通過ASA進行AnyConnect網路安全部署

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>設定</u> <u>通過ASA進行Anyconnect WebSecurity部署</u> <u>驗證</u> <u>升級/降級Anyconnect版本</u> 疑難排解

簡介

本文檔介紹如何為基於客戶端的VPN部署AnyConnect網路安全模組,該模組在思科自適應安全裝置 (ASA)上終止。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

•上傳ASA上的Anyconnect(推薦v4.1+)映像

File View Tools Wizards Window Help		Type topic to search	Go	ababa
Home 🍓 Configuration 🔯 Monitoring 🗐 Sav	e 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help			cisco
Remote Access VPN 🗗 🖗	Configuration > Remote Access VPN > Network (Client) Access > AnyConnect C	<u>lient Software</u>		
Introduction Network (Client) Access Network (Client) Access AnyConnect Connection Profiles AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software Group Policies Group Policies IPsec(IKEv1) Connection Profiles	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 commo Add C Replace Delete Delete Replace	ch string 'AnyConnect VPN Client'. The reg only encountered operation system to the tegular expression to match user-agent	ular ex top of	pression is used the list.
General Secure Mobility Solution General Address Assignment				

•在ASA上啟用VPN配置檔案,如下圖所示

File View Tools Wizards Window He	elp					Type topic to search	Go	ababa
Home 🍓 Configuration 🔯 Monitoring	🔒 Sav	e 💽 Refresh	G Back O Forward	? Help				cisco
Remote Access VPN	a t	Configuration	n > Remote Access VPN	> Network (Client) A	ccess > AnyConnec	t Connection Profiles		
Introduction Network (Client) Access Network (Client) Access AnyConnect Connection Profiles AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software Opamic Access Policies Dynamic Access Policies Secure Mobility Solution Secure Mobility Solution	~	The security end-user adr Security (DTL Access Interfac Imable C SSL access m	appliance automatically dep ninistrative rights. The Cisco S) tunneling options. tes isco AnyConnect VPN Client ust be enabled if you allow.	oys the Cisco AnyConn AnyConnect VPN Client access on the interface AnyConnect client to be	ect VPN Client to remot supports IPsec (IKEv2 s selected in the table l launched from a brown IPsec (IKEv2) Acco	te users upon connection. The initia 2) tunnel as well as SSL tunnel with below ser (Web Launch) . ess	I dient deploymer Datagram Transp	trequires A ort Layer
H Address Assignment		- 444	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Co	a uncate
Advanced Advanced Connection Profiles Connection Profiles Ortal VDI Access Convp Policies Orup Policies Orup Policies Advanced Proxies Proxies Java Code Signer Content Cache Content Rewrite Application Helper	>	outside inside Bypass in Access lists f Login Page Set Allow use Shutdow Connection Pro Connection p	Interface access lists for inbo irom group policy and user p ting er to select connection profil n portal login page. files profile (tunnel group) specifi rofile (tere,	und VPN sessions olicy always apply to the e on the login page.	e traffic,	eters. You can configure the mappi	ng from certificat	ttings ≡ e to
Device Setup		🖶 Add 🖸	Edit Delete Find:	(🛇 🙆 🗌 Match Cas	se		
🕄 Firewall		Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Pol	icy
Remote Access VPN		DefaultRAG	oup	✓		AAA(LOCAL)	DfltGrpPoli	cy
Site-to-Site VPN		DefaultWEB	VP 🗹	✓		AAA(LOCAL)	DfltGrpPoli	cy 🗸 🗸
Device Management		<			III			>
	»				Apply Res	set		

設定

通過ASA進行Anyconnect WebSecurity部署

配置中涉及的步驟如下:

- 配置Anyconnect Websecurity客戶端配置檔案
- 編輯Anyconnect VPN組策略
- 為Web安全設定拆分排除,並選擇下載Web安全客戶端模組
- 編輯Anyconnect VPN組策略並選擇網路安全客戶端配置檔案

步驟1.配置Anyconnect Websecurity客戶端配置檔案

導航至Configuration >Remove Access VPN >Network(Client)Access >Anyconnect Client Profile,點選

新增並選擇AnyConnect網路安全客戶端配置檔案。

附註:配置檔名稱在客戶端採用硬編碼,因此,無論配置何種名稱,ASA始終將 Websecurity_serviceprofile.wso推送到客戶端。

附註:這是一個沒有身份驗證許可證金鑰的預設配置檔案。

File View Tools Wizards Window Help			Туре
Home 🍓 Configuration 🔯 Monitoring 🗐 Sav	e 💽 Refresh 🚺 Back 💽	Forward 💡 Help	
Remote Access VPN 🗗 🖓	Configuration > Remote A	ccess VPN > Network (Client) Access > AnyCo	nnect Client Profile
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localization AnyConnect Client Profile Dynamic Access Policies Group Policies Figure 2000 Profiles Secure Mobility Solution	This panel is used to manage 'Add' button to add a new pr The profile Usage field is intr de Add d Edit 1	AnyConnect Client Profiles and perform group assign ofile. Pressing the Import or Export button is for uplo oduced with the Secure Mobility Solution. This field co uge Group Policy The Delete The Import Export Profile Usage	iment for AnyConnect version 2.5 or later.You can select a profile to ad and download of client profiles between local machine and device. ntains different profile usage in AnyConnect version 3.0 and later.
Advanced Gentless SL VPN Access	E	Add AnyConnect Client	Profile
AnAloca Deels AnAloca Deels AnAloca Deels AnAloca Deels AnAloca Deels Secure Desktop Manager Secure Desktop Manager Decrificate Management Decrificate Management Load Balancing DHCP Server	Profile Name Profile Usage Enter a devi automaticali	demo Web Security Service Profile	v le will be
	Profile Locat	ion disk0:/demo.wsp	Browse Flash Upload
Device Setup	Group Policy	<unassigned> Enable 'Always On VPN' for selected group</unassigned>	~
Site-to-Site VPN		OK Cancel	Help

步驟2.編輯新建立的配置檔案以新增身份驗證許可證金鑰並自定義配置。

File View Tools Wizards W	6	AnyConnect Client Profile Editor - demo						
Home 🖓 Configuration 🔯	Profile: demo							About
Remote Access VPN	Web Security	Scanning Provv						
Home Configuration ArryConnect Current Access Introduction Network (Client) Access AnyConnect Customizatio AnyConnect Customizatio AnyConnect Customizatio AnyConnect Client Softwa AnyConnect Client Softwa AnyConnect Client Softwa Dynamic Access Policies JPsec(IKEv 1) Connection I Secure Mobility Solution Address Assignment Secure Mobility Solution Address Assignment Address Assignment DAdvanced Clientiess SSL VPN Access AAA(Aocal Users AAA(Aocal Users AAA(Aocal Users AAA(Aocal Users DHot Scan Image Advanced DHCP Server DNS Advanced Secure Desktop Manager Secure Desktop Manager Advanced Secure Desktop Manager Secure Desktop Ma	Profile: demo	Scanning Proxy Scanning Proxy Scanning Proxy UK Germany France Denmark Switzerland South Africa C Default Scanning Proxy India Traffic Listen Port 80 8080 3128 443	ttly up-to-date. Host Name 108.171.128.156 108.171.129.156 80.254.150.66 80.254.155.66 196.62.220.66 ∎ M Add Delete	Plain Port 8080 8080 8080 8080 8080 8080 8080	SSL Port 443 443 443 443 443 443 443	Display/Hide Display Display Display Display Display >> i >>	Clisplay Hide Display All V	About
Device Management		<		Ш				>
Device configuration loaded successfu			OK Cancel	Help				

File View Tools Wizards W		AnyConnect Client Profile Editor - demo				
Home 🍪 Configuration	Profile: demo		About			
Home Configuration AnyConnect Consection P AnyConnect Connection P AnyConnect Customization AnyConnect Customization AnyConnect Client Profile AnyConnect Profile AnyConect P	Profile: demo Web Security Scanning Proxy Exceptions Authentication Advanced	Authentication Proxy Authentication License Key F90A686F696FF779CB758869F84A5688 ** Service Password websecurity **	About			
Firewall Remote Access VPN Site-to-Site VPN Device Management		** change requires WebSecurity service restart	~			
Device configuration loaded successfu		OK Cancel Help				
File View Tools Wizards	Window Help	Type topic to search Go	cisco			
Remote Access VPN	급 무 <u>Confic</u>	juration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile				
Introduction Intro	n Profiles ion/Localization profiles char profiles ware n Profiles =	panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a p ge group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and downle les between local machine and device. profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and Add 2 Edit 2 Change Group Policy 1 Delete 2 Import 4 Secure 1 Secure 1 Secure 1 Delete 2 Import 4 Secure 1 Delete 2 Import 4 Secure 1 Delete 2 Import 4 Delete 2 Import 4 Delete 2 Delete 2 Delete 2 Delete 2 Delete 3 Delete	rofile to edit, ad of client I later.			
Secure Mobility Solution	= Dro	fle Name Profile Lisage Group Policy Profile Location				

Address Assignment 步驟3.為Web安全設定拆分排除,並選擇下載Web安全客戶端模組

Profile Name

編輯Anyconnect VPN組策略,如下圖所示。

File View Tools Wizards Window Help Type topic to search Go								
Remote Access VPN 🗗 🖗	Configuration > Remote Access	VPN > Network (Client) Access > Gro	<u>up Policies</u>					
Introduction Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localization AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software	Manage VPN group policies. A VPN g group policy information is reference To enforce authorization attributes Add V 2 Edit 1 Delete	roup is a collection of user-oriented author ed by VPN connection profiles and user acc from an LDAP server you must use an LDA Assign	zation attribute/value pairs that may be stored inter ounts. P <u>attribute map</u> ,	nally on the device or externally on a RADIUS/L	DAP server. The			
Group Policies IPsec(IKEv1) Connection Profiles	Name	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To				
Secure Mobility Solution	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec;ssl-client;ssl-clientless	DefaultRAGroup;DefaultL2LGroup;Default	WEBVPNGroup			
Address Assignment								

Profile Usage

Veb Security

Group Policy

Profile Location

ck0. Idam

如圖所示,為Web安全設定分割排除。

E				Edit Internal Group Policy: DfltGrpPolicy
Ge Se	eneral ervers dvanced — <mark>Split Tunneling</mark> — Browser Proxy — AnyConnect Client — IPsec(IKEv1) Client	The VPN dient makes split tunneling decision DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlusion Set up Split Exclusion for Web Security. Intercept DHCP Configuration Message fr	Yes Yes Yes None None n for Web Secu	is of a network list that can be specified below by providing the proper parameters to 'Policy No No No No Vork List Below Vor
E				Edit Internal Group Policy: DfltGrpPolicy
	General Servers Advanced Split Tunneling Browser Proxy G-AnyConnect Client Desc(IKEv1) Client	The VPN dient makes split tunneling DNS Names: Send All DNS Lookups Through Tun Policy: IPv6 Policy: Network List:	g decisions or nnel: O Ye Exclu Exclu CWS	n the basis of a network list that can be specified below by providing the proper par es No ude Network List Below ude Network List Below

Pressing this button to set up split exlusion for Web Security proxies.
Set up Split Exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

選擇「下載Web安全客戶端模組」,如下圖所示。

步驟4.下載網路安全客戶端配置檔案

編輯**Anyconnect VPN組策略>要下載的客戶端配置檔案>新增**,現在選擇建立的配置檔案(如步驟 1所示)

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

按一下確定並應用更改。

驗證

當您連線到Anyconnect VPN時,ASA將通過VPN推送Anyconnect網路安全模組,如下圖所示。

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



如果您已經登入,則建議先註銷,然後重新登入以啟用該功能。

升級/降級Anyconnect版本

Q

1

如果版本升級,部署功能保持不變。但是,降級是不可能的。因此,使用當前的4.1.x示例,可以將

CISCO

其升級到4.2版

具體步驟如下:

步驟1.將最新Anyconnect軟體包4.2上傳到快閃記憶體並用最新檔案替換4.1。

在Anyconnect Client Software > Replace下,然後選擇最近的映像檔案。

File View Tools Wizards Window Help		Type topic
Home 🍇 Configuration 🔯 Monitoring 🗐 Sav	Refresh Sack SForward Prover Help	
Remote Access VPN 🗗 🖗	Configuration > Remote Access VPN > Network (Client) Access > AnyConnec	ct Client Software
Introduction Introduction 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 con Add Replace Delete A	earch string 'AnyConne nmonly encountered or
Group Policies	Image	Regular expression t
IPsec(IKEv1) Connection Profiles	disk0:/anyconnect-win-4.1.08005-k9.pkg	
	Replace AnyConnect Client Image	x
AAA/Local Users	AnyConnect Image: disk0:/anyconnect-win-4.2.01035-k9.pkg	owse Flash
Host Scan Image		Upload
Certificate Management	Regular expression to match user-agent	*
Load Balancing DHCP Server DNS	OK Cancel Help	

步驟2. 當您重新連線到Anyconnect VPN時,ASA將通過VPN推送最新的Anyconnect模組,而不更 改網路安全配置檔案。

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

AnyConnect Secure Mobility Client Downloader



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

附註:不支援降級。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

使用DART收集故障排除資訊:

DART是AnyConnect診斷和報告工具,可用於收集有助於排除AnyConnect安裝和連線問題的資料 。DART支援Windows 7、Windows Vista、Windows XP、Mac版本10.5和10.6以及Linux Redhat。 DART嚮導在運行AnyConnect的電腦上運行。它彙集了思科技術支援中心(TAC)分析的日誌、狀態 和診斷資訊,不需要管理員許可權。

雖然DART不依賴AnyConnect軟體的任何元件運行,但您可以從AnyConnect啟動它,它會收集 AnyConnect日誌檔案(如果該檔案可用)。目前,DART可以作為獨立安裝提供,或者管理員可以 將此應用程式作為AnyConnect動態下載基礎架構的一部分推送到客戶端PC。安裝後,終端使用者 可以通過**Start**按鈕從Cisco資料夾啟動嚮導。