FMCを介したFTD上のセキュアクライアントの AAAおよび証明書認証の設定

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>ネットワーク図</u>
<u>コンフィギュレーション</u>
<u>FMCでの設定</u>
<u>ステップ1:FTDインターフェイスの設定</u>
<u>ステップ 2:Cisco Secure Clientライセンスの確認</u>
<u>ステップ 3:ポリシー割り当ての追加</u>
<u>ステップ 4:接続プロファイルの設定の詳細</u>
<u>ステップ 5:接続プロファイル用のアドレスプールの追加</u>
<u>手順6: 接続プロファイルのグループポリシーの追加</u>
<u>手順7:接続プロファイル用のセキュアクライアントイメージの設定</u>
<u>ステップ 8:接続プロファイルのアクセスと証明書の設定</u>
<u>ステップ 9:接続プロファイルの概要の確認</u>
<u>FTD CLIで確認</u>
<u>VPNクライアントでの確認</u>
<u>ステップ1: クライアント証明書の確認</u>
<u>ステップ 2:CAの確認</u>
<u>確認</u>
<u>ステップ 1:VPN接続の開始</u>
<u>ステップ 2:FMCでのアクティブセッションの確認</u>
<u>ステップ 3:FTD CLIでのVPNセッションの確認</u>
<u>ステップ 4:サーバとの通信の確認</u>
トラブルシュート
<u>参考</u>

はじめに

このドキュメントでは、AAAおよび証明書認証を使用してFMCによって管理されるFTDでCisco Secure Client over SSLを設定する手順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。

- Cisco Firepower Management Center (FMC)
- •ファイアウォール脅威防御の仮想(FTD)
- VPN認証のフロー

使用するコンポーネント

- VMWare 7.4.1向けCisco Firepower Management Center
- ・シスコファイアウォール脅威対策の仮想7.4.1
- Cisco Secureクライアント5.1.3.62

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

組織がより厳格なセキュリティ対策を採用するにつれ、2要素認証(2FA)と証明書ベースの認証を 組み合わせることが、セキュリティを強化し、不正アクセスから保護するための一般的な方法に なってきています。ユーザエクスペリエンスとセキュリティを大幅に向上させる機能の1つは、 Cisco Secure Clientでユーザ名をあらかじめ入力する機能です。この機能により、ログインプロ セスが簡素化され、リモートアクセスの全体的な効率が向上します。 このドキュメントでは、事前に入力されたユーザ名をFTD上のCisco Secure Clientと統合し、ユ ーザがネットワークに迅速かつ安全に接続できるようにする方法について説明します。

これらの証明書には共通の名前が含まれており、認証の目的で使用されます。

- CA:ftd-ra-ca-common-name
- ・ クライアント証明書:sslVPNClientCN
- ・サーバ証明書:192.168.1.200

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。



ネットワーク図

コンフィギュレーション

FMCでの設定

ステップ1:FTDインターフェイスの設定

Devices > Device Managementの順に移動し、ターゲットFTDデバイスを編集して、Interfacesタ ブでFTDのInsideおよびOutsideインターフェイスを設定します。

GigabitEthernet0/0の場合、

- 名前:outside
- ・ セキュリティゾーン:outsideZone
- IPアドレス:192.168.1.200/24

GigabitEthernet0/1の場合、

- 名前:inside
- ・ セキュリティゾーン:insideZone
- IPアドレス:192.168.10.200/24

Firewall Management Cent Devices / Secure Firewall Interfaces	ter Overview	Analysis	Policies Devices	Objects Integration	De	ploy Q 🚱 🌣	admin v dual	SECURE	
1 49 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Sets DHCP VTEP									
All Interfaces Virtual Tunnels					Q. Search by name	S	Add Int	erfaces ¥	
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router		
Management0/0	management	Physical				Disabled	Global	۹.4	
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global	/	
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global	/	
GigabitEthernet0/2		Physical				Disabled		/	
GigabitEthernet0/3		Physical				Disabled		/	

FTDインターフェイス

ステップ 2: Cisco Secure Clientライセンスの確認

Devices > Device Managementに移動し、ターゲットFTDデバイスを編集し、DeviceタブでCisco Secure Clientライセンスを確認します。

Firewall Management Center Devices / Secure Firewall Device Summary	iew Analys	sis Policies Devices	Objects Integration		Depk	oy Q 💕 🌣 🛛	admin ~ diada	SECURE
1		License		Ø				
Device Routing Interfaces Inline Sets DHC	P VTEP	License Types Performance Tier:	FTDv5 - 100 Mbps	¥				
General	12	Essentials:			m		0	2
Name:	1. 1. 1.4	Export-Controlled Features:			:	Cisco Firepower Threat D	efense for VMware	•
Transfer Packets:	Ye	Malware Defense:					9A33F35ANSU	
Troubleshoot:	Download	IPS:				202	4-06-14 07:38:47	
Mode:	Route	Carrier:			ione:		UTC (UTC+0:00)	
Compliance Mode: Performance Profile:	Defaul	URL:			n: Zone setting for		7.4.1	
TLS Crypto Acceleration:	Disable	Secure Client Premier:			based Rules:		UTC (UTC+0:00)	
		Secure Client Advantage:						
Device Configuration: Import Exp	ort Download	Secure Client VPN Only:	0					
OnBoarding Method: Re	egistration Ke	If a device already has Secure Client VPI	N Only they cannot have					
Increasing Facility		has Secure Client Premier or Secure Client A has Secure Client Premier or Secure Clie have Secure Client VPN Only	ent Advantage it cannot		a com cont			
Inspection Engine					gement		/	
Inspection Engine:	Snort			Cancel Save	e Host Address:		1.114.0.49	,
Revert to Snort 2					dary Address:			

セキュアクライアントライセンス

ステップ3:ポリシー割り当ての追加

Devices > VPN > Remote Accessの順に移動し、Addボタンをクリックします。

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	¢ 🕹	0	admin \sim	cisco SECURE
													Add
Name				Status			Last Modified						
No configuration available Add a new configuration													

リモートアクセスVPNの追加

必要な情報を入力して、Nextボタンをクリックします。

- 名前:ftdvpn-aaa-cert-auth
- VPNプロトコル:SSL
- ・ ターゲットデバイス:1.x.x.49

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 💕 🌣 🎯 🛛 admin	* cisco SECURE
Remote Access VPN Policy Wizard Policy Assignment			
Targeted Devices and Protocols This wizard will guide you through the required minimal steps to configure the Remote Assess VPN policy with a new user-defined connection profile.	Before You Start Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy. Authentication Server Configure LOCAL or Realm or RADUS Server Group or SSO to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Claco credentials to download it during the witzard. Device Interface Interfaces should be already configured on targeted devices should be already configured on targeted devices of that they can be used as a security zone or interface group to enable VPN access.		
		Cancel Ba	ick Next

ポリシーの割り当て

ステップ4:接続プロファイルの設定の詳細

接続プロファイルに必要な情報を入力し、Local Realm項目の横にある+ボタンをクリックします 。

- 認証方式: クライアント証明書とAAA
- 認証サーバ:LOCAL
- ・ 証明書からのユーザ名:特定のフィールドのマッピング
- ・ 主フィールド:CN(共通名)
- セカンダリフィールド:OU(組織ユニット)

Firewall Management Center Overview Analysis Devices / VPN / Setup Wizard	Policies Devices Objects Integration	Deploy	٩	e <	0	$\operatorname{admin} \lor$	dude SECURE
Remote Access VPN Policy Wizard							
1 Policy Assignment 2 Connection Profile 3 Secur	Client (4) Access & Certificate (5) Summary						
	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:* ftdvpn-aaa-cert-auth						
	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: Client Certificate & AAA						
	Authentication Server:* LOCAL (LOCAL or Resim or RADUS) +						
	Local Realm:* +						
	Prefill username from certificate on user login window						
	Username From O Map specific field Use entire DN (Distinguished Name) as username						
	Primary Field: CN (Common Name)						
	Secondary Field: OU (Organisational Unit)						

接続プロファイルの詳細

新しいローカルレルムを追加するには、Add RealmドロップダウンリストからLocalをクリックします。

Firewall Management Ce Integration / Other Integrations / Re	enter Overview Analysis ealms	Policies Devices	Objects Integration			Deploy Q 🧬 🌣 😡	admin v exe SECURE
Cloud Services Realms Identity	y Sources High Availability eSt	treamer Host Input Client	Smart Software Manager On-Prem				
Realms Realm Sequences S	iync Results						
						Compare Re	alms Add Realm 🗸
Name *	Туре	Description		Status O	Value	State	Local
LocalRealmTest	Local			-		C Enabled	Active Directory/LDAP

ローカルレルムの追加

ローカルレルムに必要な情報を入力して、Saveボタンをクリックします。

- 名前: LocalRealmTest
- ・ ユーザ名:sslVPNClientCN



注:usernameは、クライアント証明書内の共通名です

Name*	Description
LocalRealmTest	
Local User Configuration	
∧ ssIVPNClientCN	
Username	
ssiVPNClientCN	
Password	Confirm Password

Add another local user

Cancel	Save	

ローカルレルムの詳細

ステップ5:接続プロファイル用のアドレスプールの追加

IPv4 Address Pools項目の横にあるeditボタンをクリックします。

Client	Address.	Assignment:
	1.000001.00000	a strate de la service de la

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only)	
Use DHCP Servers	
Jse IP Address Pools	
IPv4 Address Pools:	1
IPv6 Address Pools:	1

IPv4アドレスプールの追加

新しいIPv4アドレスプールを追加するために必要な情報を入力します。接続プロファイルの新しいIPv4アドレスプールを選択します。

- 名前:ftdvpn-aaa-cert-pool
- IPv4アドレス範囲:172.16.1.40 ~ 172.16.1.50

 $\mathbf{0} \times$

・マスク:255.255.255.0

Add IPv4 Pool

Name* ftdvpn-aaa-cert-pool		
Description		
IPv4 Address Range*		
172.16.1.40-172.16.1.50		
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150		
Mask*		
255.255.255.0		
Allow Overrides		
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices		
 Override (0) 		
	Cancel	Save
Ipv4アドレスプールの詳細		
手順 6:接続プロファイルのグループポリシーの追加		
Group Policy項目の横にある+ボタンをクリックします。		
Group Policy:		
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object. Group Policy:* Edit Group Policy		
	Cancel	Back Next
グループポリシーの追加		

0

新しいグループポリシーを追加するために必要な情報を入力します。接続プロファイルの新しい

グループポリシーを選択します。

- 名前:ftdvpn-aaa-cert-grp
- ・ VPNプロトコル:SSL

Add Group Policy

Name:* ftdvpn-aaa-cert-grp	
Description: General Secure	Client Advanced
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	VPN Tunnel Protocol: Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel. ✓ SSL ☐ IPsec-IKEv2

0



手順7:接続プロファイル用のセキュアクライアントイメージの設定

secure client image fileを選択し、Nextボタンをクリックします。

Firewall Management Center Overview A	nalysis Policies Devices Objects Integration	Deploy Q 🗳 🌣 🕢 admin 🗸 🐝 SECURE
Remote Access VPN Policy Wizard		
Policy Assignment 2 Connection Profile	Secure Client Access & Certificate S Summary	
	Remote User User	
	Secure Client Image	
	The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.	
	Download Secure Client packages from Cisco Software Download Center.	
	Show Re-order buttons +	
	Secure Client File Object Name Secure Client Package Name Operating System	
	Cisco-secure-client-win-5.1.3.6 cisco-secure-client-win-5.1.3.62-webdeplo Windows	

Cancel Back Next

Secure Client Imageの選択

ステップ8:接続プロファイルのアクセスと証明書の設定

VPN接続にSecurity Zoneを選択し、Certificate Enrollment項目の横にある+ボタンをクリックします。

・ インターフェイスグループ/セキュリティゾーン:outsideZone

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 💞 🌣 🔕 admin ~ 📫 secure												
Remote Access VPN Policy Wizard													
1 Policy Assignment (2) Connection Profile (3) Secure Client (6) Access & Certificate (5) Summary													
Renote Secure Citent Internet Outside Unice Resources													
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:* outsideZone +													
Z Enable 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.*													

セキュリティゾーンの選択

FTD証明書に必要な情報を入力し、ローカルコンピュータからPKCS12ファイルをインポートします。

- 名前:ftdvpn-cert
- ・登録タイプ:PKCS12ファイル

Add Cert Enrollment

Name*				Î
Description				
CA Information C	ertificate Paramet	ers Key Revo	ocation	
Enrollment Type:	PKCS12 File	•		
PKCS12 File*:	ftdCert.pfx		Browse PKCS12 File	
Passphrase*:				
Validation Usage:	Skin Check fr	SSL Client S	SL Server	
		a overlag in basic cor	is a units of the over ocranicate	
				ľ
				•
			Cancel Save	

FTD証明書の追加

Access & Certificateウィザードで入力した情報を確認し、Nextボタンをクリックします。

0



注:復号化されたVPNトラフィックがアクセスコントロールポリシー検査の対象になら ないように、復号化されたトラフィックに対してアクセスコントロールポリシーのバイ パス(sysopt permit-vpn)をイネーブルにします。

Firewall Management Center Overview Analysis Po Devices / VPN / Setup Wizard	Devices Objects Integration	Deploy Q 🥩 🌣 🕢 admin 🗸 👘 SECURE
Remote Access VPN Policy Wizard		
Policy Assignment 2 Connection Profile 3 Secure Clier	t Access & Certificate S Summary	
Remote User	Secure Client Internet Outside VPN Inside Corporate Resources	
	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.* OutsideZone Enable 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.* ftdvpn-cert +	
	Enroll the selected certificate object on the target devices	
	Access Control for VPN Traffic	
	All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.	
	Pypass Access Control policy for decrypted traffic (sysopt permit-ypn) This option bypasses the Access Control Policy issuescion, but VPM filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.	
<		•
		Cancel Back Next

```
アクセスと証明書の設定の確認
```

ステップ9:接続プロファイルの概要の確認

VPN接続のために入力した情報を確認し、Finishボタンをクリックします。

<form> Image: Second problem (Second problem) Image: Second problem) Image: Second problem) Image: Second problem (Second problem) Image: Second problem) Image: Second problem) Image: Second problem (Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem) Image: Second problem)</form>	Firewall Management Center Overview: Analysis Policies De Devices / VPN / Setup Wizard	vices Objects Integration		Deploy Q 💕 🌣 🌚	admin v diada SECU
Remote Access VPN Policy Configuration Additional Configuration Requirements Image: <	Remote Access VPN Policy Wizard 1) Policy Assignment 2) Connection Profile 3) Secure Client 4	Access & Certificate Summary			
Frewall Management Center will configure an RA VPN Policy with the following settings: Atter the wizard completes, the following completes, the following completes to be completed for VPN to with the following settings: Name: Indon-max-cent-with Connection Profile: Buyon-max-cent-with Connection Profile: Buyon-max-cent-with AAA: Connection Profile: Buyon-max-cent-with AAA: Connection Profile: Buyon-max-cent-with Automication Method: Clearmane From Centificate: COUP completes & AAA Uterrame From Centificate: Clearmane From Centificate: COUP completes & Configuration Automication Serve: - - Address Pools (IPV): - To resolve hostname specified in AAA. Servers or CAS Servers; configuration Address Pools (IPV): - To resolve hostname specified in AAA. Servers or CAS Servers; configuration Address Pools (IPV): - - Group Policy: Mather-max-cent-word: Ski, will be mateled on port 443 Policy Centificates: mayon-cent Mather face Configuration Mather face Configuration - - Mather face configuration - - Oris colve hostname specified in AAA. Servers	Remote Access VPN Policy	/ Configuration	Additional Configuration Requirements		
DHCP Servers: - Address Pools (IP-4): Rdrynn-saa-cert-pool Address Pools (IP-4): Rdrynn-saa-cert-grp Group Policy: Rdrynn-saa-cert-grp Secure Client Images: group-saa-cert-grp Interface Objects: outsideZone Device Mentity Certificate Enrollment mover - secure - sec	Firewall Management Center will of Name: Device Targets: Connection Profile: Connection Alias: AAA: Authentication Method: Username From Certifica Authentication Server: Authorization Server: Accounting Server: Address Assignment: Address from AAA:	onfigure an RA VPN Policy with the following settings Rdypn-aaa-cert-auth 1, 3.49 Rdypn-aaa-cert-auth Rdypn-aaa-cert-auth Client Certificate & AAA CC (Common Name) & GU (Organisational Unit) LocalRealmTest (Local) -	After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets. • Access Control Policy Update An Access Control rule must be defined to allow VPN traffic on all targeted devices. • NAT Exemption If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic. • DNS Configuration To resolve hostname specified in AAA Servers or CA Servers, configure DNS using PiexConfig Device on the targeted devices.		
Address Polos (IPv): - Group Policy: Rdyn-saa-cert-grp Secure Client Images: disco-secure-client-win-5.1.3.62-webdeploy-k9.a.g. Interface Objects: outsideZone Device Certificate Involue-cert Certificate enrollment object Tddyn-cert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finshing the wizard. Go to the <u>Certificate Involue-cert</u> is not installed on one or more targeted devices to the <u>Certificate Involue-cert</u> is not installed on the installation. Secure Certificate Involue-cert is not installed on the installation. Secure Certificate Involue-certificate Involue-cerificate Involue-certificate Involue-certificate Involu	DHCP Servers: Address Dools (IDvd.)	- ftdvpn-aaa-cert-pool	Port Configuration		
Interface Objects: outsideZone Device Certificates: It dvpn-cert Device Identity Certificate Enrollment Certificate enrollment object 'fidvpn-cert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the <u>Certificates page to check the status of the installation</u> .	Address Pools (IPv6): Group Policy: Secure Client Images:	- ftdvpn-aaa-cert-grp cisco-secure-client-win+5.1.3.62-webdeploy-k9.pk	SSL will be enabled on port 443. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.		
Device Certificates: Indvpri-cert Make sure to add interface from targeted devices to SecurityZone object 'outsideZone' Device Identity Certificate Enrollment Certificate enrollment object 'fit/wpri-cert' is not installed on one or more targeted devices on finishing the wizard. Go to the Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the Certificate page to check the status of the installation. Advector	Interface Objects:	outsideZone	Network Interface Configuration		
Certificate encloses of those certificates page to check the status of the installation.	Device Certificates:	Rdvpn-cert	Make sure to add interface from targeted devices to SecurityZone object 'outsideZone'		
	Certificate enrollment abject "fiday devices. Certificate installation will wizzard. Go to the <u>Certificates</u> page	in-cert' is not installed on one or more targeted be initiated on the targeted devices on finishing the to check the status of the installation.			
	<				

VPN接続の設定の確認

リモートアクセスVPNポリシーの概要を確認し、設定をFTDに展開します。

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Int	tegration	Deploy 🔍 💕 🌣 🌘	admin ~ dudu SECURE
ftdvpn-aaa-cert-auth				Save Cancel
Enter Description				A ()
				Policy Assignments (1)
Connection Profile Access Interfaces Advanced			Local Realm: LocalRealmTest	Dynamic Access Policy: None
				+
Name	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication; None Authorization; None Accounting: None	DftrGepPolicy		/1
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	📑 ftdvpn-aaa-cert-grp		/1

リモートアクセスVPNポリシーの概要

FTD CLIで確認

FMCからの展開後に、FTD CLIでVPN接続設定を確認します。

// Defines IP of interface interface GigabitEthernet0/0 nameif outside security-level 0 ip address 192.168.1.200 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 0 ip address 192.168.10.200 255.255.255.0 // Defines a pool of addresses ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0 // Defines a local user username sslVPNClientCN password ***** encrypted // Defines Trustpoint for Server Certificate crypto ca trustpoint ftdvpn-cert keypair ftdvpn-cert crl configure // Server Certificate Chain crypto ca certificate chain ftdvpn-cert certificate 22413df584b6726c 3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7 quit certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 quit // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client

enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows" anyconnect enable tunnel-group-list enable cache disable error-recovery disable // Bypass Access Control policy for decrypted traffic // This setting is displayed in the 'show run all' command output sysopt connection permit-vpn // Configures the group-policy to allow SSL connections group-policy ftdvpn-aaa-cert-grp internal group-policy ftdvpn-aaa-cert-grp attributes banner none wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-tunnel-network-list none default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable // Configures the tunnel-group to use the aaa & certificate authentication tunnel-group ftdvpn-aaa-cert-auth type remote-access tunnel-group ftdvpn-aaa-cert-auth general-attributes address-pool ftdvpn-aaa-cert-pool default-group-policy ftdvpn-aaa-cert-grp // These settings are displayed in the 'show run all' command output. Start authentication-server-group LOCAL secondary-authentication-server-group none

no accounting-server-group default-group-policy ftdvpn-aaa-cert-grp username-from-certificate CN OU secondary-username-from-certificate CN OU authentication-attr-from-server primary authenticated-session-username primary username-from-certificate-choice second-certificate secondary-username-from-certificate-choice second-certificate // These settings are displayed in the 'show run all' command output. End tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes authentication aaa certificate pre-fill-username client group-alias ftdvpn-aaa-cert-auth enable

VPNクライアントでの確認

ステップ1:クライアント証明書の確認

Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント 証明書を確認します。

🚘 Console1 - [Console Root\Certificates - Curren	t User\Personal\Certificates]				-	٥	\times
Eile Action View Favorites Window	<u>H</u> elp					-	8 ×
🗢 🔶 🙇 📷 🛍 🖬 🙆 📷						_	
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Actions	
Gertificates - Current User Berropal	SsIVPNClientCN	ftd-ra-ca-common-name	6/16/2025	Client Authentication	ssIVPNClientCer	Certificate	es 🔺
Certificates						More	• •
Inusted Koot Certification Authorities							
Certificates							
> iii Enterprise Trust							
						1	

クライアント証明書の確認

クライアント証明書をダブルクリックし、Detailsに移動して、Subjectの詳細を確認します。

• 件名:CN = sslVPNClientCN

🕵 Certificate

General	Details	Certification Pa	ath	
Show:	<al></al>		\sim	
Field			Value	^
Sig	nature al	gorithm	sha256RSA	
Sig	nature ha	ash algorithm	sha256	
Sel Iss	uer		ftd-ra-ca-common-name, Cisc	
🔄 🔛 Vali	d from		Sunday, June 16, 2024 6:12:0	
C Val	id to		Monday, June 16, 2025 6:12:	
🔤 Sut	oject	actor management	ssiVPNClientCN, ssiVPNClientO	
Put	жскеу		RSA (2048 Bits)	
- Po I	die kev na	arameterc	05.00	v
O = Cis L = Tok S = Tok C = JP	co yo yo			
		[Edit Properties Copy to File.	
			C	ж

X

クライアント証明書の詳細

ステップ 2:CAの確認

Certificates - Current User > Trusted Root Certification Authorities > Certificatesの順に移動し、認

• 発行元:ftd-ra-ca-common-name

 Console1 - [Console Root\Certificates - Currer File Action View Favorites Window 	nt User\Trusted Root Certification A Help	Authoritie&Certificates]			-	5 ×	×
 Console Root Certificates - Current User Personal Certificates Certificate Certification Authorities Active Directory User Object Trusted Publishers Untrusted Certificates Trusted People Client Authentication Issuers Smart Card Trusted Roots Certificates (Local Computer) 	Issued To COMODO RSA Certificati Copyright (c) 1997 Micros EDESKTOP-VCKHRG1 DigiCert Assured ID Root DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert High Assurance DigiCert High Assurance DigiCert Trusted Root G4 DigiCert Trusted Root G4 DigiCert Trusted Root G4 ClobalSign	Issued By COMODO RSA Certificati Copyright (c) 1997 Micros DESKTOP-VCKHRG1 DigiCert Assured ID Root DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert High Assurance DigiCert Trusted Root G4 DigiCert Trusted Root G4 DigiCert CAX3 ftd=ra-ca-common-name ClobalEign GlobalSign	Expiration Date 1/18/2038 12/30/1999 10/30/2022 11/9/2031 11/9/2031 11/9/2031 11/9/2031 11/9/2031 11/9/2031 11/9/2031 11/9/2031 1/15/2038 0/30/3031 6/16/2029 2/19/2030 12/15/2021	Intended Purposes Client Authenticati Time Stamping Server Authenticati (All> Client Authenticati Client Authenticati (All> Client Authenticati Client Authenticati Client Authenticati Client Authenticati Client Authenticati	Friendly Nan ^ Sectigo (forr Microsoft Tii www.infraey <none> DigiCert DigiCert DigiCert Glol <none> DigiCert DigiCert Tru: DCT Rest Ct <none> CtobalCy Google Trust</none></none></none>	Actions Certificates More ftd-ra-ca More	• > • >

CAの確認

確認

ステップ1:VPN接続の開始

エンドポイントで、Cisco Secure Client接続を開始します。ユーザ名はクライアント証明書から 抽出されるため、VPN認証用のパスワードを入力する必要があります。



注:ユーザ名は、このドキュメントのクライアント証明書のCN(共通名)フィールドから抽出されたものです。

Sisco Secure Client	- 0	×	S Cisco Secure Client 192.168.1.200 X	<	Sisco Secure Client	-		×
AnyConnect VPIE Contacting 192.168.1.200. 192.168.1.200	 ✓ Connect 	_	Group: [tdvpn-saa-cert-auth ~]		AnyConnect VPN: Connected to 192.168.1.200. 192.168.1.200		Disconnect	_
			Password:		00:00:07		1	Pv4
\$ ()		alaala cisco			\$			ultudu cisco
			OK Cancel					

VPN接続の開始

ステップ2:FMCでのアクティブセッションの確認

Analysis > Users > Active Sessionsの順に移動し、VPN認証のアクティブセッションを確認します。

Einewall Management Center Analysis Polcies Devices Objects Integration Depiny Q 💞 Q 🕒 admin v dates Sessions													at secure			
	Switch to legacy UI															
T	lelect													×	Refresh	Log Out
0	bowing the 1 and only session	<u>+</u>			_											E
	Losin Time	Realm/Username	Last Seen 4	Authentication.Type	Current IP	Baales	Usemane	ErstName	Last Name	Email	Department	Phone Number	Discovery, Application	Desice		^
	2024-06-17 11:38:22	LocalRealmTest(ssIVPNClientCN	2024-05-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	ss/VPNClientCN						LDAP	1		

アクティブセッションの確認

ステップ3: FTD CLIでのVPNセッションの確認

FTD(Lina)CLIで show vpn-sessiondb detail anyconnectコマンドを実行して、VPNセッションを確認します。

ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7 Assigned IP: 172.16.1.40 Public IP: 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14780 Bytes Rx : 15386 Pkts Tx: 2 Pkts Rx: 37 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth Login Time : 02:38:22 UTC Mon Jun 17 2024 Duration: 0h:01m:22s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb00718200007000666fa19e Security Grp: none Tunnel Zone: 0

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1

AnyConnect-Parent: Tunnel ID : 7.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50035 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client OS ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7390 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 7.2 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS_AES_128_GCM_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 50042 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 7390 Bytes Rx : 2292 Pkts Tx : 1 Pkts Rx : 3 Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel: Tunnel ID : 7.3 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56382 UDP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62 Bytes Tx : 0 Bytes Rx : 13094 Pkts Tx : 0 Pkts Rx : 34 Pkts Tx Drop : 0 Pkts Rx Drop : 0

ステップ4:サーバとの通信の確認

VPNクライアントからサーバへのpingを開始し、VPNクライアントとサーバ間の通信が成功することを確認します。

C:\Users\CALO>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data: Reply from 192.168.10.11: bytes=32 time=12ms TTL=128 Reply from 192.168.10.11: bytes=32 time=87ms TTL=128 Reply from 192.168.10.11: bytes=32 time=3ms TTL=128 Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Ping statistics for 192.168.10.11: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 3ms, Maximum = 87ms, Average = 26ms

*ping*に成功

パケットキャプチャを確認するには、FTD(Lina)CLIでcapture in interface inside real-timeコマンドを実行します。

<#root>

```
ftd702#
```

capture in interface inside real-time

Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request 2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply 3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request 4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply 5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request 6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply 7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request 8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo request

トラブルシュート

VPN認証に関する情報は、Linaエンジンのdebug syslogおよびWindows PCのDARTファイルに記載されています。

次に、Linaエンジンのデバッグログの例を示します。

// Certificate Authentication

Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=ssIV Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked. Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=ssIVPNClientCl

// Extract username from the CN (Common Name) field

Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5] Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 5]

// AAA Authentication

Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

これらのデバッグは、設定のトラブルシューティングに使用できる情報を提供するFTDの診断CLIから実行できます。

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

参考

<u>モバイルアクセス用のAnyconnect証明書ベース認証の設定</u>

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。