为通过FDM的FTD上的安全客户端身份验证配置 证书匹配

目录
先决条件
<u>要求</u>
使用的组件
<u>背景信息</u>
FDM中的配置
<u>- 5</u>
<u>第四步:创建安全客户端配置文件</u>
<u>第五步:将安全客户端配置文件上传到FDM</u>
<u>第六步:添加组策略</u>
步骤 7.添加FTD证书
步骤 8将CA添加到FTD
步骤 9添加远程访问VPN连接配置文件
<u>步骤 10确认连接配置文件的摘要</u>
在FTD CLI中确认
在VPN客户端中确认
步骤1:将安全客户端配置文件复制到VPN客户端
<u>第二步:确认客户端证书</u>
<u>第三步:确认CA</u>
<u>验证</u>
<u>步骤1:启动VPN连接</u>
<u>第二步:在FTD CLI中确认VPN会话</u>
<u>故障排除</u>
<u>相关信息</u>

简介

本文档介绍如何使用证书匹配进行身份验证,通过FDM在FTD上设置带SSL的Cisco安全客户端。

先决条件

要求

Cisco 建议您了解以下主题:

- Cisco Firepower设备管理器(FDM)虚拟
- 防火墙威胁防御(FTD)虚拟
- VPN身份验证流程

使用的组件

- 思科Firepower设备管理器虚拟7.2.8
- 思科防火墙威胁防御虚拟7.2.8
- 思科安全客户端5.1.4.74
- 配置文件编辑器(Windows) 5.1.4.74

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

CertificateMatch是一项功能,允许管理员配置客户端必须用来选择客户端证书以使用VPN服务器进 行身份验证的条件。此配置在客户端配置文件中指定,它是可使用配置文件编辑器管理或手动编辑 的XML文件。CertificateMatch功能可用于增强VPN连接的安全性,方法是确保仅将具有特定属性的 证书用于VPN连接。

本文档介绍如何使用SSL证书中的公用名对Cisco安全客户端进行身份验证。

这些证书中包含用于授权目的的公用名称。

- CA : ftd-ra-ca-common-name
- 工程师VPN客户端证书:vpnEngineerClientCN
- 管理器VPN客户端证书:vpnManagerClientCN
- 服务器证书: 192.168.1.200

网络图

下图显示本文档示例中使用的拓扑。



网络图

配置

FDM中的配置

步骤1:配置FTD接口

导航到Device > Interfaces > View All Interfaces,在Interfaces选项卡中配置FTD的内部和外部接口 。

对于GigabitEthernet0/0,

- 名称 : outside
- IP地址: 192.168.1.200/24

Firewal	I Device Manager Mor	mitoring Policies	Objects	Device: firepowe	ər		(Σ)		?	:	admin Administrator	~	cisco SECURE
	Device Summary Interfaces												
	Cisco Firepower Threat Defen 0/0 0/1 0/2 0/3	ase for VMware ①	MGMT CONSOLE										
	Interfaces Virtual Tunnel	Interfaces											
	9 Interfaces							Ţ R	lter				+
	NAME		LO	GICAL NAME	STATUS	MODE	IP ADDRESS		STANDBY A	DORESS	MONITO	r for ha	ACTIONS
	> 🗸 GigabitEthernet0/0		ou	tside		Routed	192.168.1.200 Static				Enabled		

FTD接口

第二步:确认思科安全客户端许可证

导航到设备>智能许可证>查看配置,确认RA VPN许可证项目中的思科安全客户端许可证。

Firewall De	evice Manager Monitoring Policies Objects Device: firepower	5. (admin Administrator v tisse SECURE
SL	UBSCRIPTION LICENSES INCLUDED	
	Threat EVABLE	Malware ENABLE Disabled by user
	This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.	This license lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
	Includes: 🍄 Intrusion Policy	Includes: C _P File Policy
	URL License EVABLE	RA VPN License Type VPN ONLY V DISABLE
	This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Apex license.
	Includes: URL Reputation	Includes: RA-VPN

第三步:添加地址池

导航到对象>网络,点击+按钮。

Firewall Device Mana	ger Monitoring Policies Objects Device	: firepower	() () () () () () () () () () () () () (cisco SECURE
Object Types ←	Network Objects and Groups			
C Networks	7 objects		Y Filter	+ 🕫
S Ports			Preset filters: System defined, User defined	
Security Zones	* NAME	TYPE VALUE		ACTIONS
Application Silters	1 IPv4-Private-10.0.0.0-8	NETWORK 10.0.0/8		

添加地址池

输入必要信息以添加新的IPv4地址池。单击OK 按钮。

- 名称 : ftd-cert-match-pool
- 类型:范围
- IP范围:172.16.1.150-172.16.1.160

Add Network Object	8	×
Name ftd-cert-match-pool		
Description		
		4
Туре		
◯ 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		

CANCEL

第四步:创建安全客户端配置文件

从<u>思科软件</u>站点下载并安装安全客户端配置文件编辑器。 导航到Server List,单击Add按钮。 输入 必要信息以添加服务器列表条目,然后单击OK按钮。

- 显示名称 : cert-match
- FQDN或IP地址: 192.168.1.200
- 主要协议:SSL

Hostname Host Addr User Group Backup Ser SCEP Mobile Sett Certificate Note: It is highly recommended that at least one server be define It Ad Det Det Server List Entry Server List Entry Server List Entry Server List Entry Formary Server Connection Information Primary Protocol SSL Image: Server Load Balancing Servers FQDN or IP A User Group Acth Method During IKE Negotilation EAP-AnyCd ItE Identity (IOS gateway only) 192.168.1.200 ItE Identity (IOS gateway only) Ib2.168.1.200 Move Up Move Up Move Up Move Up Move Up	Part 1) Profile: Untitle	ed					
Note: It is highly recommended that at least one server be define It Ad Det Server List Entry Server List Entry Server Load Balancing Servers SCEP Mobile Certificate Pinning Primary Server Connection Information Display Name (required) cert-match Primary Protocol SSL Ige: Connection Information Primary Protocol SSL Ige: Connection Information Primary Protocol SSL Ige: Load Balancing Servers Auth Method During IKE Negotiation EAP-AnyCol IRE: Identity (IOS gateway only) Ige: Identity (IOS gateway only) Ige: Load Balacup Servers Move Up Move Up Move Up	ers nning atching nrollment	Host Addr User Grou	p Backup Ser	SCEP	Mobile Sett Certificate		
Server Load Balanding Servers SCEP Mobile Certificate Pinning Primary Server Load Balanding Servers SCEP Mobile Certificate Pinning Primary Protocol SSL FQDN or IP A User Group Auth Method During IKE Negotiation EAP-AnyCol IKE Identity (IOS gateway only) 192.168.1.200 Backup Servers Host Address Add Move Up Nove D	Note: it is his	ghly recommended that at	least one server b	e define li	Ad Del Det		
Primary Server Connection Information Display Name (required) cert-match Primary Protocol SSL FQDN or IP A User Group 192.168.1.200 / Group URL IXE Identity (IOS gateway only) 192.168.1.200 Move Up Move Up Move Up Move D Move Up					Server List Entry Server Load Balancing	Servers SCEP Mobile Ce	rtificate Pinning
Backup Servers Host Address Add Move Up Move D					Primary Server Display Name (req FQDN or IP A 192.168.1.200 Group URL	uired) cert-match User Group	Connection Information Primary Protocol SSL Connection Information Connection Information Connection Information Connection Information IKE Identity (IOS gateway only)
Host Address Add Add Move Up Move D						Backup Servers	
Move Up Move D						Host Address	Add
Move D							Move Up
							Move D

服务器列表条目

导航到证书匹配,单击添加按钮。 输入必要信息以添加可分辨名称条目,然后单击OK按钮。

- 名称:CN
- 模式:vpnEngineerClientCN
- 运算符:等于



注意:选中本文档中的MatchCase选项。

File Help	or - VPN						
VPN Preferences (Part 1) Preferences (Part 2)	Certificate Profile: C:	Matching Users\jianzh3	OneDrive	- Cisco\Des	ktop\vpnCli	ent.xml	
Preferences (Part 2) Backup Servers Certificate Display Certificate Matching Server ficate Consiment Mobile Policy Server List	Key Usaq Deci Enci CRL Key Data Key Non Digi	e jpher_Only _Sign _Cert_Sign _Agreem _Endpher _Endpherm _Repudiat tal_Signa	E	xtended Key Server A ClientAu CodeSig EmailPr IPSecEr IPSecUs TimeSta OCSPSi	y Us wuth uth otect ndSystem unnel ser amp gn	DVCS	ıte
	Custom E	xtended Matc	h Key (Ma. Add Delete				Distinguished Name Entry X Name CN Pattern vpnEngineerClient
	Distinguis	ch only certific ch only certific hed Name (M	cates with K cates with E l ax	Key Usage Extended Ke	y Usage		Operator Ocual Not Equal
	Name	Pattern	Wildcard	Operator	MatchC	Edit Delete	OK Cancel

可分辨名称条目

将安全客户端配置文件保存到本地计算机,并确认配置文件的详细信息。

L

▼ <certificatematch></certificatematch>	SW: +DK11>
<pre> v<distinguishedname> v<distinguishednamedefinition matchcase="Enabled" operator="Example: CN</Name> <Pattern>vpnEngineerClientCN</Pattern> </DistinguishedNameDefinition> </DistinguishedName> </pre></td><td>qual" wildcard="Disabled"></distinguishednamedefinition></distinguishedname></pre>	
	able="feloe">
* senableAutomaticServerSelection UserControlis false	able= talse >
<pre><autoserverselectionimprovement>20<autoserverselectionsuspendtime>4 <retainvpnonlogoff>false <captiveportalremediationbrowserfailover>fal <allowmanualhostinput>true v<serverlist></serverlist></allowmanualhostinput></captiveportalremediationbrowserfailover></retainvpnonlogoff></autoserverselectionsuspendtime></autoserverselectionimprovement></pre>	rverSelectionImprovement> verSelectionSuspendTime> > se nput>
<pre></pre>	

安全客户端配置文件

第五步:将安全客户端配置文件上传到FDM

导航到对象>安全客户端配置文件,单击创建安全客户端配置文件按钮。

Firewall Device Manager Monitoring	Policies Objects Device: firepower	(b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	dialle SECURE
Object Types ←	Secure Client Profiles		
C Networks		T Filter	+
S Ports	# NAME	FILE NAME ACTIONS	
Security Zones			_
🐬 Application Filters		There are no Secure Client profile objects yet.	
€ ² URLs		Start by creating the first Secure Client profile object.	
© Geolocations		CREATE SECURE CLIENT PROFILE	
Syslog Servers			
✗ IKE Policies			
🛖 IPSec Proposals			
Secure Client Profil			
s Identity Sources			

创建安全客户端配置文件

输入必要信息添加安全客户端配置文件,并单击OK按钮。

- 名称 : secureClientProfile
- 安全客户端配置文件:secureClientProfile.xml(从本地计算机上传)

Add Secure Client Profile		•	9	×
Name secureClientProfile				
Description				
				,
UPLOAD secureClientProfile.xml				
	CANCEL		эк	
		<u></u>		

第六步:添加组策略

导航到Device > Remote Access VPN > View Configuration > Group Policies,点击+按钮。

Firewall Device M	anager Monitoring Policies Objects	Device: firepower	\odot	۵ ? :	admin Administrator	cisco SECURE
RA VPN ←	Device Summary Group Policies					
Connection Profiles	2 objects			T Filter		+
SAML Server	# NAME	ONS SERVER	IPV4 SPLIT TUNNELING	IPV6 SPLIT TUNNELING	SECURE CLIENT PROFILES	ACTIONS
	1 DfltGrpPolicy		Allow all traffic	Allow all traffic		

添加组策略

输入必要信息添加组策略,然后单击OK按钮。

- 名称:ftd-cert-match-grp
- 安全客户端配置文件:secureClientProfile

Add Group Policy		0	×
Q Search for attribute	Name		
Basic	ftd-cert-match-grp Description		
Session Settings			11
Advanced Address Assignment	DNS Server Select DNS Group		,
Split Tunneling Secure Client	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session		
Traffic Filters Windows Browser Proxy	Secure Client profiles		
	▼ Filter		
	Create new Secure Client Profile CANCEL		
	CANCEL	ОК	

组策略详细信息

步骤 7.添加FTD证书

导航到对象>证书,在+项目中单击添加内部证书。

Firewall Device Ma	nager Monitoring Policies Objects Device:	lirepower	So € Ø ? : A	imin dministrator · · · · · · SECURE
Object Types ←	Certificates			
C Networks	121 objects		Y Filter	+ -
S Ports			Preset filters: System defined, User defined	Add Internal CA
Security Zones	II NAME	Түре		Add Internal Certificate ACTIONS
Application Filters	1 AAA-Certificate-Services	Trusted CA Certificate		Add Trusted CA Certificate
- D 100 -	2 ACCVRAIZ1	Trusted CA Certificate		
CP URLS	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		
Identity Sources	9 Amazon-Root-CA-2	Trusted CA Certificate		
Linere	10 Amazon-Root-CA-3	Trusted CA Certificate		
Users	11 DefaultInternalCertificate	Internal Certificate		
옷 Certificates	12 DefaultWebserverCertificate	Internal Certificate		

添加内部证书

单击Upload Certificate and Key。



上传证书和密钥

输入FTD证书的必要信息,从本地计算机导入证书和证书密钥,然后单击OK按钮。

- 名称:ftd-vpn-cert
- 特殊服务的验证使用情况:SSL服务器

Add Internal Certificate



Ø

X

步骤 8将CA添加到FTD

导航到对象>证书,在+项目中单击添加受信任CA证书。

Firewa	II Device Manager	Monitoring	Ø Policies	⇔ Objects	Device: firepor	wer		0	?	:	admin Administrator	 viluilu cisco 	SECURE
🐬 Application	Filters 🔷	Cartificat	taa										
🖉 URLs		Certifical	les										
Geolocation	5	120 objects					T Filter	Sustana dafa	and these	affered		+ ~	.
Svslog Serv	ers						Preset niters: 8	AC208000104800	1999 - 50997.5	921009254	Add Interna	I CA	
		# NAME				TYPE					Add Interna	Certificate	ACTIONS
IKE Policies		1 NGFW-I	Default-Interr	halCA		Internal CA					Add Trustee	d CA Certificate	1
👍 IPSec Propo	sals	2 AAA-Ce	ertificate-Ser	vices		Trusted CA Certificate							
Secure Clier	t Profiles	3 ACCVR/	AIZ1			Trusted CA Certificate							
🚉 Identity Sou	ces	4 Actalis-	Authenticatio	on-Root-CA		Trusted CA Certificate							
👤 Users		5 AffirmTi	rust-Commer	cial		Trusted CA Certificate							
Q Certificates		6 AffirmT	rust-Network	ing		Trusted CA Certificate							
0.0000		7 AffirmTi	rust-Premium	n		Trusted CA Certificate							
Secret Keys				500		T							

添加受信任CA证书

输入CA的必要信息,从本地计算机导入证书。

- 名称:ftdvpn-ca-cert
- 特殊服务的验证用法:SSL客户端

Add Trusted CA Certificate	0 ×
Name ftdvpn-ca-cert	
Certificate Paste certificate, or choose a file (DER, PEM, CRT, CER)	ftd-ra-ca.crt Upload.Certificate
BEGIN CERTIFICATE MIIDbDCCA1SgAwIBAgIIUkKgLg229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1U BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChM	E F
Skip CA Certificate Check	
Validation Usage for Special Services	
SSL Client ×	~
CANCEL	ОК

步骤 9添加远程访问VPN连接配置文件

导航到Device > Remote Access VPN > View Configuration > Connection Profiles,单击CREATE CONNECTION PROFILE按钮。

Firewall Device M	anager Monitoring	Policies	:#코 Objects	Device: firepower	(Σ)			admin Administrato	 v diale SECU 	IRE
RA VPN ←		Device Summary Remote A	, ccess \	/PN Connection Profiles						
Group Policies							F ilter			+
SAML Server		•	NAME	***	GROUP POLICY			ACTIONS		
				There	are no Remote Access Con	nections	yet.			
				s	tart by creating the first Con	nection.	1			
				Ľ			1			

添加远程访问VPN连接配置文件

输入连接配置文件的必要信息,然后单击Next按钮。

- 连接配置文件名称:ftd-cert-match-vpn
- Authentication Type: 仅客户端证书
- Username From Certificate:映射特定字段
- 主字段:CN(公用名)
- 辅助字段: OU(组织单位)
- IPv4地址池:ftd-cert-match-pool

Firewall Device Manager Monitoring Policies	승규는 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	> 🚔 🐵 🕐	admin Administrator
Remote Access VPN	Connection and Client C Remote User Ex Configuration	perience 3 Global Settings	(4) Summary
Remote Users 📃 Secure Cl	ents — internet	AND	Corporate Resources
	Connection and Client Specify how to authenticate remote users and the secu- inside network.	Configuration re clients they can use to connect to the	
	Connection Profile Name This name is configured as a connection alias, it can be used to con ftd-cert-match-vpn	sect to the VPN gateway	
	Group Allas (one per line, up to 5) Group ftd-cert-match-vpn	URL (one 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	ndary Field (Organisational Unit) ~	
	 Use entire DN (distinguished name) as username Advanced 		
	Authorization Server Accoun Please select Y Pleas	ting Server ie select V	
	Client Address Pool Assignment IPv4 Address Pool Endpoints are provided an address from this pool Chapter and the pool Chapter and the pool	tiress Pool s are provided an address from this pool	
	DHCP Servers * CANCEL	р а	

VPN连接配置文件的详细信息

输入组策略的必要信息,然后单击Next按钮。

• 查看组策略:ftd-cert-match-grp

Firewall Device Manager Monitoring Policies Objects	Device: firepower	So admin Administrator - state SECUS	RE
Remote Access VPN	Connection and Client Configuration Remote User Experience	3 Global Settings 4 Summary	
Remote Users Euro Cl	ierts — Internet — R Client Certificate — OUT Set	FIREPOWER	
	Remote User Experience A group policy is a collection of user-oriented session attributes whi VPN connection is established. Select or create a Gro View Group Policy ftd-cert-match-grp Policy Group Brief Details	CE hich are assigned to client when a roup Policy object.	
	DNS + BANNER DNS Server None	Edit	
	Banner Text for Authentic BACK NEXT		

选择组策略

为VPN连接选择Certificate of Device Identity、Outside Interface、Secure Client Package。

- 设备身份证书:ftd-vpn-cert
- 外部接口:外部(GigabitEthernet0/0)
- 安全客户端软件包:cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



注意:本文档中禁用了NAT免除功能。

Firewall Device Manager Monitoring Policies Objects	Device: firepower	cisco SECURE
Remote Users Secure Clients - Internet	Client Certificate	
These setting apply to all	Global Settings s control the basic functioning of the connection. Changes to any of these options connection profiles; you cannot configure different settings in different profiles.	
Certificate of Dev ftd-vpn-cert (vice Identity Outside Interface Validation Usage: SSL Se Validation for the Outside Interface Data Name for the Outside Interface Port	
e.g. ravpn.example.	com e.g. 8080	
Decrypted VPN train policy for decrypted and the authorizatio	is subjected to access control policy inspection by default. Enabling the Bypass Access Control Irraffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL n ACL downloaded from the AAA server are still applied to VPN traffic ess Control policy for decrypted traffic (sysopt permit-vpn)	
NAT Exempt	L Baskaga	
If a user does not al installer when the C You can download s You must have the r	r autorgice instance client package installed, the system will launch the secure client fiera authencicates for the first time. The user can then install the package from the system. secure client packages from software.cisco.com (2. secessary secure client software license.	
Packages UPLOAD PAC	CKAGE v ico-secure-client-win-5.1.4.74-webdeploy-k9.pkg	
	BACK	

全局设置的详细信息

步骤 10确认连接配置文件的摘要

确认输入的VPN连接信息,然后单击FINISH按钮。

þ	Firewall Device Manager	Monitoring	Policies	0bjects	Device: firepower	\odot	۲	?	÷	admin Administrator	Ŷ	cisco SECURE

Summary

Review the summary of the Remote Access VPN configuration.

STEP 1: CONNECTION AND CLIENT CONFIGURATIO	N	
Primary Identity Source		
Authentication Type	Client Certificate Only	
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 Client Address Pool Assignment		
Pv4 Address Pool	C ftd-cert-match-pool	
Pv6 Address Pool	5 -	
DHCP Servers	-	
STEP 2: GROUP POLICY		
Group Policy Name	ĝ [®] ftd-cert-match-grp	
Banner + DNS Server		
DNS Server	1 -	
Banner text for authenticated clients	-	
Session Settings		
Maximum Connection Time / Alert Interval	Unlimited / 1 minutes	
dle Timeout / Alert Interval	30 / 1 minutes	
Simultaneous Login per User	3	
Split Tunneling		
Pv4 Split Tunneling	Allow all traffic over tunnel	
Pv6 Split Tunneling	Allow all traffic over tunnel	
Secure Client Denflor		
STEP 3: GLOBAL SETTINGS		
Certificate of Device Identity	@_ftd-vpn-cert	
Outside Interface	GigabitEthernet0/0 (outside)	
Fully-qualified Domain Name for the Outside		
nterface		
Port	443	
Access Control for VPN Traffic	No	
	No	
na caunpt	194	
inside interfaces	-	
Inside Networks Secure Client Package	-	
Packages	Windows; cisco-secure-client-win-5.1.4.74-webdeploy-k9.nkg	
ge #		

确认连接配置文件的摘要

在FTD CLI中确认

从FDM部署后,在FTD CLI中确认VPN连接设置。

// 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

在VPN客户端中确认

步骤1:将安全客户端配置文件复制到VPN客户端

将安全客户端配置文件复制到工程师VPN客户端和管理器VPN客户端。



注意:Windows计算机中安全客户端配置文件的目录:C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

📕 🛛 🛃 🗸 🕴 Profile	e					
File Home	Share	View				
← → · ↑ 📙	> Thi	s PC > Local Disk (C:) > Program[Data > Cisco > Cisco Secure Clier	nt > VPN > Profile		v ₽
- Quick access		Name	Date modified	Туре	Size	
Desktop	*	MgmtTun	€, _ ∋/2024 20:15	File folder	07.10	
👆 Downloads	*	secureClientProfile	6/., 2024 21:44 712, 2024 10:48	XSD File XML Document	97 KB 4 KB	
🗎 Documents	*					

将安全客户端配置文件复制到VPN客户端

第二步:确认客户端证书

在工程师VPN客户端中,导航到证书-当前用户>个人>证书,检查用于身份验证的客户端证书。



确认工程师VPN客户端的证书

双击客户端证书,导航到详细信息,检查主题的详细信息。

• 主题:CN = vpnEngineerClientCN

Certificate	×
General Details Certification	Path
Show: <all></all>	\sim
Field	Value Vednesday, June 18, 2025 5:
Public key parameters	vpnEngineerClientCN, vpnEngl RSA (2048 Bits) 05.00
Enhanced Key Usage	Digital Signature, Key Encipher Client Authentication (1.3.6.1
Netscape Comment Thumborint algorithm	sha1
CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	
	Edit Properties Copy to File
	OK

工程师客户端证书的详细信息

在Manager VPN Client中,导航到Certificates - Current User > Personal > Certificates,检查用于 身份验证的客户端证书。 Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

🚡 Eile Action View Favorites Window Help

🗢 ᆃ 🙇 🚾 🛍 🖻 📴 🖪	1					
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Actions	
Certificates - Current User	Supprime and the second	ftd-ra-ca-common-name	6/19/2025	Client Authentication	Certificates 4	•
Certificates					More Actions	•
> Enterprise Trust						

or ×

- 8 ×

_

确认Manager VPN客户端的证书

双击客户端证书,导航到详细信息,检查主题的详细信息。

• 主题:CN = vpnManagerClientCN

how: <all></all>	\sim	
Field	Value	^
- total	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 algorithm	cha 1	Y
CN = vpnManagerClientCN O = Cisco L = Tokyo S = Tokyo C = JP		I
	Edit Properties Copy to File	

Х

Manager客户端证书的详细信息

👔 Certificate

第三步:确认CA

在工程师VPN客户端和管理器VPN客户端中,导航到证书-当前用户>受信任的根证书颁发机构>证 书,检查用于身份验证的CA。

• 颁发者:ftd-ra-ca-common-name

Eile Action View Favorites Window	Help					- 61 2
🕨 🔿 🙍 📷 🖌 👘 🖌 📰 🕞 🖬						
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions
Certificates - Current User	2 127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati	duo-endpoir	Certificates 4
V Personal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AA/	More I
	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt	more P
 Inusted Root Certification Authorities Certificater 	Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-ca 🔺
Certificates	🔄 COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	More)
Intermediate Certification Authorities	Gopyright (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>	
> iii 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	
> Trusted 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	
		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	Giobaloign	3/18/2029	Client Authenticati	GlobalSign R	

验证

步骤1:启动VPN连接

在工程师VPN客户端中,启动Cisco安全客户端连接。无需输入用户名和密码,VPN连接成功。

S Cisco Secure Client − □ ×	S Cisco Secure Client cert-match X	S Cisco Secure Client	- 🗆 X
AnyConnect VPI: Your clent certificate will be used for authentication cert-match Connect	Your clent certificate will be used for authentication Group: ftd-cert-match-upn	AnyConnect VPII: Connected to cert-match. cert-match	V Disconnect
	OK Cancel	00:00:06	IPv4
🔅 🕕 🕴		¢ ()	-dhada Cisco

工程师VPN客户端的VPN连接成功

在管理器VPN客户端中,启动Cisco安全客户端连接。由于证书验证失败,VPN连接失败。

S Cisco Secure Client			\times	Cisco Secure Client	\times
AnyConnect VPN: Certificate Validation Failure cert-match	~	Connect	-	Certificate Validation Failure]
	- ×		alaala.		

第二步:在FTD CLI中确认VPN会话

在FTD (Lina) CLI中运行show vpn-sessiondb detail anyconnect命令,确认工程师的VPN会话。

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 : 000000000000006683932b 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

故障排除

您可以在Lina引擎的调试syslog和Windows计算机上的DART文件中找到有关VPN身份验证的信息。

这是从工程师客户端进行VPN连接期间Lina引擎中的调试日志示例。

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

相关信息

<u>为Firepower 2100配置FDM机上管理服务</u> 在FDM管理的FTD上配置远程访问VPN 配置并验证Firepower设备管理器中的系统日志

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。