在FTD上配置SSL AnyConnect管理VPN

目录

简介 先决条件 要求 使用的组件 背景信息 限制 配置 配置 步骤1.创建AnyConnect管理VPN配置文件 步骤2.创建AnyConnect VPN配置文件 步骤3.将AnyConnect管理VPN配置文件和AnyConnect VPN配置文件上传到FMC 步骤4.创建组策略 步骤5.创建新的AnyConnect配置 步骤6.创建URL对象 步骤7.定义URL别名 验证 故障排除

简介

本文档介绍如何在由思科Firepower管理中心(FMC)管理的思科Firepower威胁防御(FTD)上配置 Cisco AnyConnect管理隧道。 在下面的示例中,安全套接字层(SSL)用于在FTD和Windows 10客户 端之间创建虚拟专用网络(VPN)。

作者:思科TAC工程师Daniel Perez Vertti Vazquez。

先决条件

要求

Cisco 建议您了解以下主题:

- Cisco AnyConnect配置文件编辑器
- 通过FMC进行SSL AnyConnect配置。
- 客户端证书身份验证

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FTD版本6.7.0(内部版本65)

- •思科FMC版本6.7.0(内部版本65)
- 安装在Windows 10计算机上的Cisco AnyConnect 4.9.01095

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

从版本6.7开始,思科FTD支持配置AnyConnect管理隧道。此修复先前打开的增强请<u>求</u> <u>CSCvs78215</u>。

AnyConnect管理功能允许在终端完成其启动后立即创建VPN隧道。用户无需手动启动 AnyConnect应用,只要其系统通电,AnyConnect VPN代理服务就会检测管理VPN功能,并使用 AnyConnect管理VPN配置文件的服务器列表中定义的主机条目启动AnyConnect会话。

限制

- 仅支持客户端证书身份验证。
- Windows客户端仅支持计算机证书存储区。
- Cisco Firepower设备管理器(FDM)CSCvx90058不支持。
- Linux客户端不支持。

配置

配置

步骤1.创建AnyConnect管理VPN配置文件

打开AnyConnect配置文件编辑器以创建AnyConnect管理VPN配置文件。管理配置文件包含终端启动后用于建立VPN隧道的所有设置。

在本示例中,定义了指向完全限定域名(FQDN)dperezve.jyoungta-labdomain.cisco.com的服务器列 表条目,并选择SSL作为主协议。要添加服务器列表,请导航到**服务器**列表并**选择**添加按钮,填写 所需字段并保存更改。

4	AnyConnect	Profile	Editor -	VPN
---	------------	---------	----------	-----

Serve	r Load Balancing Servers	SCEP Mobile Certificate Pinning	
Pr	rimary Server		Connection Information
	Display Name (required)	AnyConnect_Management_Tunnel	Primary Protocol SSL V
	FQDN or IP Address	User Group	ASA gateway
	dperezve.jyoungta-labdom	ain.cisc / AnyConnect_Management_Tunnel	Auth Method During IKE Negotiation EAP-A
	Group URL		IKE Identity (IOS gateway only)
	dperezve.jyoungta-labdom	ain.cisco.com/AnyConnect_Management_Tunne	
		Backup Servers	bba
		Host Address	Add
			Move Up
			Move Down
			Delete
		OK Cancel	

 \times

除服务器列表外,管理VPN配置文件还必须包含一些必需首选项:

- AutomaticCertSelection必须设置为true。
- AutoReconnect必须设置为true。
- •必须为ReconnectAfterResume配置AutoReconnectBehavior。
- •自动更新必须设置为false。
- BlockUntrustedServers必须设置为true。
- •必须为MachineStore配置CertificateStore。
- CertificateStoreOverride必须设置为true。
- •必须将EnableAutomaticServerSelection设置为false。
- EnableScripting必须设置为false。
- RetainVPNOnLogoff必须设置为true。

在AnyConnect配置文件编辑器中,导航**至"首选项(第1部分)"**并调整设置,如下所示:

File Help

VPN	Preferences (Part 1) Profile:npect -ETD-Lab\ XML_Profile\AnyConnect_Management_Tunnel xmL						
Preferences (Part 2) Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	Profile:nnect -r TD-Labl.XML Profile Use Start Before Logon Show Pre-Connect Message Certificate Store Windows Machine macOS All Certificate Store Override Auto Connect On Start	User Controllable	^				
	 Minimize On Connect Local Lan Access Disable Captive Portal Detection Auto Reconnect Auto Reconnect Behavior ReconnectAfterResume 	 ✓ User Controllable ✓ User Controllable ✓ User Controllable User Controllable User Controllable 					
	Auto Update RSA Secure ID Integration Automatic Windows Logon Enforcement	User Controllable					
	SingleLocalLogon Windows VPN Establishment AllowRemoteUsers i	Help	~				

然后导航至"首**选项(第2部分)",并取**消选中"禁**用自动证书选**择"选项。

 \Box \times

File Help

VPN	Preferences (Part 2 Profile:nnect -FTI) D-Lab\.XML Profile\AnyConne	ect_Management_Tunnel.xml	
Backup Servers	Disable Automatic (Certificate Selection	User Controllable	^
Certificate Matching	Proxy Settings	Native	✓ User Controllable	
Mobile Policy	F	Public Proxy Server Address: Note: Enter public Proxy Server add	ress and Port here. Example:10.86.125.33:8080	
	Allow Local Proxy C	Connections		
	Enable Optimal Gat	eway Selection	User Controllable	
	Suspension Time	Threshold (hours)	4	
	Performance Impr	ovement Threshold (%)	20	
	Automatic VPN Poli Trusted Network F	cy Policy	Disconnect ~	
	Untrusted Network	Policy	Connect ~	
	Trusted DNS Dom	ains		
	Trusted DNS Serv Note: addir	ers Ig all DNS servers in use is recomm	ended with Trusted Network Detection	
	Trusted Servers @ https://	<pre>0 https://<server>[:<port>]</port></server></pre>	Add	
			Delete	
				~
		👔 Help		

步骤2.创建AnyConnect VPN配置文件

除管理VPN配置文件外,还需要配置常规AnyConnect VPN配置文件。AnyConnect VPN配置文件 用于首次连接尝试,在此会话期间从FTD下载管理VPN配置文件。

使用AnyConnect配置文件编辑器创建AnyConnect VPN配置文件。在这种情况下,两个文件都包含 相同的设置,因此可以遵循相同的步骤。

步骤3.将AnyConnect管理VPN配置文件和AnyConnect VPN配置文件上传到FMC

创建配置文件后,下一步是将其作为AnyConnect文件对象上传到FMC。

要将新的AnyConnect Management VPN配置文件上传到FMC,请导航到**Objects > Object** Management,然后从目录中选择**VPN** 选项,然后选择Add AnyConnect File按钮。

为文件提供名称,选择AnyConnect Management VPN Profile**作为文**件类型并保存对象。

 \times



现在,要上传AnyConnect VPN配置文件,请再次导航到**Objects > Object Management**,然后从目 录中选择**VPN**选项,然后选择**Add AnyConnect File**按钮。

为文件提供名称,但此时选择AnyConnect VPN Profile作为文件类型并保存新对象。

Overview Analysis Policie	s Devices Objects	AMP Intelligen	ce				. Deploy System Help ▼ d	perezve 🔻
Object Management Intrus	sion Rules							
AnyConnect File File objects represent files used in co	nfigurations, typically for remot	e access VPN policies.	They can contain AnyConnect Client Profile and A	AnyConnect Clier	nt Image	files.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
Security Intelligence DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	.9.01095-webd	AnyConnect Client Image	205
Network Lists and Feeds NPL Lists and Feeds	AnyConnect_Management_Tu					gement_Tunne	AnyConnect Management VPN Profile	2 🖉 🖯
Sinkhole	SSL_AnyConnect.xml	Name:*	SSL_AnyConnect.xml			aml	AnyConnect VPN Profile	203
्ञ्स SLA Monitor ब्रा Time Range		File Name:*	SSL_AnyConnect.xml	Browse				
🗑 Time Zone		File Type:*	AnyConnect VPN Profile	~				
Tunnel Zone		Description:	AnyConnect Client Image	^				
\$ Variable Set		Description	AnyConnect VPN Profile AnyConnect Management VPN Profile					
📎 VLAN Tag			AMP Enabler Service Profile					
A BO VPN			Feedback Profile					
ManyConnect File			ISE Posture Profile	L.				
R. Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile					
IKEv1 IPsec Proposal			Umbrella Roaming Security Profile					
IKEV1 Policy			web security service Profile	Ŷ				_
IKEV2 IPSec Proposal						Displaying	1 - 3 of 3 rows 🔣 🐇 Page 🚺 of 1) >> C
Let many V						2.5pm Jung		
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115	i.cisco.com	How To					uluilu cisco

必须将配置文件添加到对象列表并分别标记为**AnyConnect Management VPN Profile和**AnyConnect VPN配**置文件**。

Overview Analysis Policie	es Devices Objects AMP Intelligence		. Deploy System Help ▼ 🛛	lperezve 🔻
Object Management Intrus	sion Rules			
AnyConnect File File objects represent files used in co	onfigurations, typically for remote access VPN policies. They can contain	a AnyConnect Client Profile and AnyConnect Client Image files.	O Add AnyConnect File	
Security Group lag	Name	Value	Туре	
Security Intelligence DNS Lists and Feeds	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-	webd AnyConnect Client Image	2 🧷 🖯
Network Lists and Feeds URL Lists and Feeds	AnyConnect_Management_Tunnel	AnyConnect_Management_	Tunne AnyConnect Management VPN Profile	2 🦉 🖯
Sinkhole	SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile	2 🥒 🖯
🗑 Time Range				
Cone Cone				
\$ Variable Set				
VLAN Tag				
AnyConnect File				
Group Policy				
IKEv1 IPsec Proposal IKEv1 Policy				
IKEv2 IPsec Proposal IKEv2 Policy v	¢	Displ	aying 1 - 3 of 3 rows 🛛 🐇 🐇 Page 1 of	→ 1 > > C
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com	How To		uluilu cisco

步骤4.创建组策略

要创建新组策略,请导航到Objects > Object Management并从目录中选择VPN选项,然后选择 Group Policy并单击Add Group Policy按钮。

打开"**添加组策**略"窗口后,指定名称,定义AnyConnect池并打开"AnyConnect"**选项**卡。导航至 **Profile**,并在Client Profile下拉菜单中选择表示常规AnyConnect VPN Profile**的对**象。



然后导航至**Management Profile选**项卡,并在Management Profile下拉菜单中选择包含 **Management VPN Profile**的对象。



保存更改以将新对象添加到现有组策略。

Overview Analysis Policie	ies Devices Objects AMP Intelligence	ystem Help v dperezve v
Object Management Intrus	usion Rules	
Group Policy	Add Group Poli	ry Rilter
A Group Policy is a set of attribute ar profile.	and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is ob	tained from the current connection
Security Group lag	^ Name	
Security Intelligence	Nanc	
DNS Lists and Feeds	AnyConnect_Management_Tunnel	Ø 🖥
Network Lists and Feeds	DftfGraphicy	18
URL Lists and Feeds		•
Sinkhole		
SLA Monitor		
Time Range		
💮 Time Zone		
Tunnel Zone		
() URL		
S Variable Set		
S VLAN Tag		
A NON		
MnyConnect File		
R. Certificate Map		
Group Policy		
IKEv1 IPsec Proposal		
IKEv1 Policy		
IKEv2 IPsec Proposal		
IKEV2 Policy	Displaying 1 - 2 of 2 rows	< < Page 1 of 1 > > C
		بالبياب
Last login on Saturday, 2021-03-27 at	How To	cisco

步骤5.创建新的AnyConnect配置

在FMC中配置SSL AnyConnect由4个不同步骤组成。要配置AnyConnect,请导航**到Devices > VPN** > **Remote Access,**然后选择**Add**按钮。这必须打开"远**程访问VPN策略向导"**。

在**Policy Assigment** 选项卡上,选择手边的FTD设备,定义连接配置文件的名称并选中SSL复选框。

Overview Analysis Policies Dev Dashboards • Reporting Summary	ces Objects AMP Intellige	ence	$oldsymbol{ heta}_i$ Deploy Sys	tem Help v dperezve v					
Remote Access VPN Policy W	Remote Access VPN Policy Wizard								
1 Policy Assignment 2 Cor	nection Profile > 🌖 AnyCon	nnect 🔰 🕘 Access & Certificate 🔰 5	Summary						
Targeted Dev This wizard will a new user-defin Name:* Description: VPN Protocols: Targeted Device	ices and Protocols uide you through the required minimal side connection profile. AnyConnect_Management_Tunnel SSL IPsec-IKEv2 Available Devices Available Devices Content of the second	Add	Before You Start Before you start, ensure the following complete Remote Access VPN Policy. Dutentication Server Authentication VPN clients. Difigure Realm or RADIUS Server Group or SSO to authenticate VPN clients. Mare sure you have AnyConnect package for VPN Client downloaded or you have herelevant Cisco credentials to download it during the wizard. Device Interface Interfaces should be already configured on targeted devices so interface group to enable VPN access.						
			Back	Next Cancel					
Last login on Thursday, 2021-03-25 at 17:01:05	M from rtp-vpn6-107.cisco.com	How To		uluiu cisco					

在连**接配置文件**上,**选择Client Certificate Only**作为身份验证方法。这是该功能支持的唯一身份验 证。



然后在Group Policy下拉列表中选择在步骤3中创建的Group Policy对象。

Overview Analysis Policies Devices Objects AMP Intelli	gence	₽ ₁ Deploy	y System	Help 🔻	dperezve 🔻
Device Management NAT VPN > Remote Access QoS Platfo	rm Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
1 Policy Assignment 2 Connection Profile 3 AnyCo	onnect $>$ 4 Access & Certificate $>$ 5 Summary				
Authorization Server:	(Realm or RADIUS)				·
Accounting Server:	V (RADIUS)				
Client Address Assignment: Client IP address can be assigned from A assignment is tried in the order of AAA se	AA server, DHCP server and IP address pools. When multiple options are selected, II rver, DHCP server and IP address pool.	address			
Use AAA Server (Realm or RAD Use DHCP Servers Use IP Address Pools	IUS only) 🕕				
IPv4 Address Pools: An	yConnect-Pool 🥜				_
IPv6 Address Pools:	Ø				
Group Policy:					
A group policy is a collection of user-orier or create a Group Policy object.	nted session attributes which are assigned to client when a VPN connection is establ	shed. Select			
Group Policy:*	VConnect_Management_Tunnel OftGrpPolicy				
		Back	Next		Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To	i i			ululu cisco

在AnyConnect选项卡上,根据终端上的操作系统(OS)选择AnyConnect File Object。

Overview Analysis Policies	Devices Objects AMP Inte	lligence		. Deploy Sy	stem Help v	dperezve 🔻
Device Management NAT V	VPN Remote Access QoS Pla	tform Settings FlexConfig Certificate	S			
Remote Access VPN Poli	icy Wizard					
1 Policy Assignment 2	2) Connection Profile 3 Any	Connect 4 Access & Certificate	5 Summary			
			ААА			^
	AnyConnect Client Image The VPN gateway can automatically down initiated. Minimize connection setup time b	load the latest AnyConnect package to the client y choosing the appropriate OS for the selected pa	device when the VPN connection is ckage.			
	Download AnyConnect Client packages from	n Cisco Software Download Center.	Show Re-order buttons			- 1
	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System			
	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095-webdeploy-k9.pkg	Windows			
						×
				Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19	9:12:55 PM from rtp-vpn1-1115.cisco.com	How To				uluilu cisco

在Access & Certificate上,指定FTD必须使用的证书,以探测Windows客户端的身份。

注意:由于用户在使用管理VPN功能时不应与AnyConnect应用交互,因此证书需要完全受信 任,并且不得打印任何警告消息。

注意:为防止证书验证错误,证书的使用者名称中包含的公用名称(CN)字段必须与XML配置 文件服务器列表中定义的FQDN匹配(步骤1和步骤2)。



最后,在"摘要"选项卡上选择"完成"按钮以添加新的AnyConnect配置。



步骤6.创建URL对象

导航至**对象>对象管**理,**然后从**目录中选择URL。然后在"**添加URL**"下**拉菜单中**选择"添加对象"。

为对象提供名称,并使用在管理VPN配置文件服务器列表中指定的相同FQDN/用户组定义URL(步骤2)。 在本例中,URL必须为dperezve.jyoungtalabdomain.cisco.com/AnyConnect_Management_Tunnel。

Overview Analysis Policie	es Devices Objects	AMP Intelligend	ce		. ■ Deploy	System Help v dperezve	
Object Management Intrus	sion Rules						
URL	r IP address. You can use URI	objects and groups in va	rious places, including access control p	olicies and event searches. For	Add URL	Filter Show Unused Objects scontrol rule that blocks a specifi	
Cogurity Croup Tha	Name	objecto ente groupe in co		Valu	10	Override	
Security Group Tag	Maine			Valu	c	overnue	
DNS Lists and Foods			No reco	rde to dieplay			
Network Lists and Feeds		New URL Obje	NO TECO	2 X			
URL Lists and Feeds		New OKL ODJe	icts				
Sinkhole		Name	Management_Tunnel				
SLA Monitor		Description					
Time Range							
🕣 Time Zone							
and Tunnel Zone		URL	https://dperezve.jyoungta-labdoma				
() URL		Allow Overrides					
\$ Variable Set							
VLAN Tag				Save Cancel			
A PVN							
ManyConnect File							
R. Certificate Map							
Group Policy							
IKEv1 IPsec Proposal							
IKEv1 Policy							
REV2 IPsec Proposal					No data to display	<pre><< Page 1 of 1 > ></pre>	e)
			How To			-1[1-1] CISCO	5

保存更改以将对象添加到对象列表。

步骤7.定义URL别名

要启用AnyConnect配置中的URL别名,请导航至**Devices > VPN > Remote Access**,然后单击铅笔 图标进行编辑。

然后,在"连接配置文件"选项卡上,选择现有配置,导航至"别名",单击"添加"按钮并在"URL别名 "下拉**菜单中选**择"URL对象"。确保选**中"**已启用"复选框。

Overview Analysis Policies Device	Edit Connection Profile	? ×	🎙 Deploy System Help 🔻 dperezve 🔻
Device Management NAT VPN > Rem AnyConnect_Management_ Enter Description	Connection Profile:* AnyConnect_Management_Tunnel Group Policy:* AnyConnect_Management_Tunnel Edit Group Policy		E Delice Accimenter (1)
Connection Profile Access Interfaces	Client Address Assignment AAA Aliases		Policy Assignments (1)
Name DefaultWEBVPNGroup	Alias Names: Add URL Alias ? Incoming users can ch can be turned on or of Name OK Cancel	n this device	© ∕ 3
AnyConnect_Management_Tunnel			nel 🥔 🖥
	URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the for system will automatically log them in via this connection profile.	ollowing URLs,	
	URL Status		
	Save	Cancel	
Last login on Monday, 2021-04-05 at 23:55:27 PM from	rtp-vpn4-759.cisco.com How To		

保存更改并将配置部署到FTD。

验证

部署完成后,需要与AnyConnect VPN配置文件进行第一个手动AnyConnect连接。在此连接期间 ,管理VPN配置文件从FTD下载并存储在C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中。此时,必须通过管理VPN配置文件启动后续连接,无需任何用 户交互。

故障排除

对于证书验证错误:

- •确保FTD上已安装证书颁发机构(CA)的根证书。
- •确保在Windows计算机存储上安装由同一CA签名的身份证书。
- •确保CN字段包含在证书中,并且与在URL别名中定义的管理VPN配置文件和FQDN的服务器列 表中定义的FQDN相同。

对于管理隧道未启动:

•确保已下载管理VPN配置文件并将其存储在C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中。

•确保管理VPN配置文件的名称**为VpnMgmtTunProfile.xml**。 有关连接问题,请收集DART捆绑包并联系Cisco TAC以进一步研究。