通过FDM为FTD上的安全客户端配置AAA和证书 身份验证

目录
<u>先决条件</u>
· · · · · · · · · · · · · · · · · · ·
<u>使用的组件</u>
<u>背景信息</u>
<u>网络图</u>
配置
FDM中的配置
<u>步骤1:配置FTD接口</u>
<u>第二步:确认思科安全客户端许可证</u>
<u>第三步:添加远程访问VPN连接配置文件</u>
<u>第四步:为连接配置文件添加地址池</u>
<u>第五步:添加连接配置文件的组策略</u>
<u>第六步:为连接配置文件配置设备身份证书和外部接口</u>
步骤 7.为连接配置文件配置安全客户端映像
步骤 8确认连接配置文件的摘要
步骤 9将用户添加到LocalIdentitySource
<u>步骤 10将CA添加到FTD</u>
在FTD CLI中确认
在VPN客户端中确认
<u>步骤1:确认客户端证书</u>
<u>第二步:确认CA</u>
<u>验证</u>
<u>第二步:在FTD CLI中确认VPN会话</u>
<u>第三步:确认与服务器的通信</u>
<u>故障排除</u>
相关信息

简介

本文档介绍在由FDM管理的FTD上使用AAA和证书身份验证配置SSL上的Cisco安全客户端的步骤。

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

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

Firepower设备管理器(FDM)是一个基于Web的简化管理界面,用于管理Cisco Firepower威胁防御 (FTD)设备。通过Firepower设备管理器,网络管理员无需使用更复杂的Firepower管理中心(FMC)即 可配置和管理其FTD设备。FDM为基本操作(如设置网络接口、安全区域、访问控制策略和 VPN)以及监控设备性能和安全事件提供了直观的用户界面。它适用于需要简化管理的中小型部署 。

本文档介绍如何将预填充的用户名与FDM管理的FTD上的Cisco安全客户端集成。 如果您使用FMC管理FTD,请参阅<u>通过FMC在FTD上配置安全客户端的AAA和证书身份验证</u>指南。

这是证书链,带有文档中使用的每个证书的公用名称。

- CA : ftd-ra-ca-common-name
- 客户端证书:sslVPNClientCN
- 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。



配置

FDM中的配置

步骤1:配置FTD接口

导航到设备(Device) >接口(Interfaces) >查看所有接口(View All Interfaces),在接口(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

对于GigabitEthernet0/1,

- 名称 : inside
- IP地址: 192.168.10.200/24

Firewall Device Manager Monitoring Policies Objects	Device: firepor	ver		\odot	0	?	÷	admin Administrat	or	~	cisco SECU	RE
Device Summary Interfaces												
Cisco Firepower Threat Defense for VMware												
9 Interfaces					▼ R	ter						+
NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS		STANDBY A	DORESS	мо	ITOR FO	R HA	ACTION	s
> 🗸 GigabitEthernet0/0	outside		Routed	192.168.1.200 State				Ena	bled			
> V GigabitEthernet0/1	inside		Routed	192.168.10.200				Ena	bled			

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,在RA VPN许可证中确认Cisco安全客户端许可证项目。



安全客户端许可证

第三步:添加远程访问VPN连接配置文件

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

Firewall Device M	anager Monitoring	Ø Policies	Objects	Device: firepower		>		e admin e Administrator	 diality SECURE 		
RA VPN ←		Device Summ Remote	Access VI	PN Connection Pro	files						
Connection Profiles							T Filter		+		
SAML Server		•	NAME	AAA	GROUP POLICY			ACTIONS			
		There are no Remote Access Connections yet. Start by creating the first Connection.									

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IPv4地址池项目中的Create new Network按钮。

- 连接配置文件名称:ftdvpn-aaa-cert-auth
- 身份验证类型:AAA和客户端证书
- 用户身份验证的主要身份源:LocalldentitySource
- Client Certificate Advanced Settings:在用户登录窗口时从证书中预填用户名

Firewall Device Manager Monitoring Po	Vicies Objects Device: firepower	SEC
Remote Access VPN	Connection and Client 2 Remote User Experience 3 Global Settings 4 Summary	
👰 Remote Users 🗖 S		
	 Be Identity Source for User Authentication 	
	Connection and Client Configuration Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.	
	Connection Profile Name This name is configured as a connection alias, it can be used to connect to the VPN gateway	
	ftdvpn-aaa-cert-auth Group Alias (one per line, up to 5) Group URL (one per line, up to 5)	
	ftdvpn-aaa-cert-auth	
	Primary Identity Source Authentication Type Add and Client Certificate	
	Primary Identity Source for User Authentication Fallback Local Identity Source	
	LocalidentitySource Please Select Local Identity Source	
	Username from Certificate	
	Primary Field Secondary Field	
	CN (Common Name) V OU (Organisational Unit) V Use entire DN (distinguished name) as username	
	Client Certificate Advanced Settings	
	Prefil username from certificate on user login window Hide username in login window	
	Client Address Pool Assignment	
	IPv6 Address Pool Endpoints are provided an address from this pool	
	₩ Filter	
	IPv4-Private-172.16.0.0-12 Network IPv4-Private-172.16.0.0-12 Network IPv4-Private-172.16.0.0-12 Network	
	C IPv4-Private-192.168.0.0-16 Network	
	Create new Network CANCEL OK	

VPN连接配置文件的详细信息

第四步:为连接配置文件添加地址池

输入必要信息以添加新的IPv4地址池。为连接配置文件选择新添加的IPv4地址池,然后单击Next按 钮。

- 名称 : ftdvpn-aaa-cert-pool
- 类型:范围
- IP范围:172.16.1.40-172.16.1.50

Add Network Object

Nama	
rvarne	
ftdvpn-aaa-cert-pool	
Description	
	4
Туре	
Network Sange	
IP Range	
172 16 1 40-172 16 1 50	
17 6.10.1.40-17 6.10.1.00	
e.g. 192.168.2.1-192.168.2.24 or 2001:D88:0:CD30::10-2001:D88:0:CD30::100	

 \times

CANCEL	ОК	

第五步:添加连接配置文件的组策略

在查看组策略项中点击创建新组策略。

Firewall Device Manager Monitoring Policies Object	s Device: firepower	admin
	👼 identity Source for U	Jser Authentication
A group	Remote User Experience policy is a collection of user-oriented session attributes which are a VPN connection is established. Select or create a Group Polic	assigned to client when a cy object.
View Gr Filter	DittorPolicy	•
- And and a	DNS + BANNER DNS Server None	Edit
	Banner Text for Authenticated Clients None SESSION SETTINGS Maximum Connection Time / Alert Interval Unlimited / 1 Minute	25
	Idle Time / Alert Interval BACK Simultaneous Login per Unr	

添加组策略

输入必要信息以添加新组策略,然后单击OK按钮。为连接配置文件选择新添加的组策略。

• 名称:ftdvpn-aaa-cert-grp

Edit Group Policy			
Search for attribute	Name		
lic	ftdvpn-aaa-cert-grp		
General	Description		
Session Settings			
dvanced Address Assignment Split Tunneling Secure Client Traffic Filters Windows Browser Proxy	DNS Server CustomDNSServerGroup Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session	~	
	Default domain		
	Secure Client profiles		
	CANCEL	ОК	

点击设备身份证书项目中的创建新内部证书。

þ	Firewall Device Manager	Monitoring	Policies	Dbjects	Device: firepower		(ک		۲	?	:	admin Administrator	Ŷ	dialia cisco SECURE
					Globa	Settings								
			These s apply	ettings control t to all connection	the basic functioning on profiles; you cannot	of the connection. Char configure different set	nges to a ttings in	any of th different	ese opti t profiles	ons s.				
			Certificate	of Device Identi	ity	Outside Interface								
			Filter		~	Please select				~				
			,® De	efaultInternalCertif alidation Usage: S	ficate SL Client, IPSe 0	rface		Port						
			P Va	efaultWebserverC alidation Usage: S	SL Client, IPSe 0			443						
			Create.nev	v Internal Certifica	le.			e.g. 808	0					
			Access Co Decrypted Vi policy for dea and the author Bypass	ntrol for VPN Tr PN traffic is subject crypted traffic option orization ACL dow s Access Control	affic ted to access control pol ion bypasses the access on inloaded from the AAA se ol policy for decrypted	cy inspection by default. E control policy, but for remo rver are still applied to VPP I traffic (sysopt permit-	inabling t te access l traffic vpn)	he Bypass s VPN, the	Access (VPN Filte	Control er ACL				

添加内部证书

单击Upload Certificate and Key。

Choose the type of internal certificate you want to create \times



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:ftdvpn-cert
- 特殊服务的验证使用情况:SSL服务器

Add Internal Certificate



A

- 设备身份证书:ftdvpn-cert
- 外部接口:外部(GigabitEthernet0/0)

Firew	all Device Manager	Monitoring	Ø Policies	Objects	Device: firepower	-			0 (?	D	:	admin Administrator	×	cisco S	SECURE
			These se apply	ettings control t to all connectio	Global : the basic functioning of an profiles; you cannot c	Settings the connection. Chang onfigure different setti	ges to any o ings in diffe	f these rent pro	options files.						
			Certificate of ftdvpn-co	of Device Identi ert (Validation l	ty Usage: SSL Ser ∨	Outside Interface outside (GigabitE	Ethernet0/0)		~	,					
			Fully-qualifi	ied Domain Nan	ne for the Outside Interf	ace	Port 4	43							
			e.g. ravpn.ex	ample.com			e.g.	8080							

步骤 7.为连接配置文件配置安全客户端映像

在程序包项目中选择Windows

Secure Client Packag	e
If a user does not already have t installer when the client authent	he right secure client package installed, the system will launch the secure client cates for the first time. The user can then install the package from the system.
You can download secure client You must have the necessary se	packages from software.cisco.com [3]. cure client software license.
Packages	
UPLOAD PACKAGE	×
Windows	
Mac	BACK NEXT

上传安全客户端映像包

从本地计算机上传安全客户端映像文件,然后单击NextButton。



注意:本文档中禁用了NAT免除功能。默认情况下,已解密流量的绕行访问控制策略 (sysopt permit-vpn)选项处于禁用状态,这意味着已解密的VPN流量将接受访问控制策略检 查。

Firewall Device Manager	Policies Objects Device: firepower	S 🚔 🛛 (? adm	nin ninistrator	cisco SECURE
	Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy inspection by policy for decrypted traffic option bypasses the access control policy, but and the authorization ACL downloaded from the AAA server are still applii Bypass Access Control policy for decrypted traffic (sysopt	default. Enabling the Bypass Access Cont for remote access VPN, the VPN Filter Af ied to VPN traffic t permit-vpn)	trol CL		
	NAT Exempt				
	Secure Client Package	the system will launch the service client			
	Installer when the client authenticates for the first time. The user can then You can download secure client packages from software.cisco.com You must have the necessary secure client software license.	i install the package from the system.			
	Packages UPLOAD PACKAGE Y				
	Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg				
	BACK				

选择Secure Client Image Package

步骤 8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FINISHbutton。



Ø Policies Firewall Device Manager Monitoring

tite Objects

Summary

Review the summary of the Remote Access VPN configuration.

rtovpn-Aaa-Cert-Auth		
STEP 1: CONNECTION AND CLIENT CONFIGURATION		
Primary Identity Source		
Authentication Type	AAA and Client Certificate	
Primary Identity Source	1 LocalIdentitySource	
AAA Advanced Settings		
Username from Certificate	Map Specific Field	
Primary Field	CN (Common Name)	
Secondary Field	OU (Organisational Unit)	
Client Certificate Advanced Settings		
Secondary Identity Source		
Secondary Identity Source for User Authentication	-	
Fallback Local Identity Source	-	
Advanced		
Authorization Server		
Accounting Server		
	F3 ftdvnn-aaa-cett-nool	
IPv4 Address Pool	C novph-aaa-cen-pool	
IPv6 Address Pool	- 0-	
DHCP Servers	-	
	8 million	
Group Policy Name Banner + DNS Server	Be travpn-aaa-cett-grp	
DNS Server	CustomDNSServerGroup	
Banner text for authenticated clients	-	
Session Settings		
Maximum Connection Time / Alert Interval	Unlimited / 1 minutes	
Idle Timeout / Alert Interval	30 / 1 minutes	
Simultaneous Login per User	3	
Split Tunneling		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling Secure Client	Allow all traffic over tunnel	
Secure Client Profiles	-	
STEP 3: GLOBAL SETTINGS		
Certificate of Device Identity	옷 ftdvpn-cert	
Outside Interface	GigabitEthemet0/0 (outside)	
Fully-qualified Domain Name for the Outside	-	
Interface		
Port	443	
Access Control for VPN Traffic	No	
NAT Exempt		
NAT Exempt	No	
Inside Interfaces	GigabitEthernet0/0 (outside)	
Inside Networks	-	
Secure Client Package		
Packages	Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg	

Instructions

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 1 interface GigabitEthernet0/1 speed auto nameif inside cts manual propagate sgt preserve-untag policy static sgt disabled trusted 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 // Defines a local user username sslVPNClientCN password ***** pbkdf2 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftdvpn-cert enrollment terminal keypair ftdvpn-cert validation-usage ssl-server crl configure // Server Certificate crypto ca certificate chain ftdvpn-cert certificate 22413df584b6726c 3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7 quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client ssl-server 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 enable tunnel-group-list enable cache disable error-recovery disable // Configures the group-policy to allow SSL connections group-policy ftdvpn-aaa-cert-grp internal group-policy ftdvpn-aaa-cert-grp attributes dns-server value 64.x.x.245 64.x.x.184 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 none anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting // 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

在VPN客户端中确认

步骤1:确认客户端证书

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。

Sonsole1 - [Console Root\Certificates - Current Eile Action View Fav@rites Window	t User\Personal\Certificates] Help				-	0 ×
	<u>^</u>					
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Actions
Certificates - Current User Personal	SSIVPNClientCN	ftd-ra-ca-common-name	6/16/2025	Client Authentication	ssIVPNClientCer	Certificates 🔺
Certificates						More 🕨
Inusted Koot Certification Authorities						
Certificates						
> 🛄 Enterprise Trust						

确认客户端证书

双击客户端证书,导航到Details,检查Subject的详细信息。

• 主题:CN = sslVPNClientCN

💼 Certificate

General	Details	Certification i	Path
Show:	<ai></ai>		~
Field Sig Sig Val Val Val Val Val Val Val Val Val S Val Val Val Val Val Val Val Val Val Val	nature al nature hi uer ld from ld to bject blic key blic key	gorithm ash algorithm arameters	Value sha256RSA sha256 ftd-ra-ca-common-name, Cisc Sunday, June 16, 2024 6: 12:0 Monday, June 16, 2025 6: 12: SslVPNClentCN, sslVPNClentO RSA (2048 Bits) ns on
			Edit Properties Copy to File
			OK

客户端证书的详细信息

第二步:确认CA

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。

Х

• 颁发者:ftd-ra-ca-common-name

ᡖ Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authoritit Certificates] —					٥	×	¢	
File Action View Favorites Window	Help						- 8	х
🗢 🔿 📶 🥉 🗞 🔀 🚱 🛛	•]							
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Action		
Certificates - Current User	COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	Certific	ates	
Certificates	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Tii	M	ore	۲
 Trusted Root Certification Authorities Certificates 	DigiCert Assured ID Root	DESKTOP-VCKHRG1 DigiCert Assured ID Root	10/30/2022 11/9/2031	Server Authenticati <all></all>	<none></none>	ftd-ra-	ca	*
Citerprise Trost Intermediate Certification Authorities Intermediate Certification Authorities Interded Declinearer	DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert Global Root G2	DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance	11/9/2031 11/9/2031 1/15/2038 11/9/2031	Client Authenticati Client Authenticati Client Authenticati <all></all>	DigiCert DigiCert DigiCert Glol <none></none>	м	ore	,
 Instea Publishers Untrusted Certificates Third-Party Root Certification Authoriti 	DigiCert High Assurance DigiCert Trusted Root G4	DigiCert High Assurance DigiCert Trusted Root G4	11/9/2031 1/15/2038	Client Authenticati Client Authenticati	DigiCert DigiCert Tru:			
Smart Card Trusted Roots Smart Card Trusted Roots	ttd-ra-ca-common-name	ftd-ra-ca-common-name	6/16/2029	<all></all>	<none></none>			
> (Certificates (Local Computer)	GlobalSign	GlobalSign	12/15/2021	Client Authenticati	Google Trust			

确认CA

验证

步骤1:启动VPN连接

在终端上,启动Cisco安全客户端连接。用户名从客户端证书提取,您需要输入密码进行VPN身份验 证。



注意:用户名提取自本文档中客户端证书的公用名(CN)字段。

Sisco Secure Client	- 🗆 X	() Cisco Secure Client 192.168.1.200	×	S Cisco Secure Client	- 0	×
AnyConnect VPI: Contacting 192.168.1.200. 192.168.1.200	✓ Connect	Group: ftdvpn-aaa-cert-auth Usern-ame: sslVPNClientCN	~	AnyConnect VPN: Connected to 192.168.1.200. 192.168.1.200	V Disconnect	
* •	A I A	Password:		00:00:06	Pv	4
W (0)	6968	OK Cancel		* 0	Ó	460

启动VPN连接

第二步:在FTD CLI中确认VPN会话

在FTD (Lina) CLI中运行show vpn-sessiondb detail anyconnect命令以确认VPN会话。

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4 Assigned IP: 172.16.1.40 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 : 29072 Bytes Rx : 44412 Pkts Tx: 10 Pkts Rx: 442 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth Login Time : 11:47:42 UTC Sat Jun 29 2024 Duration: 1h:09m:30s Inactivity: 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000000667ff45e Security Grp: none Tunnel Zone: 0

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

AnyConnect-Parent: Tunnel ID : 4.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 49779 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 7 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 : 14356 Bytes Rx : 0 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 4.3 Assigned IP : 172.16.1.40 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 49788 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7178 Bytes Rx : 10358 Pkts Tx : 1 Pkts Rx : 118 Pkts Tx Drop : 0 Pkts Rx Drop : 0

第三步:确认与服务器的通信

从VPN客户端向服务器发出ping命令,确认VPN客户端与服务器之间的通信成功。



注意:由于在第7步中禁用了用于已解密流量的绕行访问控制策略(sysopt permit-vpn)选项,因此需要创建允许您的IPv4地 址池访问服务器的访问控制规则。

C:\Users\cisco>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data: Reply from 192.168.10.11: bytes=32 time=1ms TTL=128 Reply from 192.168.10.11: bytes=32 time=1ms TTL=128 Reply from 192.168.10.11: bytes=32 time=1ms TTL=128 Reply from 192.168.10.11: bytes=32 time=1ms 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 = 1ms, Maximum = 1ms, Average = 1ms
```

Ping成功

capture in interface inside real-time在FTD (Lina) CLI中运行命令以确认数据包捕获。

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may result in an excessive amount of non-displayed packets due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request 2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply 3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request 4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply 5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request 6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply 7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request 8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo request

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Lina引擎中的调试日志示例。

// Certificate Authentication

Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=ssIV Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked. Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=ssIVPNClientCN

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3] Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication

Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

这些调试可以从FTD的诊断CLI运行,CLI提供可用于对配置进行故障排除的信息。

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

相关信息

为Firepower 2100配置FDM机上管理服务

在FDM管理的FTD上配置远程访问VPN

<u>配置并验证Firepower设备管理器中的系统日志</u>

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)。