AT VPN • Qo	S Platform Settings Flex	Config Certificates	
					▲ Add
Name		Domain	Enrollment Type	Status	
4 🗐 ftdvha-dperezve	•				≙
SSL_SelfSigned		Global	Self-Signed	🛇 CA 🔍 ID	±2¢≣

Étape 4. Créer un domaine local sur FMC

La base de données d'utilisateur locale et les mots de passe respectifs sont stockés dans un domaine local. Pour créer le domaine local, accédez à Système > Intégration > Domaines :



Cliquez sur le bouton Ajouter un domaine. Dans la fenêtre Ajouter un nouveau domaine, attribuez un nom et choisissez l'option LOCAL dans le menu déroulant Type :

Overview Analysis Policies Devices Objects AMP	ntelligence			€ <mark>4</mark> Deplo	System	Help 🔻 dj	perezve #
	Add New Realm	θ×	Licenses 🔻	Logging •	Health • M	onitoring 🔻	Tools v
Cloud Services Realms Identity Sources High A Realms Realm Sequences Sync Results	Name" AnyConnect-Local-Auth Type LoCA Local User Configuration Username Password Confirm Password Add another local user		ne.		Compare Re	eaims Ad	d Reatm
	Cancel	Save		Go to System in Co	ontrol Panel to ac	tivate Windo	ws.
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2							cisco

Les comptes d'utilisateurs et les mots de passe sont créés dans la section Configuration utilisateur locale.

Remarque : les mots de passe doivent comporter au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

a second design and the access allowed this								
Overview Analysis Policies Devices Objects AMP I	Add New Pealm		8 Y		💘 Depl	oy System	Help v dp	erezve 🔻
	Add New Realm		• ^	Licenses *	Logging •	Health •	Monitoring •	Tools •
	Name*	Description						
Cloud Services Poplars Identity Sources High A	AnyConnect-Local-Auth							
Ciour Services Reality Jources High A	Туре							
Realms Realm Sequences Sync Results	LOCAL							
	Local User Configuration							
	∧ dperezve							
	Username							
	dperezve							
	Described of the second s	Confirm Deserved						
	Password	Contrim Password	_					
			_					
	Add another local user							
The				20				
THE				<u>ne</u> .				
			_					
		Cancel	Save		Go to System in O	ontrol Panel to	activate Windo	12.
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2								cisco

Enregistrez les modifications, puis cliquez sur Ajouter un domaine pour ajouter un nouveau domaine à la liste des domaines existants.



Étape 5. Configurer le client sécurisé Cisco SSL

Pour configurer SSL Cisco Secure Client, accédez à Devices > VPN > Remote Access :



Cliquez sur le bouton Add afin de créer une nouvelle stratégie VPN. Définissez un nom pour le profil de connexion, cochez la case SSL et sélectionnez le FTD répertorié comme périphérique cible. Tout doit être configuré dans la section Affectation de stratégie de l'Assistant Stratégie VPN d'accès à distance :



Choisissez Next afin de passer à la configuration Connection Profile. Définissez un nom pour le profil de connexion et choisissez AAA Only comme méthode d'authentification. Ensuite, dans le menu déroulant Authentication Server, choisissez LOCAL, et enfin, choisissez le domaine local créé à l'étape 4 dans le menu déroulant Local Realm :

Overview Analysis Policies Devices Objects AMP Intelligence	🄍 Deploy	System Help v	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 VPN Device Inside Corporate Resources			Î
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 This name is configured as a connection alias, it can be used to connect to the VPN gateway			
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 V (LOCAL or Realm or RADIUS)			
Local Realm:* AnyConnect-Local-Auth 🗸 🕤			
Authorization Server: CRaalm or RADIUS)			
Accounting Server:			
	Activate Back dow	Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2			·ili·ili· cisco

Faites défiler la page vers le bas, puis cliquez sur l'icône de crayon dans la section IPv4 Address Pool afin de définir le pool d'adresses IP utilisé par les clients sécurisés Cisco :

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		
Policy Assignment O Connection Profile O Any	Connect > 🕢 Access & Certificate > 😙 Summary	
Authent	ication Server:* LOCAL V (LOCAL or Realm or RADIUS)	•
	Address Pools ? ×	
Author	Available IPv4 Pools C O Selected IPv4 Pools	
Client Addres	Search	
Client P addre	Hav- dperezve-pool	
Use		
🗹 Use		
Group Policy	ad Colors	
or create a Gr	en beret	
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

Cliquez sur Next afin de passer à la section AnyConnect. Sélectionnez maintenant l'image du client sécurisé Cisco téléchargée à l'étape 2 :

				-
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 O Connection Profile AnyConnect Access & Certificate S Summary				
Remote User AnyConnect Client Internet Outside VPN Device Inside Corporate Resources				-
Any Connect Linent Image The VPM gateway can automatically download the latest AnyConnect package to the client device when the VPM connection is				
initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.				ĩ
Download AnyConnect Client packages from <u>Clico Software Download Center</u> . Show Re-order buttons				
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 Ne	xt	Cancel	
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192,166.13.2			սիսիս	Ī

Cliquez sur Next afin de passer à la section Access & Certificate. Dans le menu déroulant Interface group/Security Zone, choisissez l'interface sur laquelle Cisco Secure Client (AnyConnect) doit être activé. Ensuite, dans le menu déroulant Certificate Enrollment, choisissez le certificat créé à l'étape 3 :

Overview Analysis Policies Devices Objects AMP Intelligence	🍳 Deploy System Help 🔻 dper	ezve 🔻
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 Access & Certificate 5 Summary		
Remote User AnyConnect Client Linternet Outside User Indide Corporate Resources		
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		
connections. Interface group/Security Zone:* VLAN232 V 🛇 •		
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 Backdows Next Cano	el
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		ılı.ılı. cısco

Enfin, cliquez sur Next pour afficher un résumé de la configuration de Cisco Secure Client :



Si tous les paramètres sont corrects, cliquez sur Finish et déployez les modifications sur FTD.

Overview	Analysis Policies Devices Objects AMP Intelligen	ce					(Deploy System Help v dpere	nzve v History
								1 device selected	
T Q	Search using device name, user name, type, group or status							Deploy time: Estimate	
۲	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 chivata M		
							Go to System i	n Control Panel to activate Windows.	
Last login on	Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2							·!	luilu

Vérifier

Une fois le déploiement réussi, initiez une connexion Cisco AnyConnect Secure Mobility Client du client Windows au FTD. Le nom d'utilisateur et le mot de passe utilisés dans l'invite d'authentification doivent être identiques à ceux créés à l'étape 4 :

<u> </u>	'PN:
	S Cisco AnyConnect 10.31.124.25 ×
	Group: SSL_AnyConnect_LocalAuth ~
\$ ()	Username: dperezve
	Password: *********

Une fois les informations d'identification approuvées par le FTD, l'application Cisco AnyConnect Secure Mobility Client doit afficher l'état connecté :

Cisco Any	Connect Secure Mobility Client		_		Х
	VPN: Connected to 10.31.124.25. 10.31.124.25	~	Di	sconnect	
00:00:49				1	Pv4
Ö (i)					altalta

À partir de FTD, vous pouvez exécuter la commande show vpn-sessiondb anyconnect afin

d'afficher les sessions Cisco Secure Client actuellement actives sur le pare-feu :

firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

```
Username
           : dperezve
                                              : 8
                                   Index
                                   Public IP : 10.31.124.34
Assigned IP : 172.16.13.1
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 : 0000000000080006137dcc9
                                   Tunnel Zone : 0
Security Grp : none
```

Dépannage

Exécutez la commande debug webvpn anyconnect 255 sur FTD afin de voir le flux de connexion SSL sur FTD :

firepower# debug webvpn anyconnect 255

Outre les débogages du client sécurisé Cisco, le flux de connexion peut également être observé avec les captures de paquets TCP. Il s'agit d'un exemple de connexion réussie, une connexion normale de trois mois entre le client Windows et FTD est terminée, suivie d'une connexion SSL utilisée pour accepter les chiffrements.

*Ethernet1				- 0)
File Edit View Go	Capture Analyze Sta	stistics Telephony Wireles	as Tools Help	
4 H & 0 H D		+ e e		
				[2] [2] a
N 0.8007 == 10.31.124.25			le su la la sella e	
	10.00.00	10.01.104.04		
13 3.331022	10.31.129.39	10.31.124.25	1CP 00 51300 + 443 [518] 35600 HAINENALAU LENUN 15541400 HO-450 5044 (1589)	
15 3,332833	10,31,124,34	10.31.124.25	TCP 54 51300 + 443 fact Secal Acks1 Hin-64240 Len-0	
16 3.338665	10.31.124.34	10.31.124.25	TLSv1.2 247 Client Hello	
17 3.341963	10.31.124.25	10.31.124.34	TCP 60 443 → 51300 [ACX] Seq=1 Ack=194 Win=32768 Len=0	
18 3.341963	10.31.124.25	10.31.124.34	TLSv1.2 1171 Server Hello, Certificate, Server Key Exchange, Server Hello Done	
21 3.390864	10.31.124.34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seq=194 Ack=1118 kin=63123 Len=0	
29 5.494978	10.31.124.34	10.31.124.25	TLSv1.2 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
30 5.496969	10.31.124.25	10.31.124.34	TLSV1.2 105 Change Cipher Spec, Encrypted Handshake Message	
31 5.497462	10.31.124.34	10.31.124.25	TLSVI.2 1299 Application Data 770 60443 - 51306 TAVI Can-1500 Ark-1503 U(n-13750 Lan-8	
11 5 500054	10.31.124.25	10.31.124.34	TISAL 2 SALADIATION Data	
34 5,500054	10.31.124.25	10.31.124.34	TLSVI.2 797 Application Data	
35 5,500054	10.31.124.25	10.31.124.34	TLSv1.2 90 Application Data	
36 5.500158	10.31.124.34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seq=1532 Ack=2488 Win=64240 Len=0	
66 12.255091	10.31.124.34	10.31.124.25	TLSv1.2 1524 Application Data	
67 12.269297	10.31.124.25	10.31.124.34	TCP 60 443 + 51300 [ACK] Seq=2488 Ack=2992 Win=32768 Len=0	
68 12.269297	10.31.124.25	10.31.124.34	TCP 60.443 → 51300 [ACK] Seq+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 1433 Application Data	
71 12.269297	10.31.124.25	10.31.124.34	TLSv1.2 1433 Application Data	
72 12.269518	10.31.124.34	10.31.124.25	TCP 54 51300 + 443 [ACK] Seq+3002 ACK=5784 Win=64240 Len=0	
74 12.278473	10.31.124.25	10.31.124.34	TEVALE 1514 Application with	
75 12,278473	10, 31, 124, 25	10.31.124.34	TLSv1.2 1271 Application Data	
> Frame 13: 66 huter	s on wire (528 hits)) 66 butes cantured (Stability in interface \Device\NDF [Artificit.RIS1.dlf.ARTF.SETFOFFCATA]. id a	
> Ethernet II, Src:	Whare 96:c6:e8 (0)	0:50:56:96:c6:e8), Dst	: Whare b3:84:a7 (00:50:56:b3:84:a7)	
> Internet Protocol	Version 4, Src: 10.	.31.124.34, Dst: 10.31	124.25	
> Transmission Contr	rol Protocol, Src Po	ort: 51300, Dst Port: 4	443, Seq: 0, Len: 0	
0000 00 50 56 b3 84	a7 00 50 56 96 c6	5 e8 88 88 88 45 88 · PV·	P VE-	
0010 00 34 70 8f 40	0 00 50 05 00 00 0a	a 1f 7c 22 0a 1f -4p-		
0010 fa fa fa a al 00	00 94 50 21 04 00		4* L 1	
0040 04 02				

Après les échanges de protocole, FTD doit valider les informations d'identification avec les informations stockées dans le domaine local.

Recueillez l'offre DART et contactez le TAC Cisco pour plus d'informations.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.