# 在FMC管理的FTD上設定AnyConnect動態分割通 道

# 目錄

簡介 必要條件 需求 採用元件 背景資訊 限制 設定 步驟1.編輯組策略以使用動態拆分隧道 步驟2.配置AnyConnect自定義屬性 步驟3.驗證配置,儲存並部署 驗證 疑難排解 問題 解決方案 相關資訊 簡介

本檔案介紹如何在Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)上設定AnyConnect動 態分割通道。

# 必要條件

#### 需求

思科建議您瞭解以下主題:

- Cisco AnyConnect
- FMC基礎知識

#### 採用元件

本檔案中的資訊是根據以下軟體版本:

- FMC版本7.0
- FTD版本7.0

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。

由FMC管理的FTD上的AnyConnect動態拆分隧道配置在FMC 7.0版及更新版本上完全可用。如果運 行較舊版本,則需要按照<u>高級AnyConnect VPN部署(適用於FMC的Firepower威脅防禦)中的說明</u> 通過FlexConfig對其進行配置。

使用動態拆分隧道配置,您可以根據DNS域名微調拆分隧道配置。由於與完全限定的域名 (FQDN)關聯的IP地址可以更改,因此基於DNS名稱的分隔隧道配置可提供更動態的定義,說明哪些 流量是包括在遠端訪問虛擬專用網路(VPN)隧道中,哪些流量不是。如果為排除的域名返回的任何 地址在VPN中包含的地址池內,則這些地址將被排除。未阻止排除的域。相反,流向這些域的流量 保留在VPN隧道之外。

請注意,您還可以設定動態分割通道 定義要包含在通道中的域,否則將根據IP地址排除這些域。

#### 限制

目前,仍不支援這些功能:

- iOS(Apple)裝置不支援動態拆分隧道。 請參閱思科錯誤ID CSCvr54798
- Anyconnect Linux客戶端不支援動態拆分隧道。 請參閱Cisco錯誤IDCSCvt64988

### 設定

本節介紹如何在FMC管理的FTD上設定AnyConnect動態分割通道。

#### 步驟1.編輯組策略以使用動態拆分隧道

1.在FMC上,導航至**Devices > VPN > Remote Access**,然後選擇您要應用配置的**Connection Profile**。

Overview Analysis Policies Devices Objects AMP Intelligence	1		0, Deploy System Help v admin v
Device Management Device Upgrade NAT VPN > Remote Access 0	QoS Platform Settings FlexConfig Certificates		
SSL_AnyConnect			Save Cancel
			Policy Assignments (1)
		Local Realm: AmyConnect-Local-Aut	Dynamic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWE8VPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 5
SSL_AnyConnect_LocalAuth	Authentication: LOCAL Authorization: None Accounting: None	AnyConnect_Local_Auth	/ 9
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authorization: AnyConnect-LDAP-Auth (AD) Accounting: Mone	AnyConnect_LDAP_Auth	/ 8

2.選擇編輯組策略以修改已建立的一個組策略。

Overview Analysis Policies Devices Objects AMP Intellige	nce					0, Deploy System Help v admin
Device Management Device Upgrade NAT VPN + Remote Access	QoS Pla	tform Settings Flex	Config Certificates			
SSL_AnyConnect						Save Cancel
						Policy Assignments (1)
Connection Profile Access Interfaces Advanced					CALLE RECEIPTION TO A CONTRACTOR OF THE CALLED AND A CONTRACT OF THE CALLED AND A CONTRACT. THE CALLED AND A CONTRACT OF THE CALLED	Opininic Access Policy. <u>Environmenter</u>
						0
Name	AAA	Edit Connection Pr		2 ×		
DefaultWE8VPNGroup	Authent Authoriz Account	Connection Profile:*	SSL_AnyConnect_LocalAuth			/ 6
SSL_AnyConnect_LocalAuth	Authent Authoriz Account	Group Policy:*	Edit Group Policy		Auth	Ø 8
SSL_AnyConnect_LDAPAuth	Authent Authoriz Account	Client Address Assi	ignmene AAA Aliases	Ve/DHCP Sequere/A&A Sequere	Auth	/ 6
		Configure the 'Client	Address Assignment Policy' in the Advanced tab to de	ine the assignment criteria.		
		Address Pools:		0.		
		Name	IP Address Range			
		ftdv-dperezve-pool	172.16.13.1-172.16.13.254	28		
		DHCP Servers:		0		
		Name	DHCP Server IP Address			
		Configure device ov multiple device ov	errides in the address pool object to avoid IP address confi	ts in case of object is shared across		

# 步驟2.配置AnyConnect自定義屬性

1.在「組策略」配置下,導航至Anyconnect>自定義屬性,單擊Add(+)按鈕:

Overview Analysis Policies Devices Objects Integration		🔀 🖓 System Help v admin v
Device Management Device Upgrade NAT QoS Platform Settings FlexConfig	Certificates VPN + Remote Access Troubleshoot +	
FTD_RAVPN_Policy1		Save Carcel
		Policy Assignments (0) Local Realm: Local REALM1 Dynamic Access Policy: None
Connection Brofile Access Telesfaces Advanced	Edit Connection Profile ? ×	
Connection Prome Access Interfaces Advances	Add Group Policy ? ×	
	Name:* Anyconnect_Local_Auth	0
Namo AAA	Description:	
DefautWE8VPWGroup Authorits Authorits Accounts	General AnyConnect Advanced	/8
FTD_RAVPN_Policy11 Authents Authents Accounts	Profile AnyConnect Custom Attribute feature allows a more expedited way of configuring new Management Profile endpoint features on Firewall Threat Defense. This feature is supported on Firewall Client Modules Threat Defense 7.0 onwards.	1 /0
new-testo Authoriti Authoriti	SSL Settings	/8
	No records to display	

2.選擇**Dynamic Split Tunneling** AnyConnect屬性,然後按一下**Add(+)**按鈕以建立新的自定義屬性對 象:

Edit Connecti	ion Profile	? ×
Edit Group Po	licy	? ×
Name:*	Regular_Users_GP1	
Description:		
General Ar	nyConnect Advanced	
Profile Management Pro	AnyConnect Custom Attribute feature allows a more expedited way of configuring new endpoint features on Firewall Threat Defense. This feature is supported on Firewall	
Client Modules	Add Custom Attribute ? ×	0
Connection Set	AnyConnect Attribute:* Dynamic Split Tunneling	Ť.
	Custom Attribute Object:*	
	Add Cancel	
	Save Car	cel

3.輸入AnyConnect自定義屬性的名稱,並將域配置為動態包含或排除。

Overview Analysis Policies Devices Objects AMP Intelligence		0, Deploy System Help <del>v</del> admin v
Device Management Device Upgrade NAT VPN + Remote Access Qc	Platform Settings FlexConfig Certificates	
SSL_AnyConnect		🚍 Sova 🖉 Cancel
		Policy Assignments (1) Lecal Realm: <u>AnyConnect-Local-Aut</u> Dynamic Access Policy: <u>ansanc2-test</u>
Connection Profile Access Interfaces Advanced		
		0
Name	AA Edit Connection Profile	1 X
DefaultWEBVPNGroup	uthent uthent Edit Group Policy count	7 X
SSL_AnyConnect_LocalAuth	Viteen Name:* AnyConnect_Local_Auth	wm 20
SSL_AnyConnect_LDAPAuth	uthent uthors General AnyConnect Advanced	Auth 28 Add AnyConnect Custom Attribute 7 ×
	Concetton Set Concetton Set Co	Name:*

注意:您只能配置Include domains或Exclude domains。

在本例中,我們將cisco.com設定為要排除的網域,並將自訂屬性命名為Dynamic-Split-Tunnel,如 下圖所示:

Add AnyConnect Custor	m Attribute		? ×
Name:* Description:	Dynamic-Split-Tunnel		
AnyConnect Attribute:* Include domains:	Dynamic Split Tunneling Configure comma separated domain names that will	✓ be	
Exclude domains:	cisco.com	7	
Allow Overrides			
	Save	Cance	el 📄

### 步驟3.驗證配置,儲存並部署

驗證已設定的自訂屬性是否正確,儲存組態,並將變更部署至問題中的FTD。

lame:* Anyco	nnect_Local_Auth			
escription:				
General AnyConn	ect Advanced			
rofile fanagement Profile Jient Modules	AnyConnect Custo endpoint features	om Attribute feature on FTD. This featur	allows a more expedited way of configuring new e is supported on FTD 7.0 onwards.	•
SL Settings	Attribute	Name	Content	
Lustom Attributes	Dynamic Split Tunneling	Dynamic-Split	Include domains: None Reclude domains: cisco.com	ر ر
			Save Can	cel



您可以透過指令行介面(CLI)在FTD上運行以下命令,以確認動態分割通道組態:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <group-policy的名稱>

在本範例中,組態是下一步:

ftd# show run group-policy Anyconnect\_Local\_Auth group-policy Anyconnect\_Local\_Auth attributes vpn-idle-timeout 30 vpn-simultaneous-logins 3 vpn-session-timeout none vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelspecified ipv6-split-tunnel-policy-tunnelall split-tunnel-network-list value AC\_networks Default-domain none split-dns none address-pools value AC\_pool anyconnect-custom dynamic-split-exclude-domains value cisco.com anyconnect-custom dynamic-split-include-domains none ftd# show run webvpn webvpn enable outside anyconnect-custom-attr dynamic-split-exclude-domains anyconnect-custom-attr dynamic-split-include-domains http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable content-security-policy anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows" anyconnect profiles xmltest disk0:/csm/xmltest.xml anyconnect enable tunnel-group-list enable cache disable certificate-group-map cert\_map\_test 10 cert\_auth error-recovery disable 若要驗證使用者端上設定的動態通道排除,請執行以下操作:

1. 啟動AnyConnect軟體並按一下齒輪圖示,如下圖所示:



2.導覽至VPN > Statistics,並確認在Dynamic Split Exclusion/Inclusion下顯示的域:

🚳 Cisco AnyConnect Secure Mobility Client		-		×
cisco AnyConnect	t Secure Mobility Client			<b>(</b> )
Status Overview	Virtual Private Network (VPN)			
VPN >	Preferences Statistics Route Details Firewall Message History			
Network System Scan Roaming Security	Connection Information         State:       Connected         Tunnel Mode (IPv4):       Split Include         Tunnel Mode (IPv6):       Drop All Traffic         Dynamic Tunnel Exclusion:       cisco.com         Dynamic Tunnel Inclusion:       None         Duration:       00:00:25         Session Disconnect:       None         Management Connection State:       Disconnected (user tunnel active)         Address Information		•	^
Collect diagnostic information for all installed components.	Client (IPv4): Client (IPv6): Server: Bytes Reset	Exp	ort Stats	•

# 疑難排解

您可以使用AnyConnect診斷和報告工具(DART)來收集有助於排除AnyConnect安裝和連線問題的資料。

DART彙編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即可在客 戶端電腦上運行。

#### 問題

如果在AnyConnect自定義屬性(例如\*.cisco.com)中配置了萬用字元,則AnyConnect會話將斷開。

### 解決方案

您可以使用cisco.com網域值允許替代萬用字元。此更改允許您包括或排除www、cisco.com和 tools.cisco.com等域。

# 相關資訊

•如需其他協助,請聯絡技術協助中心(TAC)。需要有效的支援合約: <u>思科全球支援聯絡人.</u>

• 您還可以訪問Cisco VPN社群 此處.

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。