# FDMを介したFTDでのセキュア・クライアント 認証のための証明書照合の構成

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>
ネットワーク図
<u> <b> </b></u>
<u>・ ニー・ テレー・</u> ステップ1:FTDインターフェイスの設定
ー <u>ステップ 2:Cisco Secure Clientライセンスの確認</u>
<u>ステップ 3:アドレスプールの追加</u>
<u>ステップ4:セキュアクライアントプロファイルの作成</u>
<u>ステップ 5:FDMへのセキュア・クライアント・プロファイルのアップロード</u>
<u>手順6: グループポリシーの追加</u>
<u>手順 7:FTD証明書の追加</u>
<u>ステップ 8:FTDへのCAの追加</u>
<u>ステップ9: リモートアクセスVPN接続プロファイルの追加</u>
<u>ステップ 10: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:VPNクライアントへのセキュアなクライアントプロファイルのコピー</u>
<u>ステップ2:クライアント証明書の確認</u>
<u>ステップ 3:CAの確認</u>
確認
ステップ 1:VPN接続の開始
ー <u>ステップ 2:FTD CLIでのVPNセッションの確認</u>
トラブルシュート
関連情報

## はじめに

このドキュメントでは、認証に証明書照合を使用して、FDMを介してFTD上でSSLを使用する Cisco Secure Client(CSC)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。

- Cisco Firepower Device Manager(FDM)仮想
- •ファイアウォール脅威対策(FTD)仮想
- VPN認証のフロー

#### 使用するコンポーネント

- Cisco Firepower Device Manager(FDM)仮想7.2.8
- ・シスコファイアウォール脅威対策の仮想7.2.8
- Cisco Secureクライアント5.1.4.74
- プロファイルエディタ(Windows) 5.1.4.74

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

CertificateMatchは、管理者がVPNサーバとの認証用のクライアント証明書を選択するために使用 する必要がある基準を設定できるようにする機能です。この設定はクライアントプロファイルで 指定されます。クライアントプロファイルは、プロファイルエディタを使用して管理するか、手 動で編集できるXMLファイルです。CertificateMatch機能を使用すると、特定の属性を持つ証明書 のみがVPN接続に使用されるようにすることで、VPN接続のセキュリティを強化できます。

このドキュメントでは、SSL証明書の共通名を使用してCisco Secure Client(CSA)を認証する方法 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
- エンジニアVPNクライアント証明書:vpnEngineerClientCN
- マネージャVPNクライアント証明書:vpnManagerClientCN
- 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

FDMでの構成

ステップ1:FTDインターフェイスの設定

Device > Interfaces > View All Interfacesの順に移動し、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
- IPアドレス: 192.168.1.200/24

Firewall Device Manager Monitoring Policies	Objects Device: firep	power			idmin v vili Administrator cis	SECURE
Device Summary Interfaces						
Cisco Firepower Threat Defense for ViMware	MGMT					
Interfaces Virtual Tunnel Interfaces						
9 Interfaces			<b></b>	<b>T</b> Filter		+
NAME	LOGICAL NAME	STATUS MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> 🗸 GigabitEthernet0/0	outside	Routed	192.168.1.200 Static		Enabled	

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

Device > Smart License > View Configurationの順に移動し、RA VPN License項目のCisco Secure Clientライセンスを確認します。



セキュアクライアントライセンス

### ステップ3:アドレスプールの追加

Objects > Networksに移動し、+ボタンをクリックします。

Firewall Device Manag	ger Monitoring Policies Objects Device:	firepower	(). (i)	E
Object Types ←	Network Objects and Groups 7 objects		Y Filter Preset filters: System deficed. User deficed	ļ
Ports     Security Zones     Apollection Elitere	NOME     IPv4-Private-10.0.0.0-8	TYPE VALUE NETWORK 10.0.0/8	ACTIONS	

アドレスプールの追加

必要な情報を入力して新しいIPv4アドレスプールを追加します。OKボタンをクリックします。

- 名前:ftd-cert-match-pool
- タイプ:範囲
- IP範囲: 172.16.1.150 ~ 172.16.1.160

# Add Network Object

Name
ftd-cert-match-pool
Description
Type Network Host FQDN Range
IP Range
172.16.1.150-172.16.1.160
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

0

 $\times$ 

CANCEL	ОК	

Ipv4アドレスプールの詳細

#### ステップ4:セキュアクライアントプロファイルの作成

Secure Client Profile Editorを<u>Ciscoソフトウェア</u>サイトからダウンロードしてインストールします 。 Server Listに移動し、Addボタンをクリックします。 必要な情報を入力してServer List Entryを 追加し、OKボタンをクリックします。

- 表示名:cert-match
- FQDNまたはIPアドレス: 192.168.1.200
- プライマリプロトコル: SSL

references (Part 1) references (Part 2)	Server List Profile: Untit	led									
ackup Servers Certificate Pinning Certificate Matching Certificate Enrollment	Hostname	Host Addr	User Group	Backup Ser	SCEP	Mobile Sett	Certificate				
	Note: it is hi	ighly recommer	ided that at lea	ast one server t	e define <mark>r</mark> II	Ad D	el				
						Server List	Entry Balancing Ser	rvers SCEP Mobile C	ertificate Pinning		
						Primary	Server		Connection Informati	on	
						Display	Name (requir	ed) cert-match	Primary Protocol	SSL	
						192.16	8.1.200		Auth Method Du	ring IKE Negotiation EAP-	AnyConnec
						Group	URL		IKE Identity (IOS	gateway only)	
						192.16	8.1.200				
								Backup Servers			
								Host Address		Add	
										Move Up	
										Move D	
										Delete	
						_					

サーバリストエントリ

Certificate Matchingに移動し、Addボタンをクリックします。 必要な情報を入力して識別名エン トリを追加し、OKボタンをクリックします。

- 名前 : CN
- ・パターン:vpnEngineerClientCN
- 演算子:等しい



注:このドキュメントの「MatchCase」オプションをチェックしてください。

Help								
VPN Preferences (Part 1)	Certificate	Matching	3\OneDrive	- Cisco\Des	kton/wnnCli	ient yml		
Certificate Matching Certificate Matching Certificate Matching Certificate Enrollment Mobile Policy Server List	Key Usag Dec End CRL Key Dat Key Dat Key Dat	e pher_Only _Sign _Cert_Sign _Agreem _Endpher _Endpher _Repudiat tal_Signa		xtended Key ServerA ClientAi CodeSig EmailPr IPSecTr IPSecTu IPSecUs TimeSta OCSPSi	y Us with gn rotect ndSystem unnel ser amp gn	DVCS	iate	
	Custom E	xtended Mat	ch Key (Ma. Add Delete				Section Distin	guished Name Entry > CN  vpnEngineerClient
	Mate Mate Distinguis	th only certific th only certific thed Name (N	icates with F icates with F Max	Key Usage Extended Ke	y Usage	Add	Operator	Equal Order Not Equal ord Case
	Name	Pattern	windcard	Operator	matchC	Edit		OK Cancel

識別名エントリ

#### セキュアクライアントプロファイルをローカルコンピュータに保存し、プロファイルの詳細を確 認します。



セキュアなクライアントプロファイル

#### ステップ 5 : FDMへのセキュア・クライアント・プロファイルのアップロード

Objects > Secure Client Profileの順に移動し、CREATE SECURE CLIENT PROFILEボタンをクリックします。

Firewall Device Manager Monitoring	g Policies Objects Device: firepower	(>) (admin Administrator	cisco SECURE
Óbject Types ←	Secure Client Profiles		
C Networks		<b>F</b> ilter	+
与 Ports	# NAME	FILE NAME ACTIONS	
🔒 Security Zones			
🐬 Application Filters		There are no Secure Client profile objects yet.	
C <sup>2</sup> URLs		Start by creating the first Secure Client profile object.	
© Geolocations		CREATE SECURE CLIENT PROFILE	
Syslog Servers			
✗ IKE Policies			
🐴 IPSec Proposals			
Secure Client Profil			
🚭 Identity Sources			

セキュアクライアントプロファイルの作成

必要な情報を入力してセキュアなクライアントプロファイルを追加し、OKボタンをクリックしま す。

- 名前: secureClientProfile
- セキュアクライアントプロファイル:secureClientProfile.xml(ローカルコンピュータからのアップロード)

# Add Secure Client Profile

Name		
secureClientProfile		
Description		
Secure Client Profile UPLOAD secureClientProfile.xml		
	CANCEL	ОК
セキュアクライアントプロファイルの追加		

0

Х

手順6:グループポリシーの追加

Device > Remote Access VPN > View Configuration > Group Policiesの順に移動し、+ボタンをク リックします。

Firewall Device Ma	anager Monitoring Policies Objects	Device: firepower	$(\Sigma)$	🚔 💿 ? :	admin Administrator	secure
RA VPN ←	Device Summary Group Policies					
Connection Profiles	2 objects			<b>T</b> Filter		+
SAML Server	# NAME	ONS SERVER	IPV4 SPLIT TUNNELING	IPV6 SPLIT TUNNELING	SECURE CLIENT PROFILES	ACTIONS
	1 DfltGrpPolicy		Allow all traffic	Allow all traffic		

グループポリシーの追加

グループポリシーの追加に必要な情報を入力し、OKボタンをクリックします。

- 名前:ftd-cert-match-grp
- ・ セキュアクライアントプロファイル: secureClientProfile

## Add Group Policy

-		•
		,
-		

Q. Search for attribute	Name
Basic General Session Settings	ftd-cert-match-grp Description
Advanced Address Assignment Split Tunneling	DNS Server Select DNS Group
Secure Client Traffic Filters Windows Browser Proxy	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session Secure Client profiles
	CANCEL

グループポリシーの詳細

#### 手順7:FTD証明書の追加

Objects > Certificatesの順に移動し、Add Internal Certificate from +をクリックします。

Firewall Device Man	ager Monitoring Policies Objects Device: fi	repower	🕞 🚑 🕲 ? : 🕯	dmin dministrator
Object Types ←	Certificates			
C Networks	121 objects		<b>T</b> Filter	+ × 🔍 🖓 ×
S Ports			Preset filters: System defined, User defined	Add Internal CA
Security Zones	II NAME	туре		Add Internal Certificate ACTIONS
Application Filters	1 AAA-Certificate-Services	Trusted CA Certificate		Add Trusted CA Certificate
<b>62</b> 1101 e	2 ACCVRAIZ1	Trusted CA Certificate		
C UNLS	3 Actalis-Authentication-Root-CA	Trusted CA Certificate		
Geolocations	4 AffirmTrust-Commercial	Trusted CA Certificate		
Syslog Servers	5 AffirmTrust-Networking	Trusted CA Certificate		
🔏 IKE Policies	6 AffirmTrust-Premium	Trusted CA Certificate		
🏫 IPSec Proposals	7 AffirmTrust-Premium-ECC	Trusted CA Certificate		
Secure Client Profiles	8 Amazon-Root-CA-1	Trusted CA Certificate		
aldentity Sources	9 Amazon-Root-CA-2	Trusted CA Certificate		
Ilsers	10 Amazon-Root-CA-3	Trusted CA Certificate		
	11 DefaultInternalCertificate	Internal Certificate		
\$2 Certificates	12 DefaultWebserverCertificate	Internal Certificate		

内部証明書の追加

Upload Certificate and Keyをクリックします。

## Choose the type of internal certificate you want to create



証明書とキーのアップロード

FTD証明書に必要な情報を入力し、証明書と証明書キーをローカルコンピュータからインポートして、OKボタンをクリックします。

- 名前:ftd-vpn-cert
- ・ 特殊サービスの検証用途:SSLサーバ

## Add Internal Certificate



Ø

Х

内部証明書の詳細

ステップ8:FTDへのCAの追加

Objects > Certificatesの順に移動し、Add Trusted CA Certificate from +をクリックします。

Firewall Device Manager	Monitoring Policies Objects Device: fireport	wer $(b)$ (b) (c) $(c)$ (c	dmin dministrator
🐬 Application Filters	Cartificates		
C URLs	Certificates		
Geolocations	120 objects	<b>T</b> Filter	+ 🖌 🗐 🗸
Derlag Generation		Preset filters: System defined. User defined	Add Internal CA
Sysiog Servers	# NAME	туре	Add Internal Certificate ACTIONS
🔏 IKE Policies	1 NGFW-Default-InternalCA	Internal CA	Add Trusted CA Certificate
👍 IPSec Proposals	2 AAA-Certificate-Services	Trusted CA Certificate	
Secure Client Profiles	3 ACCVRAIZ1	Trusted CA Certificate	
Surces	4 Actalis-Authentication-Root-CA	Trusted CA Certificate	
1 Users	5 AffirmTrust-Commercial	Trusted CA Certificate	
2 Certificates	6 AffirmTrust-Networking	Trusted CA Certificate	
	7 AffirmTrust-Premium	Trusted CA Certificate	
- Secret Keys	Allert Trans Branchase FOO	T	

信頼済みCA証明書の追加

### CAに必要な情報を入力し、ローカルコンピュータから証明書をインポートします。

- 名前:ftdvpn-ca-cert
- 特殊サービスの検証用途:SSLクライアント

Add Trusted CA Certificate	3 ×
Name ftdvpn-ca-cert	
Certificate Paste certificate, or choose a file (DER, PEM, CRT, CER)	ftd-ra-ca.crt Upload.Certificate
BEGIN CERTIFICATE MIIDbDCCA1SgAwIBAgIIUkKgLg229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChMF	- - 
Skip CA Certificate Check	
Validation Usage for Special Services	
SSL Client ×	~
CANCEL	ок

#### ステップ9:リモートアクセスVPN接続プロファイルの追加

Device > Remote Access VPN > View Configuration > Connection Profilesの順に移動し、 CREATE CONNECTION PROFILEボタンをクリックします。

Firewall Device Man	ager Monitoring	Ø Policies	다. Objects	Device: firepower	6	)		?	e admin Adminis	trator	cisco SECURE
RA VPN ←		Device Summary Remote A	ccess V	PN Connection Profile	S						
Group Policies							<b>T</b> Filt	ter			+
📱 SAML Server		# N	IAME	AAA	GROUP POLICY				ACTIO	45	
				Th	ere are no Remote Access Start by creating the first	Connectio Connectio	ns yet. n.				
					CREATE CONNECTION	PROFILE					

リモートアクセスVPN接続プロファイルの追加

接続プロファイルに必要な情報を入力し、Nextボタンをクリックします。

- 接続プロファイル名:ftd-cert-match-vpn
- ・認証の種類:クライアント証明書のみ
- ・ 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(Organizational Unit)
- ・ IPv4アドレスプール:ftd-cert-match-pool

Firewall Device Manager Monitoring Policies	Notes         Device: firepower	⊘ ⓐ Ø ? : admin Administrator ✓ cusco SECURE
Remote Access VPN	Connection and Client     Configuration     Configuration     Configuration	3 Global Settings 4 Summary
Remote Users 📃 🖂 Secure Cit	ents — Marinet	INTERVACES
	Connection and Client Config Specify how to authenticate remote users and the secure clients th inside network.	uration rey can use to connect to the
	Connection Profile Name This name is configured as a connection alias, it can be used to connect to the Vi ftd-cert-match-vpn	PN gateway
	Group Alias (one per line, up to 5) Group URL (one ftd-cert-match-vpn	per line, up to 5)
	Primary Identity Source Authentication Type Client Certificate Only	
	Username from Certificate  Map Specific Field  Primary Field  CN (Common Name)  V  OU (Organisation	onal Unit) ~
	Use entire DN (distinguished name) as username     Advanced	
	Authorization Server Accounting Server Please select V Please select	~
	Client Address Pool Assignment IPv4 Address Pool Endpoints are provided an address from this pool	d an address from this pool
	CANCEL	

VPN接続プロファイルの詳細

グループポリシーに必要な情報を入力し、Nextボタンをクリックします。

・ グループポリシーの表示:ftd-cert-match-grp

Firewall Device Manager Monitoring Policies Objects	Device: firepower		<ul> <li>alialis SECURE</li> </ul>
Remote Access VPN	Connection and Client     Configuration     Remote User Experience	3 Global Settings 4 Summary	
Remote Users     E     Secure Cli	ents — Internet — Q Client Certificate — OUT Set It Da ACE	INFORMER	rces
	Remote User Experience A group policy is a collection of user-oriented session attributes whis VPN connection is established. Select or create a Gro View Group Policy fid-cert-match-grp Policy Group Brief Details ONS + DANNER	e h are assigned to client when a p Policy object.	
	DNS Server None Barrour Text for Authentic BACK NEXT		

グループポリシーの選択

Certificate of Device Identity、Outside Interface、Secure Client Package for VPN connectionの順 に選択します。

- デバイスIDの証明書: ftd-vpn-cert
- ・外部インターフェイス:外部(GigabitEthernet0/0)
- ・ セキュアクライアントパッケージ: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



注:このドキュメントのNAT免除の機能は無効になっています。

Firewall Device Manager Monitoring Policies C	Device: firepower	Admin admin Administrator	RE
Remote Users	Client Certificate ···· OUTSIDE	INSOE INTERFACES	
	Global Settings These settings control the basic functioning of the connection. Cf apply to all connection profiles; you cannot configure different is	changes to any of these options settings in different profiles.	
Ce	rtificate of Device Identity ttd-vpn-cert (Validation Usinge: SSL Se > outside (Giga	abitEthernet0/0)	
Ful ¢.9	ly-qualified Domain Name for the Outside Interface , ravpn.example.com	Port 443 e.g. 8080	
Ac Det pol and	cess Control for VPN Traffic crypted VPN traffic is subjected to access control policy inspection by defaul (by for decrypted traffic option bypasses the access control policy, but for re- the authorization ACL downloaded from the AAA server are still applied to V Bypass Access Control policy for decrypted traffic (sysopt perm	ilt. Enabling the Dypass Access Control emote access VPN, the VPN Filter ACL VPN traffic mit-vpn)	
	AT Exempt		
Se If a Inst You You	secure Client Package user does not already have the right secure client package installed, the syst aller when the client authenticates for the first time. The user can then install a can download secure client packages from software clience.	stem will launch the secure client il the package from the system.	
Pa	UPLOAD PACKAGE V	-	
	BACK NEXT		

グローバル設定の詳細

ステップ 10: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。

þ	Firewall Device Manager	Monitoring	Policies	iii: Objects	Device: firepower	$\odot$	۲	?	÷	admin Administrator	Ŷ	cisco SECURE

#### Summary

Review the summary of the Remote Access VPN configuration.

STEP 1: CONNECTION AND CLIENT CONDICIDATION		
Primary Identity Source		
Authentication Type	Client Certificate Only	
Polenne Identite Course		
Primary identity source		
Fallback Local Identity Source	-	
Username from Certificate	Map Specific Field	
Primary Field	CN (Common Name)	
Secondary Field	OU (Organisational Unit)	
Advanced		
Authorization Server		
Accounting Server		
IPv4 Address Pool Assignment	C ftd-cert-match-pool	
IPv6 Address Pool	°a -	
DHCP Servers	-	
STEP 2: GROUP POLICY		
Group Bolicu Nama	@ Brivert-match-on	
Banner + DNS Server	na	
DNS Server	a -	
Ranner text for authenticated allocate	-	
Session Settings	-	
Maximum Connection Time / Alert Internal	Unlimited / 1 minutes	
Ide Timeout / Alext Interval	30 / 1 minutes	
Rune remedut / Avent Interval	997 T 100000	
simuitaneous Login per User Split Tunneling	a	
Ibut Solit Tunneling	Allow all traffic over tunnel	
in the open furthering	Allow all reaffic over tunnel	
eve spic runneing Secure Client	Among all traffic over tunner	
Secure Client Profiles	C secureClientProfile	
STEP 3: GLOBAL SETTINGS		
Certificate of Device Identity	@ ftd-vpn-cert	
Outside Interface	GioabitEthemet0/0 (outside)	
Fully multified Demole Many for the Original		
runy-qualified Domain Name for the Outside Interface	-	
Port	443	
Access Control for VPN Traffic	No	
NAT Exempt		
NAT Exempt	No	
Inside Interfaces	-	
Inside Networks	-	
Secure Client Package		
Packages	III Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg	

接続プロファイルの概要の確認

### FTD CLIで確認

FDMから展開した後、FTD CLIでVPN接続設定を確認します。

// Defines IP of interface interface GigabitEthernet0/0 speed auto nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.1.200 255.255.255.0 // Defines a pool of addresses ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftd-vpn-cert enrollment terminal keypair ftd-vpn-cert crl configure // Server Certificate crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client crl configure // CA crypto ca certificate chain ftdvpn-ca-cert 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:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2 anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml anyconnect enable tunnel-group-list enable cache disable error-recovery disable

// Configures the group-policy to allow SSL connections

group-policy ftd-cert-match-grp internal group-policy ftd-cert-match-grp attributes 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-dns none split-tunnel-all-dns disable client-bypass-protocol disable msie-proxy method no-modify vlan none address-pools none ipv6-address-pools none webvpn anyconnect ssl dtls none anyconnect mtu 1406 anyconnect ssl keepalive none anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client none anyconnect dpd-interval gateway none anyconnect ssl compression none anyconnect dtls compression none anyconnect modules none anyconnect profiles value secureClientProfile type user anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication tunnel-group ftd-cert-match-vpn type remote-access tunnel-group ftd-cert-match-vpn general-attributes address-pool ftd-cert-match-pool default-group-policy ftd-cert-match-grp tunnel-group ftd-cert-match-vpn webvpn-attributes authentication certificate group-alias ftd-cert-match-vpn enable

#### VPNクライアントでの確認

ステップ1: VPNクライアントへのセキュアなクライアントプロファイルのコピー

VPNクライアントとマネージャのVPNクライアントを設計するために、セキュアなクライアント プロファイルをコピーします。



注:Windowsコンピュータのセキュアクライアントプロファイルのディレクトリ : C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

📕 🛛 🔁 📕 🗢 🗍 Profil	e				
File Home	Share	View			
← → × ↑ 📙	> Thi	s PC → Local Disk (C:) → Program	mData → Cisco → Cisco Secure Clie	nt > VPN > Profile	ن م
- Quick access		Name	Date modified	Туре	Size
Desktop	*	MgmtTun	€, _ J/2024 20:15	File folder	
Downloads	*	AnyConnectProfile vsd     secureClientProfile	6/ ., 2024 21:44 7 12,	XSD File XML Document	97 KB 4 KB
🚼 Documents	*				

VPNクライアントへのセキュアなクライアントプロファイルのコピー

ステップ2:クライアント証明書の確認

VPN Clientエンジニアで、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。



エンジニア用VPN Clientの証明書の確認

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 = vpnEngineerClientCN

Certificate	×
General Details Certification P	Path
Show: <all></all>	$\sim$
Field	Value ^ Wednesday, June 18, 2025 5:
Public key parameters	RSA (2048 Bits) 05 00
Key Usage	Digital Signature, Key Encipher Client Authentication (1.3.6.1
Thumborint algorithm	cha1
CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	
	Edit Properties Copy to File
	OK

技術士免状の内容

マネージャのVPN Clientで、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 - Current User\Personal\Certificates] σ × \_ - 8 × 🖀 Eile Action View Favorites Window Help 🗢 🔿 🙍 📅 🛍 🙆 📭 📓 📷 Console Root Issued To Issued By Expiration Date Intended Purposes Actions 🤿 Certificates - Current User 🖏 vpn Manager Client CN ftd-ra-ca-common-name 6/19/2025 **Client Authentication** Certificates . Personal More Actions ۶ Certificates Certificates > 🔛 Enterprise Trust

Manager VPN Clientの証明書の確認

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 = vpnManagerClientCN

CAR /	*
Field	Value /
- untit to	Thursday, June 19, 2025 9:41
Subject	vpnManagerClientCN, vpnMan
PUDIC KEY	RSA (2048 Bits)
Public key parameters	05 00
🗊 Key Usage	Digital Signature, Key Encipher
Enhanced Key Usage	Client Authentication (1.3.6.1
Netscape Comment	xca certificate
Thumhorint aborithm	cha1
N = vppMacacerClaptCN	
av - vprividnøger cilenterv	
) = Cisco	1
. = Tokyo S = Tokyo	
C = JP	
	Edit Properties Copy to File

Х

ステップ 3:CAの確認

👔 Certificate

エンジニアのVPNクライアントとマネージャのVPNクライアントの両方で、Certificates - Current User > Trusted Root Certification Authorities > Certificatesの順に移動し、認証に使用するCAを確 認します。

• 発行元: ftd-ra-ca-common-name

🖀 Console1 - [Console Root\Certificates - Current	User\Trusted Root Certification A	uthorities\Certificates]			(-)	٥	>	<
🚡 Eile Action View Favorites Window	Help						- 8	×
🗢 🔿 🙍 📷 🔏 🖦 🗶 🖼 🔒	1							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Action	s	
Certificates - Current User	2127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati	duo-endpoir	Certifi	cates	
V Personal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AAJ	м	ore	
A Trusted Post Castification Authorities	🔄 Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt		010	
Certificates	Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-	ca	•
Ceruncates	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	M	ore	•
> Intermediate Certification Authorities	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Tii			
> Active Directory User Object	DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati	www.infraey			
> Trusted Publishers	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	<all></all>	<none></none>			
> Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert			
> 🧾 Third-Party Root Certification Authoriti	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert			
> Constant People	🔄 DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Glol			
> Client Authentication Issuers	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	<all></all>	<none></none>			
> Smart Card Trusted Roots	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	Client Authenticati	DigiCert			
> 🗇 Certificates (Local Computer)	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Trus			
	E DOCT Doub CA V2	DCT D CA YO	2/30/2021	Client Authenticati	DST Root CA			
	🕎 ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<all></all>	<none></none>			
	Egrolobaloign	olooabign	3/18/2029	Client Authenticati	GlobalSign R			
CAの確認								

CAの唯認



#### ステップ1:VPN接続の開始

エンジニアのVPNクライアントで、Cisco Secure Client接続を開始します。ユーザ名とパスワー ドを入力する必要はなく、VPNは正常に接続されました。

S Cisco Secure Client − □ ×	S Cisco Secure Client   cert-match X	Sisco Secure Client	- 🗆 X
AnyConnect VPIL Your client certificate will be used for authentication cert-match v Connect	Your clent certificate will be used for authentication Group: ftd-cert-match-vpn V	AnyConnect VPII: Connected to cert-match. cert-match	V Disconnect
	OK Cancel	00:00:06	IPv4
Cate de la cate		¢ ()	-shada. Cisco

エンジニアのVPN ClientのVPN接続に成功しました

マネージャのVPNクライアントで、Cisco Secure Client接続を開始します。証明書の検証エラー が原因で、VPNの接続に失敗しました。



Manager VPN ClientのVPN接続の失敗

#### ステップ2: FTD CLIでのVPNセッションの確認

エンジニアのVPNセッションを確認するためにFTD(Lina)CLIでshow vpn-sessiondb detail anyconnectコマンドを 実行します。

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32 Assigned IP: 172.16.1.150 Public IP: 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 Bytes Tx : 14718 Bytes Rx : 12919 Pkts Tx: 2 Pkts Rx: 51 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn Login Time : 05:42:03 UTC Tue Jul 2 2024 Duration: 0h:00m:11s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000200006683932b Security Grp: none Tunnel Zone: 0

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

AnyConnect-Parent: Tunnel ID : 32.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50170 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.17763 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 32.2 Assigned IP : 172.16.1.150 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 50177 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 12919 Pkts Tx : 1 Pkts Rx : 51 Pkts Tx Drop : 0 Pkts Rx Drop : 0

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コンピュータのDARTファイルに記載されています。

次に、エンジニアクライアントからのVPN接続中のLinaエンジンのデバッグログの例を示します。

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClient Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

#### 関連情報

<u>Firepower 2100用のFDM On-Box Management Serviceの設定</u> FDMによって管理されるFTDでのリモート・アクセスVPNの構成 Firepower Device Manager(FDM)でのsyslogの設定と確認</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。