FTDのローカル認証でSSLセキュアクライアン トを設定する

内容 はじめに 前提条件 要件 使用するコンポーネント 背景説明 設定 コンフィギュレーション ステップ1:ライセンスの確認 ステップ2: Cisco Secure ClientPackageのFMCへのアップロード ステップ3:自己署名証明書の生成 ステップ5: SSL Cisco Secure Clientの設定 確認

<u>トラブルシュート</u>

はじめに

このドキュメントでは、Cisco FMCによって管理されるCisco FTDのローカル認証でCisco Secure Client(Anyconnectを含む)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)によるSSLセキュアクライアント(SSL)の設定
- FMCによるFirePOWERオブジェクトの設定
- FirepowerでのSSL証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ Cisco Firepower Threat Defense(FTD)バージョン7.0.0 (ビルド94)
- Cisco FMCバージョン7.0.0(ビルド94)
- ・ Cisco Secure Mobilityクライアント4.10.01075

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

この例では、Secure Sockets Layer(SSL)を使用して、FTDとWindows 10クライアント間にバー チャルプライベートネットワーク(VPN)を作成します。

リリース7.0.0以降、FMCによって管理されるFTDは、Cisco Secure Clientのローカル認証をサポ ートします。これは、プライマリ認証方式、またはプライマリ認証方式が失敗した場合のフォー ルバックとして定義できます。この例では、ローカル認証がプライマリ認証として設定されてい ます。

このソフトウェアバージョンより前のバージョンでは、FTD上のCisco Secure Clientローカル認 証は、Cisco Firepower Device Manager(FDM)でのみ使用できました。

設定

コンフィギュレーション

ステップ1: ライセンスの確認

Cisco Secure Clientを設定する前に、FMCが登録され、スマートライセンシングポータルに準拠 している必要があります。FTDに有効なPlus、Apex、またはVPN Onlyライセンスがない場合は、 Cisco Secure Clientを導入できません。

System > Licenses > Smart Licensesの順に移動して、FMCが登録されていて、スマートライセンスポータルに準拠していることを確認します。

Overview Analysis Policies	Devices Objects AMP Intelligen	ICB						🔍 De	ploy System	Help 🔻 dp	erezve v
		Configuration U	sers Domains	Integration	SecureX	Updates	Licenses + Smart Licenses	Logging •	Health •	Monitoring •	Tools v
											î
Smart License Status		Cisco Smart	Software Manager	9							
Usage Authorization:	Authorized (Last Synchronized On Sep 04 20	021)									
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 🕕										

同じページを下にスクロールします。スマートライセンスのグラフの下部には、使用可能なCisco Secure Client(AnyConnect)ライセンスのタイプと、ライセンスにサブスクライブしているデバイ スが表示されます。次のいずれかのカテゴリで、手元のFTDが登録されていることを確認します 。

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)	0			
⊳ 💋 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 Win Go to System in	dows Control Panel to activate Windows.
t login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				.,

ステップ 2:Cisco Secure ClientパッケージのFMCへのアップロード

Windows用のCisco Secure Client(AnyConnect)ヘッドエンド導入パッケージを<u>cisco.com</u>からダウ ンロードします。

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	±₩
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	±₩
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	±₩
AnyConnect Installer Transforms (Windows) tools-anyconnect-win-4.10.01075-transforms.zip	21-May-2021	0.05 MB	<u>+</u> \;

Cisco Secure Clientイメージをアップロードするには、Objects > Object Managementの順に選択 し、目次でVPNカテゴリの下にあるCisco Secure Client Fileを選択します。



Add AnyConnect Fileボタンを選択します。Add AnyConnect Secure Client Fileウィンドウで、オ ブジェクトに名前を割り当て、Browse...を選択して、Cisco Secure Clientパッケージを選択しま す。最後に、ドロップダウンメニューでファイルタイプとしてAnyConnect Client Imageを選択し ます。

Object Management Intrusion Rules AnyConnect File Image: Connect File File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files. Value Type Image: Profile Security Intelligence No records to display No records to display Metwork Lists and Feeds Add AnyConnect File ? ×	
And AnyConnect File File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.	
Ipvd Prefix List Name Value Type Ø Route Hap Security Intelligence No records to display Ø No Redsds Add AnyConnect File ? ×	
Ø Route Map No records to display Ø Route Reds Add AnyConnect File Network Lists and Feeds ? ×	
Security Intelligence No records to display DNS Lists and Feeds Network Lists and Feeds Network Lists and Feeds	
DNS Lists and Feeds Add AnyConnect File 7 ×	
Whetwork Lists and Feeds	
URL Lists and Feeds Name** Approximate Win 4.10	
Sinkhole http://www.angle.com/angle.com/angle/angl	
SLA Monitor File Name:* anyconnect-win-4.10.01075-webdeploy-k9.p Browse.	
Gen Time Range	
Time Zone File Type:* AnyConnect Client Image	
United actions and a second action ac	
C Variable Sat	
S VLAN Tag	
- BIVPN	
MANyConnect File	
R ² Certificate Map	
🚯 Custom Attribute	
🚰 Group Policy	
C IKEV1 IPsec Proposal	
E ¹ IKEVI Policy	
KEv2 Ibsec Proposal	
Biblev 2 Policy 🐡	> C

Saveボタンを選択します。オブジェクトをオブジェクトリストに追加する必要があります。



ステップ3:自己署名証明書の生成

SSL Cisco Secure Client(AnyConnect)では、VPNヘッドエンドとクライアント間のSSLハンドシェイクで使用する有効な証明書が1つ必要です。

◆ 注:この例では、この目的のために自己署名証明書が生成されます。また、自己署名証明書の他に、内部認証局(CA)または既知のCAのいずれかによって署名された証明書をアップロードすることもできます。

自己署名証明書を作成するには、Devices > Certificatesの順に移動します。

 Overview
 Analysis
 Policies
 Devices
 Objects
 AMP
 Intelligence
 Operation
 Operatio

Addボタンを選択します。次に、Add New CertificateウィンドウのDeviceドロップダウンメニュ ーにリストされているFTDを選択します。

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		
			DbA O
Name Domain	Enrollment Type Status		
	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*: ftdvha-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			-ili-ili- cisco

Add Cert Enrollmentボタン(緑色の+記号)を選択して、新しい登録オブジェクトを作成します。 ここで、Add Cert Enrollmentウィンドウでオブジェクトの名前を割り当て、Enrollment Typeドロ ップダウンメニューからSelf Signed Certificateを選択します。

Overview Analysis Policies Devices Objects AMP	Intelligence	. I Deploy System Help ▼ dperezve ▼
Device Management Device Upgrade NAT VPN V Qo	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 configure CN, please navigate to 'Certificate Parameters' tab.	
	Allow Overrides	
	Save Can	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

最後に、自己署名証明書の場合は、共通名(CN)が必要です。Certificate Parametersタブに移動して、CNを定義します。

Overview Analysis Policies Devices Objects AMP	Intelligence			0 ₄ Deploy System Help 🔻 dperezve 🔻
Device Management Device Upgrade NAT VPN • Qo	5 Platform Settings Flex	Config Certificates		
	Add Cert Enrollment		? ×	Add *
Name Domain	Name* s	SL_SelfSigned		
	Description			
	CA Information Certif	cate 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 Nur	nber		
	Allow Overrides	J		
		- Enum	Cancel	
		24/4	Cancer	Activate Windows
				ou to system in control valier to activate withoows

SaveボタンとAddボタンをクリックします。数秒後、新しい証明書を証明書リストに追加する必要があります。

Overview Analysis	Policies Devices Obje	ects AMP Ir	ntelligence		0 ₄ Deploy System Help v dperezve
Device Management	Device Upgrade NAT	VPN VQ0S	Platform Settings FlexConfig	Certificates	
					Q Add
Name		Domain	Enrollment Type	Status	
4 📓 ftdvha-dperezve	•				≙
SSL_SelfSigned		Global	Self-Signed	O CA	± \$ \$ \$ 8

ステップ4:FMCでのローカルレルムの作成

ローカルユーザデータベース及び各パスワードは、ローカルレルムに格納される。ローカルレル ムを作成するには、System > Integration > Realmsの順に移動します。



Add Realmボタンを選択します。Add New Realmウィンドウで、名前を割り当て、Typeドロップ ダウンメニューからLOCALオプションを選択します。

Overview Analysis Policies Devices Objects AMP	Intelligence		0 Opploy System Help ▼ dperezve ▼
	Add New Realm	•×	Licenses Logging Health Monitoring Tools
Cloud Services Realmo Identity Sources High Realms Realm Sequences Sync Results	Add New Realm Name* Description AnyConnect-Local-Auth Type Local Local User Configuration Username Password Confirm Password Add another local user Confirm Password Confirm Password		Licenses • Logging • Health • Monitoring • Tools • Compare Realms: Add Realm
	Cancel	ve	
Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2		_	altala cisco

ユーザアカウントとパスワードは、Local User Configurationセクションで作成します。

✤ 注:パスワードには、大文字、小文字、数字、特殊文字が少なくとも1つ含まれている必要 があります。

Add New Realm • X Licenses * Logging * Health * Monitoring * T Monitoring * T Might Af Realms Realm Sequences Sync Results Local User Configuration deprezve Username Username Username Username Username						Ueploy S	stem Help 🔻	dperezve *
Cloud Services Realms Identity Sources High A Realms Realm Sequences Sync Results Local User Configuration Appende Username Username Compare Realms Add Realms<td></td><td>Add New Realm</td><td></td><td>θ×</td><td>Licenses 🔻</td><td>Logging • Health</td><td>• Monitoring</td><td>• Tools •</td>		Add New Realm		θ×	Licenses 🔻	Logging • Health	• Monitoring	• Tools •
Add another local user	Cloud Services Realms Identity Sources Realms Realm Sequences Sync Results	Name" AnyConnect-Local-Auth Type LocAL LocAl User Configuration deprezve Username deprezve Password Add another local user	Confirm Password		Licenses •	Logging • Health	Monitoring mpare Realms	Tools
Cancel Save Go to System in Control Panel to activate Windows Go to System in Control Panel to activate Windows			Cancel	Save		Activate Windows Go to System in Control P	anel to activate Win	ndows.

変更を保存し、Add Realmをクリックして、既存のレルムのリストに新しいレルムを追加します

Overview Analysis Policies Devices Objects AMP Intel	ligence									🔍 Deplo	System	Help 🔻 🚽	dperezve v
			Configuration	Users	Domains	Integration	SecureX	Updates	Licenses •	Logging •	Health 🔻	Monitoring	 Tools
Cloud Services Realms Identity Sources High Avail	bility oStreamer	Host Input Client	Smart Software Ma	nager On	Prom								
cloud services Reality Sources Figh Availa	binty estreamer	Host Input Chent	Smart Software Ma	nager on	Prem								
Realms Realm Sequences Sync Results													
											Compare	Realms	dd Realm
Name	Туре С	Domain	AD Primary	Domain		Ba	se DN			5	tate		
AnyConnect-Local-Auth	LOCAL C	Global									Enabled	1 +	/ 🖞 🖥

ステップ 5:SSL Cisco Secure Clientの設定

0

SSL Cisco Secure Clientを設定するには、Devices > VPN > Remote Accessの順に移動します。



Addボタンをクリックして、新しいVPNポリシーを作成します。接続プロファイルの名前を定義し、「SSL」チェックボックスを選択して、ターゲット・デバイスとしてリストされている FTDを選択します。すべてがリモートアクセスVPNポリシーウィザードのポリシー割り当てセクションで設定されている必要があります。

Overview Analysis Policies Devices Objects All Device Management Device Upgrade NAT VPN > Rei	MP Intelligence mote Access QoS Platform Settings Fi	exConfig Certificates		🍳 Deploy System Help ▼ dperezve ▼
Remote Access VPN Policy Wizard				
Policy Assignment O Connection Profile	3 AnyConnect > 4 Access & Certifica	ite > (5) Summary		
Name: * Description: VPN Protocols: Targeted Devices:	SSL_AnyConnect_LocalAuth SSL IPsec-IKEv2 Available Devices Search If fdv-dperzve If fdv-dperzve If fdv-dperzve If fdv-dperzve If fdv-dperzve If fdv-dperzve	Selected Devices	Control field water, before the character to complete Remote Access VPN Policy. Authentication Server Configure (JCGL or Realm or BADIUS Server Group or SSQ to authenticate VPN clients. Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Clicor credentials to download it during the wizard. Device Interface Interfaces should be already configured on targeted <i>dipologi</i> so that they can be used as a security zone or interface group to enable VPN access.	
				Vate Backdov's Next Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2				altalta cisco

Nextを選択して、Connection Profile設定に移動します。接続プロファイルの名前を定義し、認証 方式としてAAA Onlyを選択します。次に、Authentication Serverドロップダウンメニューで LOCALを選択し、最後にLocal Realmドロップダウンメニューでステップ4で作成したローカルレ ルムを選択します。

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 Access & Certificate S Summary			
Remote User AnyConnect Client Internet Outside VPN 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 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: V O (Realm or RADIUS)			
Accounting Server:			_
	Activate Bace dow	Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168:13.2			

同じページを下にスクロールし、IPv4 Address Poolセクションにある鉛筆アイコンをクリックして、Cisco Secure Clientが使用するIPプールを定義します。

Overview Analysis Policies Devices Objects AMP Inte	ligence	. Øg 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 Anyl	Connect 🔰 🕢 Access & Certificate 🔰 🥱 Summary						
Authent	ication Server:* LOCAL V (LOCAL or Realm or RADIUS)	•					
	Address Pools ? ×						
Author	Available IPv4 Pools C Selected IPv4 Pools						
Client Addre:	Search						
Client IP addro assignment is	ddress ddress						
Use							
Use							
Group Policy							
A group policy or create a Gr	ed. Select						
Group							
	OK						
		Back Next Cancel					
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2							

Nextをクリックして、AnyConnectセクションに移動します。ここで、ステップ2でアップロード したCisco Secure Clientイメージを選択します。

Overview Analysis Policies Devices Objects AMP Intelligence	
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 Internet Outside Very Device Inside	Corporate Resources
AAA The VPM gateway can automatically download the latest AnyConnect package to the client device when the VPM cc initiated. Minimize connection setup time by choosing the appropriate 05 for the selected package.	nnection is
Download AnyConnect Client packages from <u>Cisco Software Download Center</u> . 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 Innin on Saturday. 2021-09-04 at 14:26:07 PM from 192.168.13.2	սիսիս

Nextをクリックして、Access & Certificateセクションに移動します。Interface group/Security Zoneドロップダウンメニューで、Cisco Secure Client(AnyConnect)を有効にする必要があるイン ターフェイスを選択します。次に、Certificate Enrollmentドロップダウンメニューで、手順3で作 成した証明書を選択します。

Overvlew Analysis Policies Devices Objects AMP Intelligence	0, Deploy System H	elp v dperezve v
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 Corporate Resources		ĺ
AAA 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		
Insble 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		
A G	ctivate Backdows Next	Cancel
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2		.1]1.1]1. CISCO

最後に、Nextをクリックして、Cisco Secure Clientの設定の要約を表示します。



すべての設定が正しければ、Finishをクリックして変更をFTDに展開します。

Ov	rview	Analysis Policies Devices Objects AMP Intelligen	ce					(Deploy System Help	dperezve *
									Deployment De	ployment History
									Deploy time: Esti	nate Deploy
) (a	Search using device name, user name, type, group or status								
	۲	Device	Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status	
	> 🛛	ftdvha-dperezve	dperezve		FTD		Sep 7, 2021 2:44 PM	B	Pending	
								Activate W	indows	
								Go to System i	n Control Panel to activate W	indows.
Last	login on Si	aturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2								cisco

確認

導入が成功したら、WindowsクライアントからFTDへのCisco AnyConnectセキュアモビリティク ライアント接続を開始します。認証プロンプトで使用するユーザ名とパスワードは、ステップ4で 作成したものと同じである必要があります。

	VPN:
	S Cisco AnyConnect 10.31.124.25 ×
	Group: SSL_AnyConnect_LocalAuth ~
¢ ()	Username: dperezve
	Password: *********
	OK Cancel

クレデンシャルがFTDによって承認されると、Cisco AnyConnectセキュアモビリティクライアン トアプリケーションは接続状態を表示する必要があります。

🕙 Cisco AnyC	Connect Secure Mobility Client		—		×
	VPN: Connected to 10.31.124.25. 10.31.124.25	~	D	isconnect	t
00:00:49					IPv4
Ö ()					altalta cisco

FTDから、show vpn-sessiondb anyconnectコマンドを実行して、ファイアウォールで現在アクテ

ィブなCisco Secure Clientセッションを表示できます。

firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : dperezve : 8 Index 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 : 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 : 0h:00m:30s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000080006137dcc9 Tunnel Zone : 0 Security Grp : none

トラブルシュート

FTDでdebug webvpn anyconnect 255コマンドを実行し、FTDのSSL接続フローを確認します。

firepower# debug webvpn anyconnect 255

Cisco Secure Clientデバッグの他に、TCPパケットキャプチャでも接続フローを確認できます。 これは、接続が成功し、WindowsクライアントとFTD間の通常の3つのハンドシェイクが完了した 後、暗号の同意に使用されるSSLハンドシェイクが完了した例です。

*Ethernet1					- a ×
File Edit View Go	Capture Analyze St	atistics Telephony Wirele	ess Tools He	lp	
🖌 🔳 🌊 🛞 📘 🗖	S S 9 + + 1	S T 1 📜 🚍 🔍 🤆	a, a, 👳		
ip.addr == 10.31.124.2	25				X = +
the Trace	da an	Contraction .	Contract	and the	
13 3.331622	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 3.332733	10.31.124.25	10.31.124.34	TCP	60 443 → 51300 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460	
15 3.332833	10.31.124.34	10.31.124.25	TCP	54 51300 + 443 [ACK] Seg=1 Ack=1 Win=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 [ACK] 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 Win=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 5.497482	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	60 443 = 51300 [ACK] Seq=1169 Ack=1532 Win=32768 Len=0	
33 5,500054	10.31.124.25	10.31.124.34	TLSv1.2	594 Application Data	
34 5.500054	10.31.124.25	10.31.124.34	TLSv1.2	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	1431 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	
73 12.278473	10.31.124.25	10.31.124.34	TLSv1.2	1514 Application Data	
74 12.278473	10.31.124.25	10.31.124.34	TLSv1.2	1514 Application Data [TCP segment of a reassembled POU]	
75 12.278473	10.31.124.25	10.31.124.34	TLSv1.2	1271 Application Data	
> Frame 13+ 66 but	es on wire (\$28 hits) 66 butes cantured ((528 bits) on	interface \Device\NDF (DC144C43-8181-44CC-485F-84CFC2FFC8C9), id 0	
> Ethernet II. Scr.	1 Whate Shichies (8	0:50:56:96:c6:e8). Dst	ti Whate har	R4:a7 (00:50:56:b3:R4:a7)	
> Internet Protoco	Version 4. Sect 18	31.124.34 Dot: 10.31	1.124.25		
Transmission Con	trol Protocol Sec 8	ort: 51300 Det Port:	441 Seat 8	Lent A	
	and motorouty set i		and, seen of	Cont o	
0000 00 50 56 b3 5	04 -7 00 C0 CC 04 /	4 + 0 0 0 A 5 00 . Di		ē.	
0010 00 34 70 8f 4	40 00 50 06 00 00 0	a 1f 7c 22 Ba 1f 40		E	
0020 7c 19 c8 64 6	01 bb 94 5b 21 b4 0	0 00 00 00 50 02	d []		
0030 fa f0 0c a0 0	00 00 02 04 05 b4 0	1 03 03 08 01 01			
0040 04 02					

プロトコルのハンドシェイク後、FTDはローカルレルムに保存された情報を使用してクレデンシャルを検証する必要があります。

DARTバンドルを収集し、さらに調査するためにCisco TACに連絡します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。