在FTD上配置AnyConnect VPN客户端:发夹和 NAT免除

目录
<u>简介</u>
先决条件
使用的组件
<u>背景信息</u>
<u>步骤1:导入SSL证书</u>
<u>第二步:配置RADIUS服务器</u>
<u>第三步:创建IP池</u>
<u>第四步:创建XML配置文件</u>
<u>第五步:上传Anyconnect XML配置文件</u>
<u>第六步:上传AnyConnect映像</u>
步骤 7.远程访问VPN向导
<u>NAT免除和发夹</u>
步骤1:NAT免除配置
<u>第二步:发夹配置</u>
<u>验证</u>
<u>故障排除</u>

简介

本文档介绍如何在FMC管理的Firepower威胁防御(FTD)v6.3上配置思科远程访问VPN解决方案 (AnyConnect)。

先决条件

要求

Cisco 建议您了解以下主题:

- 基本的远程访问VPN、安全套接字层(SSL)和互联网密钥交换版本2(IKEv2)知识
- 基本身份验证、授权和记帐(AAA)以及RADIUS知识
- 基本的FMC知识
- 基本的FTD知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科FMC 6.4
- 思科FTD 6.3
- AnyConnect 4.7

本文档介绍在Firepower威胁防御(FTD)版本6.3(由Firepower管理中心(FMC)管理)上配置思科远程访问VPN解决方案(AnyConnect)的过程。

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

本文档旨在介绍FTD设备上的配置。如果您寻找ASA配置示例,请参阅文档

: <u>https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html</u>

限制:

目前,这些功能在FTD上不受支持,但在ASA设备上仍然可用:

- 双AAA身份验证(在FTD 6.5版上可用)
- 动态访问策略
- 主机扫描
- ISE终端安全评估
- RADIUS CoA
- VPN负载均衡器
- 本地身份验证(在Firepower设备管理器6.3上可用。Cisco Bug ID CSCvf92680)
- LDAP属性映射(通过FlexConfig提供,思科漏洞ID <u>CSCvd64585</u>)
- AnyConnect自定义
- AnyConnect脚本
- AnyConnect本地化
- 毎应用VPN
- ・ SCEP代理
- WSA集成
- ・ SAML SSO(思科漏洞ID <u>CSCvq90789</u>)
- RA和L2L VPN的同步IKEv2动态加密映射
- AnyConnect模块(NAM、Hostscan、AMP Enabler、SBL、Umbrella、网络安全等)。DART是此版本中默认安装的唯一模块。
- TACACS、Kerberos(KCD身份验证和RSA SDI)
- 浏览器代理

配置

要通过FMC中的远程访问VPN向导,必须完成以下步骤:

步骤1:导入SSL证书

配置AnyConnect时,证书至关重要。SSL和IPSec仅支持基于RSA的证书。

IPSec支持椭圆曲线数字签名算法(ECDSA)证书,但是,当使用基于ECDSA的证书时,无法部署新的AnyConnect软件包或XML配置文件。

它可用于IPSec,但您必须预部署AnyConnect软件包和XML配置文件,所有XML配置文件更新必须 在每个客户端上手动推送(Cisco bug ID <u>CSCtx42595</u>)。

此外,证书必须包含带有DNS名称和/或IP地址的公用名(CN)扩展,以避免Web浏览器中出现"不受 信任的服务器证书"错误。

注意:在FTD设备上,生成证书签名请求(CSR)之前需要证书颁发机构(CA)证书。

- 如果在外部服务器(例如Windows Server或OpenSSL)中生成CSR,manual enrollment method将会失败,因为FTD不支持手动密钥注册。
- 必须使用其他方法,例如PKCS12。

为了使用手动注册方法获取FTD设备的证书,需要生成CSR,使用CA对其进行签名,然后导入身份 证书。

1.导航到设备>证书,然后选择添加,如图所示。

Overview Analysis	Policies Devices Ob	jects AMP Inte	lligence		Deploy (2 System	Help 🔻	admin 🔻
Device Management	NAT VPN VOS	Platform Settings	FlexConfig Certif	icates				
							0	Add
Name		Domain	Enrollment Ty	e Status				
		No	o certificates Add	Certificates				

2.选择Device并添加新的Cert Enrollment对象,如图所示。

Overview Analysis Policies Devices	Objects AMP I	ntelligence		Deploy	2 System	Help 🔻	admin ▼
Device Management NAT VPN • Q	oS Platform Settings	s FlexConfig Certificates					
						\odot	Add
Name	Domain	Enrollment Type	Status				
		No cortificatos Add Cortif	icatos				
		No certificates Add Certifi	icates				
	Add New Certificat	te		? ×			
	Add a new certificate to identify certificate.	the device using cert enrollment obj	ect which is used to generate	CA and			
	Device*:	FTD-Virtual	~				
	Cert Enrollment*:	Select a certificate entrollment of	bject 🗸 🕐				
			Add	ancel			
Add	d Cert Enrollment			? ×			
Na	ame*						
De	escription						
	CA Information Cer	tificate Parameters Key Rev	ocation				
E	inrollment Type:	SCEP	*				
E	inrollment URL:*	http://					
	Challenge Password:						
	Confirm Password:						
R	Retry Period:	1 Minutes (R	ange 1-60)				
R	Retry Count:	10 (R	ange 0-100)				
r	ingerprint:	Ex: e6f7d542 e355586c a758e7cb b	dcddd92				
Alle	ow Overrides						
			Save	Cancel			

3.选择手动注册类型并粘贴CA证书(用于签署CSR的证书)。

Add Cert Enrollment

Name*	Anyconnect-certificate					
Description						
CA Information	Certificate Parameters	Кеу	Revocation			
Enrollment Type:	Manual				×	
CA Certificate:*	/3C4hi07uzuR0ygwKEB 4x3nk3tTUhYpfmbWqV RqV66GI9iE7Z2 xiVrSrJFqhkrT795kMb8 VLSP+vHGm8X g6wEFsKuZay27a48e/I LhBNFbyBVb9 d0jUkrndSvzQDR5qSo- VMYhIVBOT8h H8eMjSQIGhhHbouKoPV mwNgySmTP9cHa 9Or3RIWRzEa11HE3ml DI8ZcLYmfaIdC W2c2uBROyVDxCvq4f0 usiu9KTGH1 btVKEYACKVyETw== END CERTIFICATE	kaMdg4D vAXM7Gf amBxhb JG2LgRD +HINEm /izQmM0 HO4Rj6D)4ISEIBf((/z NDRVWG9BZ1sv 4eXYXxUg3mODf hrA0Kt+jwbS7DG 3E8/q20wrtlZpD RvGnTB6EKiY1vt X0nmgufjx+TZR WFSd5rAD/bvk2	k3shDK2Bogklzxu IPqZ76RSTAT0+v 3SK4mfZsZqhFdQ 4MpAabyhr+hEpd x4CUW8HcgDdDv YczownSKLL7LcW 2n6xrJI1SLqABMJ	иб 1 Р Р 1 Ј	
Allow Overrides						
				Sa	ve	Cancel

4.选择Certificate Parameters选项卡,然后为Include FQDN字段选择"自定义FQDN",并填写图像 中所示的证书详细信息。

A	dd Cert Enrollment						? ×
	Name*	An	yconnect-certificate				
	Description						
	CA Information Ce	rtific	ate Parameters	Key	Revocation		
	Include FQDN:		Use Device Hostname	as FQE	DN	•	
	Include Device's IP Addre	ess:					
	Common Name (CN):		vpn.cisco.com				
	Organization Unit (OU):		TAC				
	Organization (O):		Cisco				
	Locality (L):		МХ				
	State (ST):		Mexico				
	Country Code (C):		МХ				
	Email (E):						
	Include Device's Serial	l Num	ber				
	Allow Overrides						
						Save	Cancel

5.选择键选项卡,然后选择键类型,您可以选择名称和大小。对于RSA,最低要求为2048字节。6.选择"保存",确认设备,然后在证书注册下,选择刚创建的信任点,选择添加以部署证书。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:	FTD-Virtual	~	
Cert Enrollment*:	Anyconnect-certificate	~	٥
Cert Enrollment Details:			
Name:	Anyconnect- certificate		
Enrollment Type:	Manual		
SCEP URL:	NA		
			Add Cancel

7.在状态列中,选择ID图标,然后选择是以生成CSR,如图所示。

Overview Analysis Policies Devices	Objects AMP Inte	lligence		Deploy 🔩 System	Help 🔻 admin 🔻
Device Management NAT VPN • Qo	S Platform Settings	FlexConfig Certificates			
					O Add
Name	Domain	Enrollment Type	Status		
4 🗐 FTD-Virtual					
Anyconnect-certificate	Global	Manual	CA CA	A ID A Identity certificate import required	🗗 🗘 🗒
	Warnin	g			
	want to	This operation will generate Certificate Signing Request do o continue?	you		
		Yes No.			

8.复制CSR并用您首选的CA(例如GoDaddy或DigiCert)签名。

9.从CA收到身份证书(必须采用base64格式)后,选择Browse Identity Certificate,然后在本地计 算机上查找证书。选择导入。

Import Identity Certif	icate	? >
Step 1 Send Certificate Signing Re	equest (CSR) to the Certificate Autho	prity.
Certificate Signing Request	t (Copy the CSR below and send to th	he Certificate Authority):
BEGIN CERTIFICATE RE MIIC9TCCAd0CAQAwejELM/ A1UEBxMCTVgxFjAUBgNVB/ MQwwCgYDVQQLEwNUQUM hkiG9w0BAQEFAAOCAQ8AM gQTJd6kUaUDdM8YqD209C 9dSOIE3bkpY+VVkQKvd2Pfd XUXtzuwHsTM8fgZSBK18C7 inkEEDM8PtBUvP77315Yo5M	QUEST AkGA1UEBhMCTVgxDzANBgNVBAgTBk: AMTDXZwbi5jaXNjby5jb20xDjAMBgNVB 4xFzAVBgkqhkiG9w0BCQIWCGNpc2Nv 1IIBCgKCAQEAzgnRRu5LjeufjMoVw1u0 6XLVSsYML3K87zJgsbQkX/+uGzg4CJd3 dlXrSW7/EOIFU2fiS7uQzioZuLfCGo2bc7 iL65aMfmjPwJUX5I/NuNNhx9iR7uNJ5C	alleGljbzELMAkG BAoTBUNpc2Nv YXNhMIIBIJANBgkq DFx5CPnpTjCRR 34T1Wa661iml 7K3Uuj4VV CBj7UdYV+dv rzCENM1uxd5PWK
Step 2 Once certificate authority r	esponds back with identity certificate	e file, import it to device.
Identity Certificate File:	Anyconnect-Document.pem	Browse Identity Certificate
		Import Cancel

10.导入后,CA和ID证书详细信息将可供显示。

Overview Analysis Policies Device	objects AMP Intelligen	ce		Deploy 🥊	2 System	Help 🔻	admin 🔻
Device Management NAT VPN •	QoS Platform Settings Flexe	Config Certificates					
						\odot	Add
Name	Domain	Enrollment Type	Status				
🖌 🗐 FTD-Virtual							
Anyconnect-certificate	Global	Manual	CA ID			P	Φ 🗎

第二步:配置RADIUS服务器

在FMC管理的FTD设备上,不支持本地用户数据库,必须使用其他身份验证方法,例如RADIUS或 LDAP。

1.导航到对象 > 对象管理 > RADIUS服务器组 > 添加RADIUS服务器组,如图所示。

Add RADIUS Server Group

Name:*	Radius-server			
Description:				
Group Accounting Mode:	Single	•		
Retry Interval:*	10		(1-10) Seconds	
Realms:		•		
Enable authorize only				
Enable interim account update				
Interval:*			(1-120) hours	
Enable dynamic authorization				
Port:*			(1024-65535)	
RADIUS Servers (Maximum 16 serve	rs)			0
IP Address/Hostname				
	No records to display			
			Save	Cancel

2.为Radius Server Group分配名称并添加Radius服务器IP地址以及共享密钥(需要共享密钥才能将 FTD与Radius服务器配对),完成此表单后,请选择Save(如图所示)。

Add RADIUS Server Group

Name	:*	Radius-server	
Descri	ption:		
Group	Accounting Mode:	Single 💙	
Retr	New RADIUS Server		? ×
	IP Address/Hostname:*	192.168.10.34 Configure DNS at Threat Defense Platform Settings to	o resolve hostname
□ E	Authentication Port:*	1812	(1-65535)
	Key:*	•••••	
	Confirm Key:*	•••••	
RAD	Accounting Port:	1813	(1-65535)
	Timeout:	10	(1-300) Seconds
IP	Connect using:	• Routing O Specific Interface (1)	
		Default: Diagnostic Interface	▼ ③•
	Redirect ACL:		 O
		Save	Cancel
			Save Cancel

? ×

3. RADIUS服务器信息现在在Radius服务器列表中可用,如图所示。

Add RADIUS Server Group

Name:*	Radius-server				
Description:					
Group Accounting Mode:	Single	~			
Retry Interval:*	10	(1-10) Seconds			
Realms:		~			
Enable authorize only					
Enable interim account update					
Interval:*		(1-120) hours			
Enable dynamic authorization					
Port:*		(1024-65535)			
RADIUS Servers (Maximum 16 server	rs)				
				0	
IP Address/Hostname					
192.168.10.34			600	ï	
		Save	Ca	ncel	

第三步:创建IP池

1.导航到对象 > 对象管理 > 地址池 > 添加IPv4池。

2.分配IP地址的名称和范围,不需要Mask字段,但可以如图所示指定。

? X

Add IPv4 Pool

Name*	vpn-pool]	
IPv4 Address Range*	192.168.55.1-192.168.55.253		
	Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150		
Mask	255.255.255.0		
Description			
Allow Overrides]	
Configure device over shared across multiple	rrides in the address pool object to avoid IP address co le devices	onflicts in case	of object is
		Save	Cancel

第四步:创建XML配置文件

1.从Cisco.com下载配置文件编辑器工具并运行该应用程序。

2.在"配置文件编辑器"应用程序中,导航到服务器列表,然后选择添加,如图所示。

VPN Preferences (Part 1)	Server List						
Preferences (Part 2)							
Gartificate Dinning	Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins
Certificate Matching							
Mobile Policy							
Server List							
	Note: it is hi	ably recommend	led that at least	one server he defin	ed in a profile	Add	Delete
	Note. It is in	ignly recommend	ieu that at least	one server be dem		Auu	Delete
						Edit	Details

3.分配显示名称、完全限定域名(FQDN)或IP地址,然后选择确定(如图所示)。

Server List Entry

Server	Load Balancing Ser	vers S	CEP	Mobile	Certificate Pinning			
Pr	imary Server					Connection Informa	tion	
I	Display Name (require	ed) C	Corpor	ate - FTI	D (SSL)	Primary Protocol	SSL 🗸	
F	QDN or IP Address				User Group	🗸 ASA gateway		
[vpn.cisco.com			/	ssl	Auth Method	During IKE Negotiation	EAP-AnyConnect \lor
(Group URL					IKE Identity (OS gateway only)	
[
	Ва	ckup Sei	rvers					
		Host A	ddres	s			Add	
							Move Up	
							Move Down	
							Delete	
					ОК	Cancel		

4.现在可在Server List菜单中看到该条目:

VPN 	Server List Profile: Untitled							
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	Hostname	Host Address	User Group	Backup Server	SCEP	Mobile Settings	Certificate Pins	
	Note: it is highly recommen	nded that at least one	e server be defined in	n a profile.	Ad	d De	elete	

5.定位至文件 > 另存为。

注意:使用带有.xml扩展名的易于识别名称保存配置文件。

第五步:上传Anyconnect XML配置文件

1.在FMC中,导航至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。

2.为对象指定名称,然后单击浏览,在本地系统中找到客户端配置文件,然后选择保存。

么》	主意:	确保选择Anyconnect Client Profile作为文件类型。
----	-----	--------------------------------------

Add AnyConnect File

Name:*	Corporate-profile(SSL)	
File Name:*	FTD-corp-ssl.xml	Browse
File Type:*	AnyConnect Client Profile	~
Description:		

? X

第六步:上传AnyConnect映像

1.从思科下载网页下载webdeploy(.pkg)映像。

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	± 👾 🖺
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

2.导航到"对象"(Objects)> "对象管理"(Object Management)> "VPN"(VPN)> AnyConnect文件 (AnyConnect File)> 添加AnyConnect文件(Add AnyConnect File)。

3.为Anyconnect软件包文件指定名称,并在选择文件后从本地系统选择.pkg文件。

4.选择保存。

Add AnyConnect	: File	?	×
		_	
Name:*	MAC4.7		
File Name:*	anyconnect-macos-4.7.04056-webdeploy-k9 Browse		
File Type:*	AnyConnect Client Image	~	
Description:			
		_	
	Save Cancel		

注意:可根据您的要求(Windows、Mac、Linux)上传其他软件包。

步骤 7.远程访问VPN向导

根据前面的步骤,可以相应地执行远程访问向导。

1.导航到设备 > VPN > 远程访问。

2.分配远程访问策略的名称,然后从Available Devices中选择FTD设备。

Overview Analysis Pol	licies Device	es Objects AMP Intelli	gence	lexConfig Certificates		Deploy 🧕	System	Help 🔻	admin 🔻
Remote Access VPN	Policy Wiz	ard	in octango i	Certificates					
1 Policy Assignment	2 Conne	ection Profile 3 AnyCo	onnect) (4)	Access & Certificate	5 Summary				
Ta Th a r Na De VP Ta	argeted Device is wizard will guid new user-defined of ame:* escription: PN Protocols: argeted Devices:	es and Protocols le you through the required minimal connection profile. TAC SSL IPsec-IKEv2 Available Devices Search FTD-Virtual	steps to configure t	he Remote Access VPN policy wi	th Before y configura complete Authent Configura to auther to auther Make su for VPN the relev it during Device J Interface enable V	ore You Start you start, ensure the following ation elements to be in place to Remote Access VPN Policy. tication Server e Realm or RADIUS Server Group nticate VPN clients. nect Client Package Client downloaded or you have ant Cisco credentials to download the wizard. Interface is should be already configured on devices so that they can be used curity zone or interface group to IPN access.			
						Back	Next	Ca	ncel

3.分配连接配置文件名称(连接配置文件名称是隧道组名称),选择Authentication Server和 Address Pools,如图所示。

<text></text>	Overview Analysis Policies Devices	Objects	AMP Intellige	nce		Deploy 02	System Hel	p 🔻 admin 🔻
<section-header> Image: Series of the series of t</section-header>	Device Management NAT VPN > Rem	ote Access	QoS Platform	n Setting	s FlexConfig	Certificates		
<complex-block></complex-block>	Remote Access VPN Policy Wiza	rd						
<image/>	1 Policy Assignment 2 Connec	tion Profile	3 AnyCon	nect	Access 8	Certificate	Summ	ary
<form>Checking the standing standing standing standing for a VM connection. These policies pratient to creating the tunnel itself, show AAA is a conclusion without show addresses are areasing and involve to user attributes, which are defined in group policies. Correction Profile Image: Standing and Standing</form>	Remote User AnyConnect Client	Inte	imet	Outsic	e VPN Device	Inside	Corporate Reso	urces
<form>Conceilion Profiles specify the tunnel group policies for a VPK connection. These policies periation to results field, how AAA is a consonibiled and how addresses are assigned. They are conditived and are defined in group policies. Conceilion Profile Name:</form>	Connection Profile:							
Mencetion Profile Nears: Image: Image	Connection Profiles specify the tunne accomplished and how addresses are	l group policies for assigned. They al	a VPN connection. so include user attr	These po ibutes, w	licies pertain to crea hich are defined in g	ating the tunnel its roup policies.	elf, how AAA is	
Iterate configured as connection alls, if can be used to connect to the PHP determination. Action 1. A Configure 1.	Connection Profile Name:*	TAC						
Authorization Server: Use same authentication server (CADUS) Accounting Server: (RADUS) Client PI Address Cashe sasigned 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 pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pools. Use AAA Server (RADUS only) Use DHCP Servers Use DHCP Servers Use DHCP Servers IPv6 Address Pools: Vpr-pool IPv6 Address Pools: Vpr-pool Agroup 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: RemoteAccess-GP-SSL Edit Group Policy Edit Group Policy	Authentication, Authorization & A Specify the method of authentication Authentication Method: Authentication Server:*	This name is config accounting (AAA) (AAA, certificates AAA Only Radius-server	gured as a connection : or both), and the A	AA serve	can be used to conne rs that will be used f (Realm or RADIUS	ct to the VPN gatew for VPN connection	ıs.	
Accounting server:	Authorization Server:	Use same auther	ntication server	▼ ○	(RADIUS)			
IPv4 Address Pools: vpn-pool IPv6 Address Pools: 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:* RemoteAccess-GP-SSL Git Group Policy Back Next Cancel	Client Address Assignment: Client IP address can be assigned fro assignment is tried in the order of AA Use AAA Server (RADIUS of Use DHCP Servers Use IP Address Pools	m AAA server, DH AA server, DHCP se only) 🕕	CP server and IP ac rver and IP addres	ddress pool.	(Notes)	ptions are selected	d, IP address	
IPv6 Address Pools: 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:* RemoteAccess-GP-SSL Edit Group Policy Back Next Cancel	IPv4 Address Pools:	vpn-pool		ø				
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: Croup Policy: Edit Group Policy Edit Group Policy Back Next Cancel	IPv6 Address Pools:			62				
Group Policy:* RemoteAccess-GP-SSL Edit Group Policy Edit Group Policy Back Next Cancel	Group Policy: A group policy is a collection of user- or create a Group Policy object.	oriented session a	tributes which are	assigned	to client when a VP!	N connection is est	ablished. Select	
Back Next Cancel	Group Policy:*	RemoteAccess-G	P-SSL	▼ ○				
Back Next Cancel								
						Back	Next	Cancel

4.选择+符号以创建组策略。

Add Group Policy

Name:*	RemoteA	ccess-GP				
Description:						
General An	yConnect	Advanced				
IP Address Pools Banner DNS/WINS Split Tunneling		VPN Tunnel Pro Specify the VPN configured for u SSL IPsec-IKEv2	otocol: I tunnel types that users to connect o	user can use. At least ver a VPN tunnel.	one tunneling mode	must be
					Save	Cancel

5.(可选)可以基于组策略配置本地IP地址池。如果未配置,则从连接配置文件(隧道组)中配置 的池继承该池。

Add Group Policy

Name:*	RemoteA	ccess-GP					
Description:							
General An	yConnect	Advanced					
VPN Protocols		IP Address Pool	ls:				\odot
IP Address Pools		Name		IP Address Range			
DNS/WINS Split Tunneling		vpn-pool		192.168.55.1-192.168	3.55.253		
						Save	Cancel

6.对于此场景,所有流量都通过隧道路由,IPv4分割隧道策略设置为Allow all traffic over the tunnel,如图所示。

Edit Group Policy

Name:*	ne:* RemoteAccess-GP-SSL cription: eneral AnyConnect Advanced N Protocols Address Pools nner S/WINS Split Tunnel Network List Ty Standard Access List: DNS Request Split Tunneling DNS Requests: Domain List:				
Description:					
General An	yConnect	t Advanced			
VPN Protocols		IPv4 Split Tunneling:	Allow all traffic over tunnel	~	
IP Address Pools Banner		IPv6 Split Tunneling:	Allow all traffic over tunnel	~	
DNS/WINS		Split Tunnel Network List Type:	Standard Access List C Extended Access	List	
Split Tunneling		Standard Access List:		~	
		DNS Request Split Tunneling			
		DNS Requests:	Send DNS requests as per split tunnel policy	~	
		Domain List:			
			Save	Ca	incel

7.为Anyconnect配置文件选择.xml配置文件,然后选择保存,如图所示。

Add Group Policy

Name:*	RemoteA	Access-GP-SSL		
Description:				
General An	yConnec	t Advanced		
Name:* RemoteAccess-GP-SSL Description:				
SSL Settings		features. FTD deploys	the profiles during AnyConnect	client connection.
Connection Setting	gs	Client Profile:	Corporate-profileSSL	▼ ③
		Standalone profile edit profile. You can downlo	or can be used to create a new bad the profile editor from Cisco	or modify existing AnyConnect Software Download Center.
				Save Cancel

8.根据运行的系统要求选择所需的AnyConnect映像,然后选择Next(如图所示)。

Overvie Device M Remot	anaç e A	Analysis Policies Devices gement NAT VPN ▶ Remo cccess VPN Policy Wizar	Objects AMF te Access QoS	P Intelligenco Platform So	e ettings	FlexConfig	Deploy Certificate	0 2 S	System H	Help ▼	admin 🔻
1 Poli	icy /	Assignment $>$ 2 Connect	ion Profile	AnyConne	ct 4	Access 8	k Certificate	>	5 Sum	nmary	
Rem	Any	AnyConnect Client	Internet		Outside	VPN Device	Inside		Corporate R	esources	
	The initia	VPN gateway can automatically down ted. Minimize connection setup time b	load the latest AnyCo y choosing the approp	nnect package to riate OS for the s	the client d elected packa	device when t age.	the VPN connec	tion is			
	Dow	nload AnyConnect Client packages from	m Cisco Software Dow	nload Center.	s	how Re-orde	r buttons	0			
		AnyConnect File Object Name	AnyConnect Clien	t Package Name	e	Operating	System				
		MAC4.7	anyconnect-macos-	4.7.04056-Webde	эрюу-кэ	Mac OS	*				
						(Back		Next	Ca	ncel

9.选择安全区和设备证书:

• 此配置定义VPN终止所在的接口以及SSL连接上显示的证书。

注意:在此场景中,FTD配置为不检查任何VPN流量,并会切换访问控制策略(ACP)选项。

Overview Analy	sis Policies Devices Obje	cts AMP Intelligence	Deploy 🧕	System Help 🔻 admin 🔻
Device Management	NAT VPN > Remote Acce	QoS Platform Setting	FlexConfig Certificates	
Remote Acces	s VPN Policy Wizard			
1 Policy Assign	ment $>$ 2 Connection Pro	ofile > 3 AnyConnect	4 Access & Certificate	5 Summary
Remote User	AnyConnect Client	Internet Outsk	le VPN Device Inside	Corporate Resources
	Network Interface for Incomi	ng VPN Access	AAA	
	Select or create an Interface Group o connections.	or a Security Zone that contains the	network interfaces users will access f	or VPN
	Interface group/Security Zone:*	outside	• •	
		Enable DTLS on member interfa	ces	
	Device Certificates Device certificate (also called Identity certificate which is used to authentic Certificate Enrollment:* Access Control for VPN Traffie All decrypted traffic in the VPN tunne bypass decrypted traffic from the Acc Bypass Access Control policy for This option bypasses the Access C AAA server are still applied to VPN	c c c c c c c c c c c c c c c c c c c	vay to the remote access clients. Sele Policy by default. Select this option to ACL and authorization ACL downloaded f	ect a
			Back	Next Cancel

10.选择完成并部署更改:

与VPN、SSL证书和AnyConnect软件包相关的所有配置均通过FMC Deploy进行推送,如图所示。



NAT免除和发夹

步骤1:NAT免除配置

NAT免除是首选转换方法,用于防止流量在流经VPN隧道(远程访问或站点到站点)时路由到互联 网。

当来自内部网络的流量要流经隧道而不进行任何转换时,需要执行此操作。

New Network	Object				? ×
Name	vpn-pool				
Description					
Network	O Host	Range	 Network 	○ FQDN	
	192.168.55.0/24	1			
Allow Overrides					
				Save	Cancel

2.导航到设备(Device)> NAT,选择相关设备使用的NAT策略,并创建新语句。

Manual NAT Pulo						
IAT Rule: Manual NAT Rule		▼ Insert: In Category ▼ NAT Rules Before ▼		▼ NAT Rules Before ▼]	
Static	~ (✓ Enable				
Translation	PAT Pool	Advanced				
ects 🖒		Source Interfac	ce Objects (1)	Destination Interface Object	s (1)	
		inside-zone	ā	outside-zone	ij.	
	Add	to				
	Add	to				
	Destin	ation				
	Static Translation ects	Static	Static C Enable Translation PAT Pool Advanced ects C Source Interfac Add to Source Add to Destination	Static C Enable Translation PAT Pool Advanced ects C Source Interface Objects (1) Add to Add to Destination	Static C Enable Translation PAT Pool Advanced ects C Source Interface Objects (1) Destination Interface Object Add to Add to Destination	

3.选择FTD(原始源和转换后的源)后面的内部资源和目标作为Anyconnect用户的ip本地池(原始目标 和转换后的目标),如图所示。

Add NAT Rule								? ×
NAT Rule: M	anual NAT Ru	ule 💙	Ins	sert:	In Category	▼ NAT Rules Before	~	
Description:								
Interface Objects Tra	anslation	PAT Pool	Advanced					
Original Packet					Translated Packet			
Original Source:*	FTDv-Ins	ide-SUPERNE		~ 🔾	Translated Source:	Address	*	
Original Destination:	Address			~		FTDv-Inside-SUPERNE	~] 💿
	vpn-pool			~ ()	Translated Destination:	vpn-pool	*	0
Original Source Port:				v O	Translated Source Port:		~	
Original Destination Port:				v 🔾	Translated Destination Port:		~] 💿
						0	KCand	cel

4.确保切换选项(如图所示),要在NAT规则中启用"no-proxy-arp"和"route-lookup",请选择 OK(如图所示)。

Edit NAT Rule								? ×
NAT Rule:		Manual NAT Rule		::	In Category	▼ N	ore 💙	
Туре:	Static	*	Enable					
Description:								
Interface Objects	Translation	PAT Pool	Advanced					
Translate DNS repl	ies that match th	is rule						
Fallthrough to Inter	rface PAT(Destina	ation Interface)					
IPv6								
Net to Net Mapping	1							
🔽 Do not proxy ARP d	on Destination In	terface						
Perform Route Look	kup for Destination	on Interface						
Unidirectional								
							ОК	Cancel

5.这是NAT免除配置的结果。

1 e Static 🚠 inside-zone 🚔 outside-zone 💂 FTDv-Inside-SUPERNE 💂 vpn-pool 🔮 FTDv-Inside-SUPERNE 💂 vpn-pool 🔮 Dns:false 🥜 🕯 上一节中使用的对象如下所述。

Name Description	FTDv-Inside-SU	JPERNE		
Network	O Host	O Range	O Network	O FQDN
Allow Overrides	10.124.0.0/16			
Name	vpn-pool			
Description				
Network	O Host	O Range	O Network	O FQDN
	192.168.55.0/2	24		
Allow Overrides				

第二步:发夹配置

这种转换方法也称为U-turn,它允许流量通过接收流量的同一接口进行传输。

例如,当Anyconnect配置了Full tunnel拆分隧道策略时,根据NAT免除策略访问内部资源。如果 Anyconnect客户端流量要到达互联网上的外部站点,发夹NAT(或U-turn)负责将流量从外部路由 到外部。

在NAT配置之前,必须创建VPN池对象。

1.创建新的NAT语句,在NAT Rule字段中选择Auto NAT Rule,然后选择Dynamic作为NAT Type。

2.为源接口对象和目标接口对象(外部)选择同一接口:

Add NAT Rule							? ×
NAT Rule: Type:	Auto NAT Rule Dynamic	*	🕑 Enable				
Interface Objects	Translation	PAT Pool	Advance	d			
Available Interface O	bjects 🖒			Source Interface Objects (1)		Destination Interface Objects	5 (1)
Search by name	le	AS	dd to ource dd to tination	outside-zone	÷	outside-zone	
						ок	Cancel

3.在"转换"选项卡中,选择vpn-pool对象作为原始源,然后选择目标接口IP作为转换源,然后选择确 定(如图所示)。

Add NAT Rule				? ×
NAT Rule:	Auto NAT Rule 💙			
Туре:	Dynamic 🗸	🕑 Enable		
Interface Objects	Translation PAT Pool	Advanced		
Original Packet			Translated Packet	
Original Source:*	vpn-pool	v 📀	Translated Source:	Destination Interface IP
Original Port:	TCP		Translated Port:	The values selected for Destination Interface Objects in 'Interface Objects' tab will be used
				OK Cancel

4.这是NAT配置的摘要,如图所示。

Rule	s											
att Fi	Iter by Device	Filter	Rules								× O	Add Rule
						Original Packet			Translated Packet		1	
	Direction	Туре	Source Interface Obje	Destination Interface Obje	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
• N.4	T Rules Before											
1	*	Static	📩 inside-zone	📩 outside-zone	FTDv-Inside-SUPERNE	💭 vpn-pool		FTDv-Inside-SUPERNE	📰 vpn-pool		Ons:false route-looku no-proxy-ar	26
Au	to NAT Rules											
	+	Dyna	📩 outside-zone	📩 outside-zone	👳 vpn-pool			🍓 Interface			🔩 Dns:false	00
* N#	T Rules After											

5.单击保存并部署更改。

验证

使用本部分可确认配置能否正常运行。

在FTD命令行中运行这些命令。

- · sh crypto ca certificates
- show running-config ip local pool
- show running-config webvpn
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

故障排除

当前没有可用于此配置的特定故障排除信息。</>

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)。