在 ASA 上配置 AnyConnect 管理 VPN 隧道

目录

<u>筒介</u> <u>先决条件</u> <u>要求</u> 使用的组件 <u>背景信息</u> 管理隧道的运行 限制 配置 通过ASDM/CLI在ASA上进行配置 创建AnyConnect管理VPN配置文件 AnyConnect管理VPN配置文件 AnyConnect管理VPN配置文件的部署方法 (可选)配置自定义属性以支持全隧道配置 验证 故障排除 相关信息

简介

本文档介绍如何将ASA配置为VPN网关通过管理VPN隧道接受来自Cisco AnyConnect安全移动客户端的连接。

先决条件

要求

Cisco 建议您了解以下主题:

- 通过自适应安全设备管理器(ASDM)配置VPN
- •基本自适应安全设备(ASA)CLI配置
- •X509证书

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ASA软件版本9.12(3)9
- 思科ASDM软件版本7.12.2
- Windows 10与Cisco AnyConnect安全移动客户端4.8.03036版

注意:下载AnyConnect VPN Web部署软件包(anyconnect-win*.pkg or anyconnect-macos*.pkg)下载思科 软<u>件(</u>仅限注册客户)。将AnyConnect VPN客户端复制到要下载到远程用户计算机的ASA的闪 存中,以与ASA建立SSL VPN连接。有关详细信息,请参阅ASA配置指南的<u>安装</u> 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

管理VPN隧道可确保在客户端系统启动时连接到企业网络,而不仅仅是在最终用户建立VPN连接时 。您可以在办公室外终端(尤其是用户通过VPN不经常连接到办公室网络的设备)上执行补丁管理 。需要企业网络连接的终端OS登录脚本也受益于此功能。

AnyConnect Management Tunnel允许管理员在用户登录之前将AnyConnect连接起来,而无需用户 干预。AnyConnect管理隧道可与受信任网络检测结合使用,因此仅当终端位于外部并与用户发起的 VPN断开连接时才会触发。AnyConnect管理隧道对最终用户是透明的,并在用户启动VPN时自动断 开。

操作系统/应用	最低版本要求
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect版本	4.7.00136
macOS AnyConnect版本	4.7.01076
Linux	不支持

管理隧道的运行

AnyConnect VPN代理服务在系统启动时自动启动。它检测到管理隧道功能已启用(通过管理 VPN配置文件),因此它会启动管理客户端应用以启动管理隧道连接。管理客户端应用使用管理 VPN配置文件中的主机条目发起连接。然后VPN隧道会照常建立,但有一个例外:管理隧道连接期 间不会执行软件更新,因为管理隧道对用户是透明的。

用户通过AnyConnect UI启动VPN隧道,这将触发管理隧道终端。管理隧道终止后,用户隧道的建 立会照常继续。

用户断开VPN隧道,从而触发管理隧道的自动重建。

限制

配置

- 不支持用户交互
- 仅支持通过计算机证书存储区(Windows)进行的基于证书的身份验证
- 实施严格的服务器证书检查
- 不支持专用代理
- 不支持公共代理(在未从浏览器检索本地代理设置的平台上支持ProxyNative值)
- 不支持AnyConnect自定义脚本

注意:有关详细信息,请参阅<u>关于管理VPN隧道。</u>

本节介绍如何将Cisco ASA配置为VPN网关,以通过管理VPN隧道接受来自AnyConnect客户端的连接。

通过ASDM/CLI在ASA上进行配置

步骤1:创建AnyConnect组策略。导航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.点击 Add.

注意:建议创建仅用于AnyConnect管理隧道的新AnyConnect组策略。

S	Home 🍕 Configuration 📴 Monitoring 识	Save 🔇 Refresh 🔇 Back 🔘 Forv	vard ? Help Type topic Go			dialo cisco				
	O O Remote Access VPN	Configuration > Remote Ac	cess VPN > Network (Client) Acces	s > Group Policies						
ks 💼 Device List	Introduction AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes	roup is a collection of user-oriented VPN connection profiles and user ac from an LDAP server you must use a isign	authorization attribute/value pairs that may be stored in counts. n <u>LDAP attribute map</u> .	iternally on the device or externally on a RADIUS/LDAP server. The group	•				
2	AnyConnect Client Software		-		Connection Profiles /Users	_				
ookr	UP Dynamic Access Policies	Name	Туре	Tunneling Protocol	Assigned To					
68 [***]	Bi Procestion Profiles	AnyConnect	Internal	ssi-client	AnyConnect					
	IPsec(IKEv2) Connection Profiles	DfitGrpPolicy (System Default)	Internal	ikev1;ikev2;i2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Defa	IKWE				
	Secure Mobility Solution									
	Address Assignment									
	Advanced									
	Clientless SSL VPN Access									
	AAA/Local Users									
	AAA Server Groups									
	LDAP Attribute Map									
	SI Local Users									
	Gastificate Manager									
	Language Localization									
	%ª Load Balancing									
	PDHCP Server									
	J DNS									
	Advanced									
	R Device Setue									
	Device Setup									
	Firewall									
	Kemote Access VPN									
	Site-to-Site VPN	Find:	Match Case							
	Device Management			Reset Apply						
	-	* Keset Appry								

第二步:提供 Name 组策略。分配/创建 Address Pool.选择 Tunneling Protocols 作为 SSL VPN Client 和/或 IPsec IKEv2,如图所示.

9. 🛡		Edit Internal Group Policy: AnyConnect_MGM1_runnel	
General	Name: AnyConnect_MGMT_	Tunnel	
Advanced	Banner: 🗹 Inherit		
	SCEP forwarding URL: 🗹 Inherit		
	Address Pools: Inherit VPN_P	ool	Select.
	IPv6 Address Pools: 🗸 Inherit		Select.
	More Options		_
	Tunneling Protocols:	Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/	IPsec
	Filter:	🗹 Inherit	Manage
	Access Hours:	✓ Inherit 0	Manage
c	Simultaneous Logins:	🗸 Inherit	
	Restrict access to VLAN:	✓ Inherit C	2
	Connection Profile (Tunnel Group) Lock:	☑ Inherit	2
	Maximum Connect Time:	✓ Inherit Unlimited minutes	
	Idle Timeout:	✓ Inherit None minutes	
	Security Group Tag (SGT):	✓ Inherit None (2 – 65519)	
	On smart card removal:	☑ Inherit O Disconnect O Keep the connection	
	Timeout Alerts		
	Maximum Connect Time Alert Interval:	✓ Inherit Default minutes	
	Periodic Certificate Authentication Interva	I: 🔽 Inherit 🗌 Unlimited hours	
Find:	💿 Next	Previous	

第三步: 导航至 Advanced > Split Tunneling.配置 Policy 作为 Tunnel Network List Below 并选择 Network List,如 图所示.

• • •		Edit Internal G	roup Policy: AnyConnect_MGMT_	Tunnel	
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client HPsec(IKEv1) Client	The VPN client makes split tunneling de fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlu	Edit Internal G cisions on the Inherit Inherit Inherit Inherit Inherit Sion for Web S	roup Policy: AnyConnect_MGMT_ basis of a network list that can Yes No Tunnel Network List Below VPN-Split security proxies.	funnel be specified below by providing the proper parameters to 'Policy' an	d 'Networl Manag
•	Pressing this button to set up split exlu Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	from Microso	ecunty proxies. ft Clients		
Find:	Next	Previous Help	Cancel OK		

注意:如果未同时为IP协议(IPv4和IPv6)推送客户端地址, Client Bypass Protocol 设置必须为 enabled 以便对应的流量不会受到管理隧道的干扰。要配置,请参阅<u>步骤4</u>。

第四步: 导航至 Advanced > AnyConnect Client. 设置 Client Bypass Protocol 到 Enable. 点击 OK 保存,如图所示。

• •		Add Internal Group Policy	
General	Keep Installer on Client System:	☑ Inherit O Yes O No	
Servers	Datagram Transport Layer Security (DTLS):	☑ Inherit	
Split Tunneling	DTLS Compression:	☑ Inherit	
Browser Proxv	SSL Compression:	☑ Inherit O Deflate O LZS O Disable	
▶ IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	🗹 Inherit 💿 Enable 💿 Disable	
	Client Bypass Protocol:	Inherit O Enable Disable	
	FQDN of This Device:	🗹 FQDN	
	MTU:	🗹 Inherit	
	Keepalive Messages:	☑ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	🗹 Inherit	٢
0	Always-On VPN:	☑ Inherit O Disable O Use AnyConnect Profile setting 0	
	Client Profiles to Download:	🗹 Inherit	
		Add 1 Delete	
		Profile Name Profile Usage/Type	
			- 1
			- 1
			- 1
Find:	Novt A		
rind.	- Next		
		Help Cancel OK	

第五步:如图所示,单击 Apply 将配置推送到ASA。

🔥 Home 🍓 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	ard ? Help Type topic Go		cisco
000 Remote Access VPN	O O Configuration > Remote Acc	ess VPN > Network (Client) Acces	s > Group Policies	
Pintroduction Introduction Pintroduction Pintrodu	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes f Add C C C to the construction attributes f	roup is a collection of user-orientec VPN connection profiles and user ac from an LDAP server you must use a sign	i authorization attribute/value pairs that may be stored in counts. n <u>LDAP attribute map</u> .	iternally on the device or externally on a RADIUS/LDAP server. The group
AnyConnect Client Software	Norma	Track	Toronto Protocol	Connection Profiles/Users
9 BD Crown Policies	Name	Туре	Tunneling Protocol	Assigned To
Psec(IKEv1) Connection Profiles	AnyConnect	Internal	ssi-client	AnyConnect
IPsec(IKEv2) Connection Profiles	DriturpPolicy (System Default)	Internal	ikev2;iztp-ipsec	DefaultkAGroup;Default2LGroup;DefaultADMINGroup;DefaultWE
Secure Mobility Solution	AnyConnect_MGM1_10nnet	internat	ikev2,551=Citerik	panyconnect_wowr_runner
Address Assignment				
Clientless SSL VPN Access				
V 🖌 AAA/Local Users				
AAA Server Groups				
Se LDAP Attribute Map				
g Local Users				
Secure Desktop Manager				
El Certificate Management				
Language Localization				
Sector Balancing				
P DHCP Server				
A DNS				
Advanced				
R Darley Color				
Device Setup				
Firewall				
Remote Access VPN				
Site-to-Site VPN	Find:	Match Case		
Device Management				
5			Reset Apply	

组策略的CLI配置:

```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
```

第六步:创建AnyConnect连接配置文件导航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. 点击 Add.

注意:建议创建仅用于AnyConnect管理隧道的新AnyConnect连接配置文件。

🚳 Home 🤹 Configuration 📝 Monitoring 🔋	🚽 Save 🔇 Refresh 🔇 Back 🌘	Forward 💡 Help Type	topic Go			cisco
OO Remote Access VPN	O O Configuration > Rem	ote Access VPN > Network	(Client) Access > AnyConnect Co	nnection Profiles		
	The security appliance autor VPN Client supports IPsec (IR Access Interfaces Enable Clisco AnyConnec SSL access must be enabled Interface SSL Access autoide	natically deploys the Cisco (EV2) tunnel as well as SSL t t VPN Client access on the if you allow AnyConnect Cl if you allow AnyConnect Cl Enable DTLS Allow	AnyConnect VPN Client to remote us unnel with Datagram Transport Laye interfaces selected in the table below ent to be launched from a browser (I (IRUV2) Access Access Enable Client Services	ers upon connection. The initial r Security (DTLS) tunneling optic V Veb Launch) . Device Certificate	client deployment requires end-use	r administrative rights. The Cisco AnyConnect
 Secure Mobility Solution 	Sypass interface access Access lists from group poli Login Page Setting Allow user to select con Shutdown portal login p Connection Profiles Connection profile (tunnel g	lists for inbound VPN sessi cy and user policy always a nection profile on the login age. roup) specifies how user is	ons pply to the traffic. page. •	You can configure the mapping	from certificate to connection profil	e hers.
INS ▶ 3 Advanced	Add Edit Delete	Find: SSL Enabled	O Match Case IPsec Enabled	Aliases	Authentication Method	Group Policy
	DefaultRAGroup				AAA(LOCAL)	DfltGrpPolicy
	DefaultWEBVPNGroup				AAA(LOCAL)	DfltGrpPolicy
	AnyConnect			AnyConnect	AAA(LOCAL)	AnyConnect
Certice Setup Certice Setup Certice Setup Certice Setup Certice Setup Certice Management Certice Management	Let group URL take prece	edence if group URL and cer	tificate map match different connec	ion profiles. Otherwise, the con	nection profile that matches the cert	ificate map will be used.
*				Reset Apply		

步骤 7.提供 Name 连接配置文件,并设置 Authentication Method 作为 Certificate only.选择 Group Policy 作为 第1步中创建<u>的配置</u>。

Basic	Name:	AnyConnect_MGMT_Tunnel		
Advanced	Aliases:			
	Authentication			
	Method:	Certificate only		
	AAA Server Group:	LOCAL	0	Manage
		Use LOCAL if Server Group fails		
	SAML Identity Provider			
	SAML Server :	None	0	Manage
	Client Address Assignment			
	DHCP Servers:			
		• None OHCP Link OHCP Subnet		
	Client Address Pools:			Select
	Client IPv6 Address Pools:			Select
	Default Group Policy			
	Group Policy:	AnyConnect_MGMT_Tunnel	٥	Manage
	(Following fields are linked	t to attribute of the group policy selected above.)		
	🗹 Enable SSL VPN clier	nt protocol		
	✓ Enable IPsec(IKEv2)	client protocol		
	DNS Servers:			
	WINS Servers:			
	Domain Name:			
Find:		Next Previous		

注意:确保ASA上存在来自本地CA的根证书。 导航至 Configuration > Remote Access VPN > Certificate Management > CA Certificates 添加/查看证书。

注意:确保同一本地CA颁发的身份证书存在于计算机证书存储区(适用于Windows)和/或系 统密钥链(适用于macOS)中。

步骤 8导航至 Advanced > Group Alias/Group URL.点击 Add 在 Group URLs 并添加 URL.确保 Enabled 已选中 。点击 OK 保存,如图所示。 Add AnyConnect Connection Profile

Basic V Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securld messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Delete (The table is in-line editable.) Alias
	Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel Cancel OK
Find:	Next Previous
	Help Cancel OK

如果使用IKEv2,请确保 IPsec (IKEv2) Access 在用于AnyConnect的接口上启用。

○ ○ ○ Remote Access VPN	O O Config	uration > Remot	e Access VPN > I	Network (Client) /	Access > AnyConnect Co	nnection Profiles					
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	he security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN lient supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.									
ManyConnect Customization/Local	Access Interfac	:es									
AnyConnect Client Profile	SSL access n	isco AnyConnect	VPN Client access you allow AnyCor	on the interfaces	selected in the table belo aunched from a browser (w Web Launch) .					
Group Policies	Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acc Allow Access	Enable Client Services	Device Certificate					
Prec(KEVI) Connection Profiler	outside	~	~		Image: A start and a start						
Secure Mobility Solution	inside			<u>н</u> е	0	Port Settings					

步骤 9点击 Apply 将配置推送到ASA。

...



连接配置文件(隧道组)的CLI配置:

tunnel-group AnyConnect_MGMT_Tunnel type remote-access tunnel-group AnyConnect_MGMT_Tunnel general-attributes default-group-policy AnyConnect_MGMT_Tunnel tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes authentication certificate group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable

步骤 10确保在ASA上安装受信任证书并绑定到用于AnyConnect连接的接口。导航至 Configuration > Remote Access VPN > Advanced > SSL Settings 添加/查看此设置。

注意:请参阅在ASA上安装身份证书。

O Remote Access VPN	O O Configuration > Remote Acces	ss VPN > Advanced > SSL Settings				
Introduction						
Network (Client) Access	Configure SSL parameters. These para	meters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization AnyConnect Client Profile	The minimum SSL version for the sec	urity appliance to negotiate as a "server":	TLS V1	0	OTLSV1 OTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the sec	urity appliance to negotiate as a "client":	TLS V1	0		
Group Policies	Diffie-Hellman group to be used with	SSL:	Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	0		
Secure Mobility Solution	Encryption					
Standard Address Assignment	Cipher Version	Cinhar Saruribul aud		Cipher Algorithm	e / Custom String	1
3 Advanced	Default	Madium		DES_CRC2_SUA	AFC128_SUA DUE_DCA_AFC128_SUA AFC256_SUA DUE_DCA	Edit
Clientless SSL VPN Access	TISVI	Medium		DHE-PSA-AES2	CE-SUA AECOSE-SUA DUE-DCA-AECIDE-SUA AECIDE-SUA	
AAA/Local Users	TISVI 1	Medium		DHE-RSA-AES2	SG_SHA AES25G_SHA DHE_DCA_AES128_SHA AES128_SHA	
AAA Server Groups	10/1.2	Medium		CONE CODE		
Se LDAP Attribute Map	0710/1	Medium		DUE DEA AFEN	AES230-GUM-SHA304 ECDHE-RSA-AES230-GUM-SHA304 D	
C Local Lisers	010/1	Medium		CODUC CODEA	10-3NA AE3230-3NA DHE-K3A-AE3128-3NA AE3128-3NA	
Secure Deckton Manager	011391.2	Medium		ECDHE-ECDSA-	AES250-GCM-SHA384 ECDHE-KSA-AES250-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing	Conver Name Indication (CNI)					
DHCP Server	Server wame indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						Edit
SSI Settings						CON
Reference Identity						Delete
D Cartificate to Am Connect						
Certificate to AnyConnect						
HITP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Certificates					
	Specify which certificates, if any, s	hould be used for SSL authentication on ea	ch interface. The fallback certificate	will be used on interfa	ces not associated with a certificate of their own.	
	Interface	Drimany Castificate	Lond Polyaging Castificate		Key Ture	
Pevice Setup	Interrace	Primary Cercincate	coad balancing Certificate		Key-Type	Edit
	inside					
irewall	management					
	outside	ROOT-CA:hostname=ASA.example	.co		Primary: RSA (2048 bits), Load Balancing: none	
emote Access VPN						
ite-to-Site VPN						
Device Management						
			Deces Control	h.		

SSL信任点的CLI配置:

ssl trust-point ROOT-CA outside

创建AnyConnect管理VPN配置文件

步骤1: 创建AnyConnect客户端配置文件。导航至 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.点击 Add,如图所示.

1	Home 🥸 Configuration 📴 Monitori	ng 🔚 Save 🔇 Refresh	G Back 🔘 Forward	Help Type topic Go				cisco
	O O Remote Access VPN	0 0 0 Configuration >	Remote Access VPN >	Network (Client) Access > A	nyConnect Client Profile			
oolmarks Device Li	Introduction Introduction AnyConnect Connection Profil AnyConnect Customization/Ltc AnyConnect Cleart Profile AnyConnect Cleart Profile AnyConnect Cleart Profile AnyConnect Cleart Software AnyConnect Software AnyConnect Cleart Software	This panel is used to m button to add a new pr The profile Usage field HostScan configuration	nanage AnyConnect Clien ofile. Pressing the Import is introduced with the Se n can be performed by go nange Group Policy	it Profiles and perform group a t or Export button is for uploas cure Mobility Solution. This fi sing to Secure Desktop Manage elete El Import & Export	ssignment for AnyConnect and download of client p eld contains different profi r/HostScan. If 'HostScan' i /alidate	version 2.5 or later.You can sel rofiles between local machine ar le usage in AnyConnect version s not visible under 'Secure Desk	ect a profile to edit, change group or to delete. You can select the 'Add' d device. 3.0 and later. top Manager', you will need to restart ASDM.	
	Psec(IKEv1) Connection Profil	Profile Name		Profile Usage		Group Policy	Profile Location	
	PrecKIEV2 Connection Profil Secure Mobility Solution Address Assignment Genetics SSL VPN Access Advanced Advanced Advanced Server Croups Advanced VERKEN Connection Cateway Other Server Load Balancing Other Server Connection Cateway SSL Settings							
	Reference Identity Crypto Engine Crypto Engine							
	Device Setup							
	Firewall							
	Site-to-Site VPN							
	Device Management				Reset	Apply		

第二步:提供 Profile Name.选择 Profile Usage 作为 AnyConnect Management VPN profile.选择 Group Policy <u>第</u> 1步<u>中创建</u>。点击 OK ,如图所示.

ofile Name		Profile Usage	Group Policy	Profile Location
	• • •	Add AnyConnect Client Prof	ile	
	Profile Name	AnyConnect_MGMT_Profile		
	Profile Usage	AnyConnect Management VPN Profile	0	
	Enter a device f created if it do	ile path for an xml file, ie. disk0:/ac_profile. The file will es not exist.	l be automatically	
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Browse Flash	
			Upload	
	Group Policy	AnyConnect_MGMT_Tunnel	0	
		Enable 'Always On VPN' for selected group		
		Help Cancel	OK	
			Reset Apply	

第三步:选择已创建的配置文件,然后点击 Edit,如图所示.



第四步:导航至 Server List.点击 Add 添加新的服务器列表条目,如图所示。

4					Ab
/PN Preferences (Part 1)	Server List				
Preferences (Part 2)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Matching					
Server List					
	Note: at most o	one server can be defined	l in a management VP	N profile. Add	Delete
				Edit	Details

第五步:提供 Display Name.添加 FQDN/IP address 的ASA。提供 User Group 作为隧道组名称。 Group URL 自动填入 FQDN 和 User Group.点击 OK.

	Server Certificate Pinning
Primary Server Display Name (required) AnyConnect_M FQDN or IP Addr User Gr asa.example.com / AnyCo Group URL asa.example.com/AnyConnect_MGMT_Tu	_MGMT_Tunnel _MGMT_Tunnel Primary Protocol Scoup (required) Connect_MGMT_ Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up Move Down Delete
	OK Cancel

注意:FQDN/IP地址+用户组必须与步骤8中配置AnyConnect连接配置文件时提到的组URL<u>相</u> <u>同</u>。

注意:将IKEv2用作协议的AnyConnect也可用于建立到ASA的管理VPN。确保 Primary Protocol 设置为 IPsec 在<u>步骤5</u>中。

第六步:如图所示,单击 OK 保存。

8 🔿 🖶	Any	Connect Client Profile Edi	tor - AnyConnect_MGN	IT_Profile	
Profile: AnyConnect_MG	MT_Profile				About
VPN	Server List				
[©] Preferences (Part 2)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Pinning	AnyConnect_MGM	T_T asa.example.com	AnyConnect_MGMT	_T Inherited	
Server List					
	Note: at most o	ne server can be defined	in a management VPN	profile. Add	Delete
				Edit	Details
		lista		1	
		нер Са		1	

步骤 7.点击 Apply t将配置推送到ASA,如图所示。

🚮 Hor	me 🔧 Configuration 📴 Monito	ing 识 Save 🔇 Refresh 🔇 Back 🔘	Forward 💡 Help Type topic Go			cisco
0	O O Remote Access VPN	O O Configuration > Remote Acce	ess VPN > Network (Client) Access > AnyConnect (Client Profile		
vice List	? Introduction Network (Client) Access	This panel is used to manage AnyCon	nnert Client Profiles and perform group assignment fr	or AnyConnect version 2.5 or later You can select a pro	file to edit, change group or to delete. You can select the 'Add'	
8	AnyConnect Connection Profil AnyConnect Customization/Lc	button to add a new profile. Pressing The profile Usage field is introduced	the Import or Export button is for upload and downlo with the Secure Mobility Solution. This field contains	oad of client profiles between local machine and device different profile usage in AnyConnect version 3.0 and	later.	
arks	AnyConnect Client Profile MayConnect Client Software	HostScan configuration can be perfor	rmed by going to Secure Desktop Manager/HostScan.	If 'HostScan' is not visible under 'Secure Desktop Man	ager', you will need to restart ASDM.	
Bookm	Poinces Policies	🗣 Add 🗹 Edit 🔀 Change Group Po	olicy 📋 Delete 🛃 Import 🖏 Export 🔊 Validate			
	IPsec(IKEv1) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	IPsec(IKEv2) Connection Profil	AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm	
	Secure Mobility Solution					
	Address Assignment					
	Advanced					
P.	Clientless SSL VPN Access					
Ψ.	AAA/Local Users					
	AAA Server Groups					
	Mag LDAP Attribute Map					
	1 Local Users					
P	Manager					
P.	Certificate Management					
	🔯 Language Localization					
	Set Load Balancing					
	DHCP Server					
	A DNS					
Ψ.	3 Advanced					
	2 Connection Gateway					
	SSL Settings					_
	Reference Identity					
	Certificate to AnyConnect and					
	HTTP Redirect					
	Maximum VPN Sessions					
	SI Crypto Engine					
3	Device Setup					
Ę	Firewall					
3	Remote Access VPN					
8	Site-to-Site VPN					
	Device Management			Reset Apply		
	÷					

添加AnyConnect管理VPN配置文件后的CLI配置。

webvpn enable outside hsts enable max-age 31536000 include-sub-domains no preload no anyconnect-essentials anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm anyconnect enable tunnel-group-list enable cache disable error-recovery disable 1 group-policy AnyConnect_MGMT_Tunnel internal group-policy AnyConnect_MGMT_Tunnel attributes vpn-tunnel-protocol ikev2 ssl-client split-tunnel-network-list value VPN-Split client-bypass-protocol enable address-pools value VPN_Pool webvpn anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt

AnyConnect客户端计算机上的AnyConnect管理VPN配置文件:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<UseStartBeforeLogon UserControllable="false">false"/schemas.xmlsoap.org/encoding/
```

<ShowPreConnectMessage>false</ShowPreConnectMessage>

```
<ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
```

--- Output Omitted ---

```
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

注意:如果用户AnyConnect VPN配置文件中使用了受信任网络检测(TND),则建议匹配管理 VPN配置文件中相同的设置,以获得一致的用户体验。根据应用到用户VPN隧道配置文件的 TND设置触发管理VPN隧道。此外,管理VPN配置文件中的TND Connect操作(仅在管理 VPN隧道处于活动状态时实施)始终应用于用户VPN隧道,以确保管理VPN隧道对最终用户 透明。

注意:在任何最终用户PC上,如果管理VPN配置文件启用了TND设置,且用户VPN配置文件 缺失,则它会考虑TND的默认首选项设置(在AC客户端应用中的默认首选项中禁用),以代 替缺失的用户VPN配置文件。这种不匹配可能导致意外/未定义的行为。

默认情况下,TND设置在默认首选项中禁用。

要克服AnyConnect客户端应用中的默认首选项硬编码设置,最终用户PC必须拥有两个VPN配 置文件,一个用户VPN配置文件和一个AC管理VPN配置文件,并且两者必须具有相同的 TND设置。

管理VPN隧道连接和断开背后的逻辑是,为了建立管理VPN隧道,AC代理使用用户VPN配置 文件TND设置,并且对于断开管理VPN隧道,它检查管理VPN配置文件TND设置。

AnyConnect管理VPN配置文件的部署方法

 使用ASA连接配置文件成功完成用户VPN连接,以便从VPN网关下载AnyConnect管理VPN配置 文件。

注意:如果用于管理VPN隧道的协议是IKEv2,则需要通过SSL建立第一个连接(为了从 ASA下载AnyConnect管理VPN配置文件)。

AnyConnect管理VPN配置文件可以通过GPO推送或手动安装手动上传到客户端计算机(确保配置文件名称为 VpnMgmtTunProfile.xml影响。

需要添加配置文件的文件夹位置:

Windows 窗口版本: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun macOS: /opt/cisco/anyconnect/profile/mgmttun/

(可选)配置自定义属性以支持全隧道配置

默认情况下,管理VPN隧道需要包括隧道配置的分割以避免对用户发起的网络通信的影响。在用于 管理隧道连接的组策略中配置自定义属性时,可以覆盖此属性。

步骤1:导航至Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. 点击 Add,如图所示.



步骤 2将自定义属性Type设置为 ManagementTunnelAllAllowed 并提供 Description. 点击 OK,如图所示.

		Description	1	
• • •	Create Custom Attr	ribute Type		
Type:	Create Custom Attr	ribute Type		
Type:	Create Custom Attr anagementTunnelAllAllowed anagementTunnelAllAllowed	ribute Type		
Type: M Description:	Create Custom Attr anagementTunnelAllAllowed anagementTunnelAllAllowed	ribute Type		
Type: M Description:	Create Custom Attr anagementTunnelAllAllowed anagementTunnelAllAllowed	ribute Type		

第三步: 导航至 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. 点击 Add,如图所示.



第四步:选择"类型"作为 ManagementTunnelAllAllowed. 将名称设置为 true.点击 Add提供自定义属性值 ,如图所示。

me Values		
•	Create Custom Attribute N	ame
Type:	ManagementTunnelAllAllowed	ᅌ Manage
Name:	true	
	Value	Add
		Edit
		Delete
Configure Values:		
comigure values.		

第五步:将值设置为 true.点击 ок,如图所示.

0.0.0

		Create Custom Attribute N	ame	
Type:	ManagementTunnel	AllAllowed	٥	Manage
Name:	true			
	Value		Add	
•		Add Value	P.0.	
true				
true				
Value:				

第六步:导航至 Configuration > Remote Access VPN > Network (Client) Access > Group Policies.选择Group Policy。 点击 Edit ,如图所示.

ổ Home 🦓 Configuration 📴 Monitoring 🏢	Save 🔇 Refresh 🔇 Back 🔘 Fo	rward 🦻 Help Type topic Go			cisco
OO Remote Access VPN	Configuration > Remote A	ccess VPN > Network (Client) A	ccess > Group Policies		
Pintroduction Introduction Introduction AntyConnect Connection Profiles SnyConnect Customization/Localization AnyConnect Client Profile AnyConnect Client Software	Manage VPN group policies.A VPN server. The group policy informati To enforce authorization attribute Add C Edit Delete	group is a collection of user-orie on is referenced by VPN connections from an LDAP server you must u Assign	nted authorization attribute/value pairs that ma n profiles and user accounts. se an <u>LDAP attribute map</u> .	y be stored internally on the device or externally on a RADIUS/LDA	Р
Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users	
a Group Policies	AnyConnect	Internal	ssl-client	AnyConnect	
IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;D	ef
IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
Secure Mobility Solution					
 Advanced AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attribute Names Pace Act Manager Clentless SSL VPN Access AAAS server Groups DAA Attribute Map Clentlese Management Secure Desktop Manager Clentlicate Management Load Blaincing Pol Posver DNS Advanced 					
Bevice Setup					
<u>Derice Setup</u>					
💱 Firewall					
Remote Access VPN					
Site-to-Site VPN	Find:	Match Case			
Device Management					
÷			Reset Apply		

步骤 7.如图所示,导航至 Advanced > Split Tunneling.将策略配置为 Tunnel All Networks.

• •		Edit Intern	nal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling de fields.	cisions on the	e basis of a network list that can be specified below by providing the proper parameters to 'Policy	' and 'Network Li:
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	The VPN client makes split tunneling de fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlu Set up Split Exclusion for Web Secur Intercept DHCP Configuration Message	cisions on the linherit Inherit Inher	e basis of a network list that can be specified below by providing the proper parameters to 'Policy Yes No Tunnel All Networks Security proxies. oft Clients	' and 'Network Li:
Find:	S Next	Previous		
		H	Help Cancel OK	

步骤 8导航至 Advanced > Anyconnect Client > Custom Attributes.点击 Add,如图所示.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel
General Servers V Advanced Split Tunneling Browser Proxy V AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes V IPsec(IKEv1) Client	Configuration of custom policy attributes. Image: Configuration of custom policy attributes. Type Name of Value
Find:	Next Previous
	nep Carter OK

步骤 9 选择属性类型作为 ManagementTunnelAllAllowed 并选择值作为 true.点击 OK,如图所示.

	Name of Value	
• •	Create Custom Attribute	
Attribute type:	ManagementTunnelAllAllowed	
Omit the value		
Select Value:	true 🗘 Manage	

步骤 10点击 Apply 将配置推送到ASA,如图所示。

🚮 Home 🍕 Configuration 📴 Monitoring 🚛	Save 🔇 Refresh 🔇 Back 🔘 Forw	ard 💡 Help Type topic Go		alah cisco
000 Remote Access VPN	O O Configuration > Remote Acc	ess VPN > Network (Client) Acces	ss > Group Policies	
Introduction I	Manage VPN group policies A VPN g policy information is referenced by To enforce authorization attributes f Add C C Edit 1 Delete As	oup is a collection of user-oriente /PN connection profiles and user ac from an LDAP server you must use a sign	d authorization attribute/value pairs that may be stored in counts. an LDAP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The group
AnyConnect Client Software	Name	Type	Tunneling Protocol	Connection Profiles/Users
Group Policies	AmConnect	Internal	ssigned	Assigned To
Psec(IKEv1) Connection Profiles	DftGroPolicy (System Default)	Internal	ikev1:ikev2:l2tp=insec	DefaultRAGroup: DefaultL2LGroup: DefaultADMINGroup: DefaultWE
IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2:ssl-client	AnyConnect_MGMT_Tunnel
Secure Mobility Solution		· · · · · · · · · · · · · · · · · · ·		
Address Assignment				
Advanced				
Clientless SSL VPN Access				
Add Separ Crown				
LDAP Attribute Map				
Cocal Users				
A Secure Desktop Manager				
Certificate Management				
Language Localization				
Sector Balancing				
DHCP Server				
a DNS				
B) Advanced				
Device Setup				
Firewall				
Remote Access VPN				
Site-to-Site VPN	Find:	Match Case		
S Device Management				
			Reset Apply	

CLI配置 ManagementTunnelAllAllowed 添加自定义属性:

webvpn

enable outside

anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
hsts
enable
max-age 31536000

```
include-sub-domains
 no preload
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
anyconnect enable
tunnel-group-list enable
cache
 disable
 error-recovery disable
1
anyconnect-custom-data ManagementTunnelAllAllowed true true
1
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
client-bypass-protocol enable
address-pools value VPN_Pool
anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

```
验证
```

使用ASA CLI验证管理VPN隧道连接 show vpn-sessiondb detail anyconnect 命令。

ASA# show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
Username
           : vpnuser
                                    Index
                                                : 10
                                    Public IP
Assigned IP : 192.168.10.1
                                                 : 10.65.84.175
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
           : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-
256
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
           : 17238
                                              : 1988
Bytes Tx
                                    Bytes Rx
         : 12
Pkts Tx
                                    Pkts Rx
                                                 : 13
                                    Pkts Rx Drop : 0
Pkts Tx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
           : 0h:11m:36s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                                : none
                                    VLAN
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
--- Output Omitted ---
DTLS-Tunnel:
 Tunnel ID
              : 10.3
 Assigned IP : 192.168.10.1
                                    Public IP : 10.65.84.175
 Encryption : AES-GCM-256
                                      Hashing
                                                 : SHA384
 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
                                      UDP Src Port : 57053
 Encapsulation: DTLSv1.2
```

UDP Dst Port :	443	Auth Mode	:	Certificate
Idle Time Out:	30 Minutes	Idle TO Left	:	18 Minutes
Client OS :	Windows			
Client Type :	DTLS VPN Client			
Client Ver :	Cisco AnyConnect VPN A	Agent for Windo	ws	4.8.03036
Bytes Tx :	17238	Bytes Rx		: 1988
Pkts Tx :	12	Pkts Rx		: 13
Pkts Tx Drop :	0	Pkts Rx D	ro	p:0

验证ASDM上的管理VPN隧道连接。

导航到Monitoring > VPN > VPN Statistics > Sessions。按AnyConnect**客户端**过滤以查看客户端会 话。

🚮 Home 🦓 Configuration [🦉 Mo	onitoring 🔜 Save 🄇	🔖 Refresh 🔇 😋 Ba	ck 🔘 Forward 💡	Help Type topic	Go					cisco
Device List Bookmarks	000 Monitoring	> VPN > VPN Stati	stics > Sessions							
OOO Device List										
Add 🚺 Delete 🔊 Connect	Туре	Active		Cumulative		Peak Concurre	nt	Inactive		
Find: Go	AnyConnect Client		1		1	19		1		0
10.106.39.196	550,100,010									Ű
10.106.64.230										
■ 10.106.51.99:444										
OOO VPN										
VPN Statistics	Filter By AnyCor	nnect Client	ᅌ 🛛 All Se	essions ᅌ		Fil	ter			
VPN Cluster Loads	Username	Group Policy	Assigned IP Address	Protocol		Login Time	Bytes Tx	Inactivity	Audit !	Details
Crypto Statistics	vpnuser	AnyConnect_MGMT	192.168.10.1	AnyConnect-Paren	it	10:52:25 UTC	34688	0h:00m:00s	c0a80	
Compression Statistics		AnyConnect_MGMT	10.65.84.175	AnyConnect-Paren	it: (1)none	0h:01m:31s	33954			Logout
Global IKE/IPsec Statistics									_	Ping
Protocol Statistics										
VLAN Mapping Sessions										
Clientless SSL VPN										
Shared SSL VPN										
WSA Sessions										
Interfaces										
C ²¹ VPN										
	To sort VPN session	s, right-click on th	e above table and se	elect Table Sort Ord	er from pop	oup menu.				
Kouting	Locout Bu:			Locout Sessions						
Sea Properties	Logout by Al	Jessio 🗹		Logour sessions						

验证客户端计算机上的管理VPN隧道连接:

Sisco AnyConnect Secure Mobil	ty Client		-	×				
cisco AnyCon	nect Secure Mobi	lity Clie	nt	()				
Virtual Private Network (VPI	Virtual Private Network (VPN)		Diagnostics					
Preferences Statistics Route Detai	ls Firewall Message History							
Connection Information State:	Disconnected		•	^				~
Tunnel Mode (IPv4):	Not Available		Cisco AnyCon	nnect Sec	cure Mobility Client			^
Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available 00:00:00 None Connected (asa.example.com)			VPN: Ready to	connect.	~	Connect	
Address Information								
Client (IPv4):	Not Available						Carad	
Client (IPv6):	Not Available		¢ ()				1	diadia cisco
Bytes	not Avdilable		•	*				
		Reset	Export Stats					

故障排除

新的UI统计行(管理连接状态)可用于排除管理隧道连接问题的故障。以下是常见的错误状态:

已断开连接(禁用):

- •此功能已禁用。
- •确保管理VPN配置文件已通过用户隧道连接(要求您将管理VPN配置文件添加到用户隧道组策略)部署至客户端,或通过手动上传配置文件实现带外部署。
- •确保管理VPN配置文件配置有包含隧道组的单个主机条目。

已断开连接(受信任网络):

•TND检测到受信任网络,因此未建立管理隧道。

已断开连接(用户隧道处于活动状态):

•用户VPN隧道当前处于活动状态。

已断开连接(进程启动失败):

•尝试管理隧道连接时遇到进程启动失败。

已断开连接(连接失败):

- 建立管理隧道时遇到连接故障。
- •确保证书身份验证在隧道组中配置,组策略中不存在标语,并且服务器证书必须受信任。

已断开连接(无效的VPN配置):

- •从VPN服务器收到无效的拆分隧道配置。
- 检查管理隧道组策略中的拆分隧道配置。

已断开连接(软件更新挂起):

• AnyConnect软件更新当前处于挂起状态。

已断开连接:

•管理隧道即将建立或由于其他原因无法建立。

<u>收集DART以</u>进一步排除故障。

相关信息

- <u>管理VPN隧道的配置</u>
- <u>管理VPN隧道故障排除</u>
- <u>技术支持和文档 Cisco Systems</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)。