在FTD上設定SSL AnyConnect管理VPN

目錄

簡介 必要條件 需求 採用元件 背景資訊 限制 設定 組態 步驟1.建立AnyConnect管理VPN配置檔案 步驟2.建立AnyConnect VPN配置檔案 步驟3.將AnyConnect管理VPN配置檔案和AnyConnect VPN配置檔案上傳到FMC 步驟4.建立組策略 步驟5.建立新的AnyConnect配置 步驟6.建立URL對象 步驟7.定義URL別名 驗證 疑難排解

簡介

本檔案介紹如何在思科Firepower管理中心(FMC)管理的Cisco Firepower威脅防禦(FTD)上配置 Cisco AnyConnect管理隧道。 在下面的示例中,安全套接字層(SSL)用於在FTD和Windows 10客戶 端之間建立虛擬專用網路(VPN)。

作者:Daniel Perez Vertti Vazquez,思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco AnyConnect Profile Editor
- 通過FMC配置SSL AnyConnect。
- 客戶端證書身份驗證

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• Cisco FTD版本6.7.0(內部版本65)

- Cisco FMC 6.7.0版(內部版本65)
- Cisco AnyConnect 4.9.01095安裝在Windows 10電腦上

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

自6.7版起,思科FTD支援配置AnyConnect管理隧道。此修復了先前開啟的增強功能請求 <u>CSCvs78215</u>。

AnyConnect管理功能允許在終端完成啟動後立即建立VPN隧道。使用者無需手動啟動 AnyConnect應用,只要他們的系統通電,AnyConnect VPN代理服務就會檢測管理VPN功能,並使 用AnyConnect管理VPN配置檔案的伺服器清單中定義的Host Entry啟動AnyConnect會話。

限制

- 僅支援客戶端證書身份驗證。
- Windows客戶端僅支援電腦證書儲存。
- Cisco Firepower裝置管理器(FDM)<u>CSCvx90058</u>上不支援。
- Linux客戶端不支援。

設定

組態

步驟1.建立AnyConnect管理VPN配置檔案

開啟AnyConnect配置檔案編輯器以建立AnyConnect管理VPN配置檔案。管理配置檔案包含終端啟 動後用於建立VPN隧道的所有設定。

在此示例中,定義了一個指向完全限定域名(FQDN)dperezve.jyoungta-labdomain.cisco.com的伺服 器清單條目,並選定SSL作為主要協定。要新增伺服器清單,請導航到**伺服器清單**並選擇**新增**按鈕 ,填寫所需欄位並儲存更改。

- an	AnyConnect	Profile	Editor -	VPN
------	------------	---------	----------	-----

Server L	Load Balancing Servers	SCEP Mobile Cer	tificate Pinning			
	J.		5			
Prima	ary Server			Connection Infor	mation	
Disp	play Name (required)	AnyConnect_Manag	gement_Tunnel	Primary Protoc	ol SSL \vee	
FQ	DN or IP Address	User Gro	up	ASA gatew	ау	
dpe	erezve.jyoungta-labdom	nain.cisc / AnyConn	ect_Management_Tunnel	Auth Metho	d During IKE Negotiatior	EAP-A
Gro	oup URL			IKE Identity	(IOS gateway only)	
dpe	erezve.jyoungta-labdom	ain.cisco.com/AnyCo	onnect_Management_Tunnel			
		Backup Servers				
		Host Address			Add	
		Host Address			Add	
					Move Up	
					Move Down	
					Delete	
					201010	
			ov			
			OK Cancel			

除了伺服器清單,管理VPN配置檔案還必須包含一些必需的首選項:

- AutomaticCertSelection必須設定為true。
- AutoReconnect必須設定為true。
- •必須為ReconnectAfterResume配置AutoReconnectBehavior。
- AutoUpdate必須設定為false。
- BlockUntrustedServers必須設定為true。
- •必須為MachineStore配置CertificateStore。
- CertificateStoreOverride必須設定為true。
- EnableAutomaticServerSelection必須設定為false。
- EnableScripting必須設定為false。
- RetainVPNOnLogoff必須設定為true。

在AnyConnect Profile Editor中,導航至首選項(第1部分),並按如下方式調整設定:

 \times

File Help

			_					
VPN Preferences (Part 1) Preferences (Part 2) Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Profile\AnyConnect_Management_Tunnel.xml							
	Use Start Before Logon Show Pre-Connect Message Certificate Store Windows Machine macOS All ✓ Certificate Store Override Auto Connect On Start ✓ ✓ Minimize On Connect Local Lan Access ✓ Disable Captive Portal Detection ✓ Auto Reconnect Auto Reconnect Behavior ReconnectAfterResume ✓ Auto Update RSA Secure ID Integration Automatic	 ❑ User Controllable ⊇ User Controllable ⊇ User Controllable ⊇ User Controllable ⊇ User Controllable ❑ User Controllable 	~					
	Vindows Logon Enforcement SingleLocalLogon V Windows VPN Establishment							
	Ailowkemoteusers	Help	~					

然後導覽至**首選項(第2部分)**,並取消選中Disable Automatic Certificate Selection選項。

 \Box \times

File Help

VPN	Preferences (Part 2	2)		
	Profile:nnect -FT	D-Lab\.XML Profile\AnyConr	nect_Management_Tunnel.xml	
Certificate Pinning	Disable Automatic	Certificate Selection	User Controllable	
一层 Certificate Matching 易 Certificate Enrollment	Proxy Settings	Native	V User Controllable	
		Public Proxv Server Address:		
	Allow Local Proxy	Note: Enter public Proxv Server ad Connections	dress and Port here. Example:10.86.125.33:8080	
	Enable Optimal Ga	teway Selection	User Controllable	
	Suspension Time	Threshold (hours)	4	
	Performance Imp	rovement Threshold (%)	20	
	Automatic VPN Pol Trusted Network	icy Policy	Disconnect ~	
	Untrusted Networ	k Policy	Connect \checkmark	
	Trusted DNS Dom	nains		
	Trusted DNS Serv Note: addi Trusted Servers (vers ng all DNS servers in use is recom @ https:// <server>[:<port>]</port></server>	mended with Trusted Network Detection	
	https://		Add	
			Delete	
				~
		📢 Help		

步驟2.建立AnyConnect VPN配置檔案

除管理VPN配置檔案外,還需要配置常規AnyConnect VPN配置檔案。AnyConnect VPN配置檔案 用於第一次連線嘗試,在此會話期間,管理VPN配置檔案從FTD下載。

使用AnyConnect配置檔案編輯器建立AnyConnect VPN配置檔案。在這種情況下,兩個檔案都包含 相同的設定,以便可以遵循相同的過程。

步驟3.將AnyConnect管理VPN配置檔案和AnyConnect VPN配置檔案上傳到FMC

建立配置檔案後,下一步是將其作為AnyConnect檔案對象上傳到FMC。

若要將新的AnyConnect管理VPN配置檔案上傳到FMC,請導航到Objects > Object Management,然後從目錄中選擇VPN選項,然後選擇Add AnyConnect File按鈕。

提供檔案的名稱,選擇AnyConnect Management VPN Profile作為檔案型別並儲存對象。

 \times



現在,若要上傳AnyConnect VPN配置檔案,請再次導航到Objects > Object Management,然後從 目錄中選擇VPN選項,然後選擇Add AnyConnect File按鈕。

提供檔案的名稱,但這次選擇AnyConnect VPN Profile作為檔案型別並儲存新對象。

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	te access VPN policies.	They can contain AnyConnect Client Profile and <i>i</i>	AnyConnect Clien	it Image f	îles.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	9.01095-webd	AnyConnect Client Image	200
Network Lists and Feeds IIII Lists and Feeds	AnyConnect_Management_Tu					gement_Tunne	AnyConnect Management VPN Profile	2 🖉 🖯
Sinkhole	SSL_AnyConnect.xml	Name:*	SSL_AnyConnect.xml		-	ml	AnyConnect VPN Profile	200
ास्त्र SLA Monitor ब्राह्म Time Range		File Name:*	SSL_AnyConnect.xml	Browse				
Time Zone		File Type:*	AnyConnect VPN Profile	~				
Inter Zone		Description:	AnyConnect Client Image AnyConnect VPN Profile	î				
\$ Variable Set			AnyConnect Management VPN Profile					
VLAN Tag			AMP Enabler Service Profile					
AnyConnect File			Feedback Profile					
R. Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile	- 18				
IKEv1 IPsec Proposal			Umbrella Roaming Security Profile	- 18				
S IKEv1 Policy			Web Security Service Profile	~				
() IKEv2 IPsec Proposal	<							>
B IKEv2 Policy						Displaying	1 - 3 of 3 rows 🛛 🛠 Page 1 of 3	S K K
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115	5.cisco.com	How To					uluilu cisco

必須將配置檔案新增到對象清單,並分別標籤為AnyConnect Management VPN Profile 和 AnyConnect VPN Profile。

Overview Analysis Policie	es Devices Objects AMP Intelligence		. Deploy System Help ▼ d	perezve 🔻
Object Management Intru	sion Rules			
AnyConnect File File objects represent files used in co	onfigurations, typically for remote access VPN policies. They can contain J	AnyConnect Client Profile and AnyConnect Client Image files.	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 SLA Monitor SLA Monitor Time Range Time Zone Time Zone Variable Set Variable Set VLAN Tag VNN AnyConnect File Group Policy	SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile	2 🥜 🖯
IKEv1 IPsec Proposal IKEv1 Policy IKEv1 Policy IKEv2 IPsec Proposal IKEv2 Policy	C	Displ	laying 1 - 3 of 3 rows 🛛 🗧 Page 🚺 of	> 1 > > c սիսիս

步驟4.建立組策略

若要建立新的組策略,請導航到Objects > Object Management,然後從目錄中選擇VPN選項,然後 選擇Group Policy,然後在Add Group Policy按鈕上按一下。

Add Group Policy 視窗開啟後,分配名稱,定義AnyConnect池並開啟AnyConnect 頁籤。導航到 Profile,然後在Client Profile下拉選單中選擇代表常規AnyConnect VPN配置檔案的對象。



然後導航到**Management Profile**頁籤,然後在**Management Profile**下拉選單中選擇包含 Management VPN Profile**的對**象。



儲存更改以將新對象新增到現有組策略。

Overview Analysis Policie	s Devices Objects AMP Intelligence		🌒 Deploy System Help 🔻 dp	erezve 🔻
Object Management Intrus	ion Rules			
Group Policy A Group Policy is a set of attribute ar profile.	d value pairs, stored in a group policy object, that define the remote acc	cess VPN experience. The RADIUS authorization server assigns the g	Add Group Policy	connection
Security Group Tag	Name			
DNS Lists and Feeds	AnyConnect_Management_Tunnel			6
Network Lists and Feeds	DfltGrpPolicy			/ 8
URL Lists and Feeds				
SIA Monitor				
Time Range				
👼 Time Zone				
Annel Zone				
🙆 URL				
\$ Variable Set				
📎 VLAN Tag				
4 😰 VPN				
MnyConnect File				
R. Certificate Map				
Group Policy				
IKEV1 IPsec Proposal				
IKEv1 Policy				
IKEv2 IPsec Proposal		Dicelard	ing 1 - 2 of 2 round 1/ / Dags 1 of 1	
W INEVZ POlicy		Ushay	ing 1 - 2 of 2 forms in C Page 1 of 1	110
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com	How To		uluilu cisco

步驟5.建立新的AnyConnect配置

FMC中的SSL AnyConnect配置由4個不同的步驟組成。要配置AnyConnect,請導航到**Devices >** VPN > Remote Access,然後選擇Add按鈕。此操作必須開啟**遠端訪問VPN策略嚮導**。

在**Policy Assigment**索引標籤上選擇手邊的FTD裝置,定義連線配置檔案的名稱並勾選SSL覈取方塊。

Overview Analysis Policies Devic Dashboards • Reporting Summary •	es Objects AMP Intelli	igence			$oldsymbol{ heta}_1$ Deploy Syster	n Help v	dperezve 🔻
Remote Access VPN Policy Wiz	ard						
1 Policy Assignment 2 Conn	ection Profile 🔰 3 AnyCo	onnect > 4	Access & Certificate	5) Summary			
Targeted Devic This wizard will gui a new user-defined Name:* Description: VPN Protocols: Targeted Devices:	es and Protocols de you through the required minima connection profile. AnyConnect_Management_Tunnel SSL IPSec-IKEv2 Available Devices Search Rdv-dperezve Rtdv-fejimene	Add	the Remote Access VPN policy with Selected Devices	Before You 3 Before You 3 Before you start, configuration elem complete Remote A Authentication Sic Configure Realm o or SSQ to authenti AnyConnect Clier Make sure you has for VPN Client do the relevant Clisco it during the wizarr Device Interfaces Interfaces Interfaces Interfaces Should b targeted <i>devices</i> sa as a security zone enable VPN access.	Start ensure the following ents to be in place to iccess VPN Policy. Erver r RADIUS Server Group tate VPN clients. It Package re AnyConnect package winloaded or you have credentials to download j. is already configured on that they can be used a or interface group to		
					Back	ext	Cancel
Last login on Thursday, 2021-03-25 at 17:01:05 PM	from rtp-vpn6-107.cisco.com		How To				

在Connection Profile上選擇Client Certificate Only作為身份驗證方法。這是該功能支援的唯一身份 驗證。

Overview Analysis Policies Devices Objects AMP In	elligence		y System	Help 🔻	dperezve 🔻
Device Management NAT VPN > Remote Access QoS P	atform Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
1 Policy Assignment 2 Connection Profile 3 A	yConnect $>$ 4 Access & Certificate $>$ 5 Summary				
Connection Profile: Connection Profiles specify the tunn accomplished and how addresses ar	group policies for a VPN connection. These policies pertain to creating the tunnel itself, how assigned. They also include user attributes, which are defined in group policies.	VAA is			^
Connection Profile Name:*	AnyConnect_Management_Profile				
	This name is configured as a connection alias, it can be used to connect to the VPN gateway				
Authentication, Authorization & Specify the method of authentication	ccounting (AAA): (AAA, certificates or both), and the AAA servers that will be used for VPN connections.				
Authentication Method:	Client Certificate Only				
Username From Certificate:	AAA Only ^istinguished Name) as username				
Primary Field:	SAML				
Secondary Field:	Client Certificate & AAA				
Authorization Server:	(Realm or RADIUS)				
Accounting Server:	V (RADIUS)				
Client Address Assignment:					
Client IP address can be assigned for assignment is tried in the order of A	m AAA server, DHCP server and IP address pools. When multiple options are selected, IP add A server, DHCP server and IP address pool.	355			
Use AAA Server (Realm or	RADIUS only) 🕕				
Use DHCP Servers					~
		Back	Nex	t	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To				cisco

然後在「組策略」(Group Policy)下拉選單中,選擇在步驟3中建立**的組策**略對象。

Overview Analysis Policies Devices Objects AMP Int	elligence	. ●1 Deplo	y System	Help 🔻	dperezve 🔻
Device Management NAT VPN > Remote Access QoS Pl	tform Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
1 Policy Assignment 2 Connection Profile 3 An	yConnect $>$ 4 Access & Certificate $>$ 5 Summary				
Authorization Server:	(Realm or RADIUS)				-
Accounting Server:	✓ ((RADIUS)				
Client Address Assignment: Client IP address can be assigned fro assignment is tried in the order of AA	n AAA server, DHCP server and IP address pools. When multiple options are selected, IP add A server, DHCP server and IP address pool.	ress			
Use AAA Server (Realm or Use DHCP Servers Use IP Address Pools	(ADIUS only) 🕕				
IPv4 Address Pools:	AnyConnect-Pool 🖉				
IPv6 Address Pools:	Ø				
Group Policy:					
A group policy is a collection of user- or create a Group Policy object.	riented session attributes which are assigned to client when a VPN connection is established	. Select			
Group Policy:*	AnyConnect_Management_Tunnel 💙 📀				
	AnyConnect_Management_Tunnel				
	DfltGrpPolicy V				
		Back	Nex	d	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To				uluilu cisco

在AnyConnect頁籤上,根據終端上的作業系統(OS)選擇AnyConnect檔案對象。

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

在Access & Certificate上,指定FTD必須使用的證書,以向Windows客戶端探測其身份。

附註:由於使用者在使用管理VPN功能時不應與AnyConnect應用互動,因此證書需要完全受 信任,並且不得列印任何警告消息。

附註:為了防止證書驗證錯誤,證書的使用者名稱中包含的公用名(CN)欄位必須與伺服器 XML配置檔案清單(步驟1和步驟2)中定義的FQDN匹配。



最後,在Summary頁籤上選擇Finish按鈕以新增新的AnyConnect配置。



步驟6.建立URL對象

導航到對象>對象管理,然後從目錄中選擇URL。然後在Add URL下拉選單中選擇Add Object。

提供對象的名稱,並使用在管理VPN配置檔案伺服器清單中指定的FQDN/使用者組定義URL(步驟 2)。 在本例中,URL必須是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

儲存更改以將對象新增到對象清單。

步驟7.定義URL別名

要在AnyConnect配置中啟用URL別名,請導航至**Devices > VPN > Remote Access**,然後按一下鉛 筆圖示進行編輯。

然後,在Connection Profile選項卡上,選擇手頭的配置,導航到Aliases,在Add按鈕上按一下,然 後在URL Alias下拉選單中選擇URL Object。確保選中Enabled覈取方塊。

Overview Analysis Policies Device	Edit Connection Profile ?	🗙 🎙 Deploy System Help 🔻 dperezve 🔻
Device Management NAT VPN ► Rem AnyConnect_Management_	Connection Profile:* AnyConnect_Management_Tunnel Group Policy:* AnyConnect_Management_Tunnel Edit Group Policy	Policy Assignments (1)
Connection Profile Access Interfaces	Client Address Assignment AAA Aliases Alias Names: Add URL Alias ?	
Name	Incoming users can ch can be turned on or of Can be turned on on or of Can be turned on or	
DefaultWEBVPNGroup	Name OK Cancel	/ 8
AnyConnect_Management_Tunnel		inel 🥜 🖥
	URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.	
	URL Status	
	Save Cancel	
Last login on Monday, 2021-04-05 at 23:55:27 PM from	n rtp-vpn4-759.cisco.com How To	cisco

儲存變更並將組態部署到FTD。



部署完成後,需要與AnyConnect VPN配置檔案進行第一個手動的AnyConnect連線。在此連線期間 ,管理VPN配置檔案從FTD下載並儲存在C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中。此後,後續連線必須通過管理VPN配置檔案啟動,無需任何使 用者互動。

疑難排解

對於證書驗證錯誤:

- •確保在FTD上安裝憑證授權單位(CA)的根憑證。
- 確保在Windows電腦應用商店上安裝由同一CA簽名的身份證書。
- 確保CN欄位包含在證書中,並且與管理VPN配置檔案的伺服器清單中定義的FQDN和URL別名 中定義的FQDN相同。

對於未啟動的管理隧道:

•確保管理VPN配置檔案已下載並儲存在C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中。

•確保管理VPN配置檔案的名稱為**VpnMgmtTunProfile.xml**。 對於連線問題,請收集DART捆綁包並聯絡Cisco TAC進行進一步研究。