通过ASA部署AnyConnect网络安全

目录

简介 <u>先决条件</u> <u>要求</u> 使用的组件 <u>背景信息</u> 配置 通过ASA部署AnyConnect Web安全 验证 升级/降级AnyConnect版本 故障排除

简介

本文档介绍为在思科自适应安全设备(ASA)上终止的基于客户端的VPN部署AnyConnect网络安全模块。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

背景信息

• 在ASA上上传Anyconnect(建议v4.1+)映像

File View Tools Wizards Window Help		Type topic to search	Go
Home 🍪 Configuration 🔯 Monitoring 🗐 Sav	e 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help		CISCO
Remote Access VPN 🗗 🗜	Configuration > Remote Access VPN > Network (Client) Access > AnyConnect C	<u>Client Software</u>	
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localization AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software AnyConnect Client Software Group Policies	AnyConnect Client Images Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most common Add C Replace Delete + C	ch string 'AnyConnect VPN Client'. The regu only encountered operation system to the	ular expression is used
IPsec(IKEv1) Connection Profiles Secure Mobility Solution Address Assignment	disk0;/anyconnect-win-4.1.08005-k9.pkg		

•在ASA上启用VPN配置文件,如图所示

File View Tools Wizards Window He	lp					Type topic to search	Go	alah
Home 🦓 Configuration 🔯 Monitoring	🔚 Save	e 💽 Refresh 🕻	Back 💽 Forward	? Help				cisco
Remote Access VPN	8 P	Configuration :	Remote Access VPN :	> Network (Client) A	ccess > <u>AnyConnec</u>	t Connection Profiles		
Introduction Network (Client) Access Network (Client) Access AnyConnect Connection Profiles AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software Group Policies Group Policies Secure Mobility Solution Secure Mobility Solution	×	The security ag end-user admin Security (DTLS) Access Interface Imable Cisc SSL access mus Interface	pliance automatically depl instrative rights. The Cisco tunneling options. s to AnyConnect VPN Client st be enabled if you allow / SSL Access Allow Access	oys the Cisco AnyConn AnyConnect VPN Client access on the interface AnyConnect client to be Enable DTLS	ect VPN Client to remot supports IPsec (IKEv2 s selected in the table l launched from a brows IPsec (IKEv2) Acco Allow Access	e users upon connection. The initia e) tunnel as well as SSL tunnel with 1 below ser (Web Launch) . ess Enable Client Services	I client deploymer Datagram Transp	rt requires A
Clentless SSL VPN Access Connection Profiles Fortal VDI Access Group Policies VDI Access Group Policies Fortal Forcoding Proxy Bypass Fortal Java Code Signer Content Cache Content Cache Content Cache Aplication Helper	~	Utside U	erface access lists for inbo m group policy and user po g	und VPN sessions blicy always apply to the e on the login page.	e traffic.	eters. You can configure the mapping	ng from certificat	ttings ≡ e to
Device Setup		💠 Add 📝	Edit Delete Find:	(🗇 🔘 🗌 Match Cas	e		
Firewall		Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Pol	icv
Remote Access VPN		DefaultRAGrou	up Qu	V	,	AAA(LOCAL)	DfltGrpPol	cy
Site-to-Site VPN		DefaultWEBVP	🗸	✓		AAA(LOCAL)	DfitGrpPol	SY V
Device Management		<						>
	»				Apply Res	set		

配置

通过ASA部署AnyConnect Web安全

配置中涉及的步骤如下:

- 配置AnyConnect网络安全客户端配置文件
- •编辑Anyconnect VPN组策略
- •为Web安全设置拆分排除并选择下载Web安全客户端模块
- 编辑Anyconnect VPN组策略并选择网络安全客户端配置文件

步骤1.配置AnyConnect Websecurity客户端配置文件

导航至配置>删除接入VPN>网络(客户端)接入>Anyconnect客户端配置文件,单击

添加并选择AnyConnect网络安全客户端配置文件。

注意:配置文件名称在客户端上是硬编码的,因此,无论配置了什么名称,ASA始终将 Websecurity_serviceprofile.wso推送到客户端。

注意:这是没有身份验证许可证密钥的默认配置文件。

File View Tools Wizards Window Help							Туре
Home 🆓 Configuration 🔯 Monitoring 🗐 S	ave 💽 Refresh	G Back O F	Forward 🦹 Help				
Remote Access VPN 🗗 🖓	Configuratio	n > Remote Acc	ess VPN > Networ	k (Client) Access > AnyCo	nnect Client Pro	<u>file</u>	
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localization AnyConnect Client Profile AnyConnect Client Software Dynamic Access Policies Group Policies IPsec(IKEv1) Connection Profiles Secure Mobility Solution	This panel is 'Add' button The profile U & Add 2 Profile Nam	used to manage Ar to add a new profil Isage field is introdu Sedit X Change	nyConnect Client Pro e. Pressing the Impo uced with the Secure Group Policy	files and perform group assign rt or Export button is for uplo Mobility Solution. This field co elete The Import Export	nment for AnyConn ad and download o ntains different pro Dalidate	ect version 2.5 or later. You of f client profiles between loca ofile usage in AnyConnect ve Group Policy	an select a profile to imachine and device. rsion 3.0 and later.
Address Assignment						,	
Advanced Glentless SSL VPN Access AAA/Local Users		6	A	dd AnyConnect Client	Profile	×	
Host Scan Image		Profile Name	demo				
		Profile Usage	Web Security Serv	ice Profile	~		
Language Localization Load Balancing DHCP Server DHCP Server		Enter a device automatically cr	file path for an xml fi eated if it does not (le, ie. disk0:/ac_profile. The fi exist.	le will be		
Advanced		Profile Location	disk0:/demo.wsp			Browse Flash	
-						Upload	
A Device Setup		Group Policy	<unassigned></unassigned>		~		
Firewall			Enable 'Always	On VPN' for selected group			
Remote Access VPN							
Site-to-Site VPN				OK Cancel	Help		
Davice Management							

步骤2.编辑新创建的配置文件以添加身份验证许可证密钥并自定义配置。

File View Tools Wizards V	6		AnyConnect Client Pro	file Editor - de	mo		x
Home 🆓 Configuration	Profile: demo						About
Remote Access VPN	Web Security	Scanning Provv					
Remote Access VPN Introduction Network (Client) Access AnyConnect Connection F AnyConnect Customization AnyConnect Client Profile The Connect Client Software Organization ParyConnect Client Software Image: Access Policies Image: Advanced Imag	Web Security Scanning Proxy Exceptions Authentication Advanced	Scanning Proxy Scanning Proxy list is current Scanning Proxy UK Germany France Demark Switzerland South Africa C C Default Scanning Proxy India Traffic Listen Port	tly up-to-date. Host Name 108, 171, 128, 156 108, 171, 129, 156 80, 254, 150, 66 196, 26, 220, 66 197, 196, 196, 196, 196, 196, 196, 196, 196	Plain Port 8080 8080 8080 8080 8080 8080 8080 1000	SSL Port 443 443 443 443 443 443 443 443	Display/Hide Display Display Display Display Display Display > > > > > > > > > > > > > > > > > > >	
Device configuration loaded successfu			OK Cancel	Help			

File View Tools Wizards W	6	AnyConnec	t Client Profile Editor - demo	×
Home 🦓 Configuration	Profile: demo			About
Home Configuration AnyConnect Client Profile Dynamic Access Policies Jesec(IKEv1) Connection F Secure Mobility Solution Secure Mobility Solution Advanced Clientess SSL VPN Access AAA/Local Users AAA/Local Users	Profile: demo	Authentication Proxy Authentication License Key Service Password	F90A686F696FF779CB758B69F84A5688 websecurity Use Group Include List Add Delete	About
A Scare Desktop Manager Certificate Management Language Localization Load Balancing DHCP Server DNS Device Setup Frewall Remote Access VPN Site-to-Site VPN Device Management		Custom matching and reporting for mach Computer Name Custom Groups (optional)	ines not joined to domains	ice restart ✓
Device configuration loaded successfu		ОК	Cancel Help	
File View Tools Wizards	Window Help	fresh 🔇 Back 💽 Forward 🤗 Help	Туре	topic to search Go CISCO
Remote Access VPN Introduction AnyConnect Connection AnyConnect Clent Profile AnyConnect Clent Soft AnyConnect Clent Soft Fight AnyConnect Soft Fight AnyC	Profiles on/Localization are h Profiles	anal is used to manage AnyConnect Client Pro e group or to delete. You can select the 'Add' iss between local machine and device. rofile Usage field is introduced with the Secure and C Edit Change Group Policy C Device le Name Profile Usage Web Security	C(Client) Access > AnyConnect Client Profile files and perform group assignment for AnyConnect button to add a new profile. Pressing the Import or fi Mobility Solution. This field contains different profile slete I Import Export I Validate e Group Policy y Service Profile DftGrpPolicy	version 2.5 or later. You can select a profile to edit, Export button is for upload and download of client usage in AnyConnect version 3.0 and later. Profile Location disk0:/demo.wsp

步骤3.为Web安全设置拆分排除并选择下载Web安全客户端模块

编辑Anyconnect VPN组策略,如图所示。

File View Tools Wizards Window Help							
Home 🆧 Configuration 🔯 Monitoring	CISC Configuration 🖗 Monitoring 🔚 Save 🕀 Refresh 🔇 Back 🔇 Forward 🦞 Help						
Remote Access VPN 🗇 🗜	Configuration > Remote Access V	<u> PN > Network (Client) Access > Grou</u>	p Policies				
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localization AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software	11) Access Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. 11) Access group policy information is referenced by VPN connection profiles and user accounts. 12) Access To enforce authorization attributes from an LDAP server you must use an LDAP attribute map. etC Client Fonfile						
Group Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To			
Secure Mobility Solution	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec;ssl-dient;ssl-dientless	DefaultRAGroup;DefaultL2LGroup;DefaultV	VEBVPNGroup		
⊕ Address Assignment ⊕ 100 Advanced							

如图所示,为Web安全设置拆分排除。

E		Edit Internal Group Policy: DfltGrpPolicy
General	The VPN dient makes split tunneling decision	ns on the basis of a network list that can be specified below by providing the proper parameters to 'Policy
-Advanced	DNS Names:	
Browser Proxy Browser Proxy	Send All DNS Lookups Through Tunnel: (○ Yes
	Policy:	Exclude Network List Below
	IPv6 Policy:	Exclude Network List Below
	Network List:	None
	Pressing this button to set up split exlusion	for Web Sequrity proxies.
	Set up Split Exclusion for Web Security	Web Security Proxies Exclusion
	Intercept DHCP Configuration Message fro	om Microsoft Enter a new or select an existing access list used for Web Security split exclusion. ASDM will set up the access list for use in the network list. Access list name: CWS-Tower Create Access List Update Access List Cancel
6	1	Edit Internal Group Policy: DfltGrpPolicy
General	The VPN dient makes split tunneling	decisions on the basis of a network list that can be specified below by providing the proper par
	DNS Names:	
Browser Proxy	Send All DNS Lookups Through Tunn	nel: 🔿 Yes 💿 No
	Policy:	Exclude Network List Below
	IPv6 Policy:	Exclude Network List Below
	Network List:	CWS-Tower
	Pressing this button to set up split e	extusion for Web Security proxies.

选择下载网络安全客户端模块,如图所示。

步骤4.下载Web安全客户端配置文件

编辑**Anyconnect VPN组策略>要下载的客户端配置文件>添加,**现在选择创建的配置文件(如步骤 1中所示)

Intercept DHCP Configuration Message from Microsoft Clients

General	Keep Installer on Client System:	● Yes ○ No	
-Advanced	Datagram Transport Layer Security (DTLS):	Enable O Disa	ble
Split Tunneling Browser Proxy	DTLS Compression:	Enable Disa	ble
AnyConnect Client	SSL Compression:	○ Deflate ○ LZS	Disable
	Ignore Don't Fragment(DF) Bit:	 Enable Disa 	ble
Dead Peer Detection	Client Bypass Protocol:	○ Enable	ble
Customization	FQDN of This Device:		
⊡·IPsec(IKEv1) Client	MTU:	1406	
	Keepalive Messages:	Disable Interval	Select AnyConnect Client Profiles
	Optional Client Modules to Download:	websecurity	This panel is used to select existing AnyConnect profile for a group policy. To create or edit a profile, go to Remote
	Always-On VPN:	🔿 Disable 💿 Use d	Access VPN>Network (Client) Access>AnyConnect Client Profile.
	Client Profiles to Download:		Select a profile name and the usage will be determined automatically. The 'View Profile' button will open the profile viewer (no edition) if the AnyConnect 2.5 client or later is installed and if the profile usage is determined.
		Add Delete	Otherwise, it will show the profile content as XML text.
		Profile Name	Profile Name: demo
			Profile Usage: Web Security Service Profile
<			
Find:	Next Previous	5	
			OK Cancel Help

点击OK并应用更改。

验证

当您连接到Anyconnect VPN时,ASA将通过VPN推送Anyconnect网络安全模块,如图所示。

S Cisco AnyConnect 10.106.36.30	⊙ Cisco AnyConnect Secure Mobility Client - □ ×
Username: user1 Password: *******	VPN: Contacting 10.106.36.30. 10.106.36.30 Connect
OK Cancel	



如果已登录,则建议注销,然后重新登录以启用功能。

升级/降级AnyConnect版本

Q

1

升级版本后,部署功能将保持不变。但是,无法降级。因此,使用当前4.1.x示例,可将其升级到

CISCO

4.2版

涉及的步骤如下:

步骤1.将最新的Anyconnect软件包4.2上传到闪存,并用最新文件替换4.1。

在"AnyConnect客户端软件">"替换"下,然后选择最近的映像文件。

File View Tools Wizards Window Help		Type topic
Home 🍇 Configuration 🔯 Monitoring 🗐 Sav	Refresh Sack Sorward Provided Help	
Remote Access VPN 🗗 🖓	Configuration > Remote Access VPN > Network (Client) Access > AnyConnec	t Client Software
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localization AnyConnect Client Profile AnyConnect Client Software Dynamic Access Policies	AnyConnect Client Images Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the set to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most com Add C Replace Delete Delete Delete	arch string 'AnyConne monly encountered of
Group Policies	Image	Regular expression t
IPsec(IKEv1) Connection Profiles	disk0:/anyconnect-win-4.1.08005-k9.pkg	
	Replace AnyConnect Client Image	x
Clientless SSL VPN Access AAA/Local Users	AnyConnect Image: disk0:/anyconnect-win-4.2.01035-k9.pkg Br	owse Flash
Host Scan Image		Upload
E Certificate Management	Regular expression to match user-agent	×
Language Localization Load Balancing DHCP Server DNS	OK Cancel Help	

第二步: 当您重新连接到Anyconnect VPN时,ASA将通过VPN推送最新的Anyconnect模块,而不 会更改网络安全配置文件。

S Cisco A	AnyConnect Secure Mobility Client 🗕 🗆 🛛 🛛
	VPN: Exiting. Upgrade in progress. 10.106.36.30 ∨ Connect
	Web Security: Enabled (India)
\$ (i)	Altabr

AnyConnect Secure Mobility Client Downloader



The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.01035. Please wait...

注意:不支持降级。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

使用DART收集故障排除信息:

DART是AnyConnect诊断和报告工具,您可以使用它收集数据,以排除AnyConnect安装和连接故障。DART支持Windows 7、Windows Vista、Windows XP、Mac版本10.5和10.6以及Linux Redhat。DART向导在运行AnyConnect的计算机上运行。它为思科技术支持中心(TAC)分析整理日 志、状态和诊断信息,不需要管理员权限。

虽然DART不依赖于AnyConnect软件的任何组件来运行,但您可以从AnyConnect启动它,但它将 收集AnyConnect日志文件(如果可用)。目前,DART可作为独立安装使用,或者管理员可以将此 应用作为AnyConnect动态下载基础设施的一部分推送到客户端PC。安装后,最终用户可以从 Cisco文件夹通过"开始"按钮启**动向**导。