# 配置安全客戶端的本地LAN訪問

### 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> 設定 <u>FMC配置</u> <u>安全客戶端配置</u> <u>安全客戶端配置</u> <u>安全使用者端</u> <u>FTD CLI</u> <u>疑難排解</u>

## 簡介

本文檔介紹如何配置Cisco Secure Client以訪問本地LAN,同時仍然保持與頭端的安全連線。

## 必要條件

#### 需求

思科建議您瞭解以下主題:

- 思科安全防火牆管理中心(FMC)
- Cisco Firepower威脅防禦(FTD)
- 思科安全使用者端(CSC)

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 思科安全防火牆管理中心虛擬裝置版本7.3
- Cisco Firepower威脅防禦虛擬裝置版本7.3
- 思科安全使用者端版本5.0.02075

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

本文檔中描述的配置允許Cisco安全客戶端對本地LAN擁有完全訪問許可權,同時仍然保持與前端和 公司資源的安全連線。這可用於允許客戶端列印或訪問網路訪問伺服器(NAS)。

## 設定

#### FMC配置

在本文檔中,假設您已經有一個工作正常的遠端訪問VPN配置。

要新增本地LAN訪問功能,請導航到Devices > Remote Access,然後按一下相應遠端訪問策略上 的Edit按鈕。

þ	Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	<b>(</b> ) ;	¢ 0	admin $\vee$	cisco SECURE
													Add
Nan	ne		Status				Last Modified						
AC-	Policy		Targeting Up-to-dat	1 devices e on all target			2023-07-18 11:55:56 Modified by "admin"					· 「	

#### 然後, 導航到Advanced > Group Policies。

Firewall Management Devices / VPN / Edit Advanced	Center	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (	¢ 🎙	0	admin ~	-ilialia cisco	SECURE
AC-Policy													Save	Cancel
Enter Description												Polic	v Assiann	nents (1)
								Local Realm: LC	CAL			Dynamic Ac	cess Polic	sy: None
Connection Profile Access Interfa	aces Advand	ced												
Secure Client Images	Group Policie	s												
✓ Secure Client Customization	Group policy can I	be assigned to \	/PN user throug	h connection p	profile or by RA	DIUS server d	uring authentication.							
GUI Text and Messages	Following are the	group policies tl	hat are associa	ed with this Re	emote Access \	VPN configurat	ion. Add a group poli	icy if it is required to b	e assigi	ned by	RADIU	S server during	g authentic	ation.
Icons and Images														+
Scripts	Name		F	rotocol			DNS Servers		VPN	Filter				
Binaries														
Custom Installer Transforms	LocalLAN		s	SL,IKEV2										/ 🖬
Localized Installer Transforms	BlueGP		s	SL,IKEV2										11
Address Assignment Policy	RedGP		s	SL IKEV2										1 -
Certificate Maps	Neuur		,	56,INC #2										-
Group Policies														
LDAP Attribute Mapping														
Load Balancing														

按一下要配置本地LAN訪問的組策略上的Edit按鈕,並導航到Split Tunneling頁籤。

## Edit Group Policy

LocalLAN Description:
Description:
General Secure Client Advanced
VPN Protocols IPv4 Split Tunneling:
IP Address Pools Allow all traffic over tunnel
Banner IPv6 Split Tunneling:
DNS/WINS
Split Tunneling Split Tunnel Network List Type:
Standard Access List:
- +
DNS Request Split Tunneling
DNS Requests:
Send DNS requests as per split t▼
Domain List:
Cancel

在IPv4分割通道部分中,選擇Exclude networks specified below 選項。這提示選擇標準訪問列表。

6

## Edit Group Policy

Name:*	
LocalLAN	
Description:	
General Secu	re Client Advanced
VPN Protocols	IPv4 Split Tunneling:
IP Address Pools	Exclude networks specified belo
Banner	IPv6 Split Tunneling:
DNS/WINS	Allow all traffic over tunnel
Split Tunneling 🧕	Split Tunnel Network List Type: <ul> <li>Standard Access List</li> <li>Extended Access List</li> </ul>
	Standard Access List:
	<b>▼</b> +
	DNS Request Split Tunneling
	DNS Requests:
	Send DNS requests as per split t▼
	Domain List:
	Cancel

按一下+ 按鈕建立新的標準訪問清單。

Edit Standard Access List Object						
Name LocalLAN-Access						
▼ Entries (0)						
				Add		
Sequence No	Action	Network				
No records to display						
Allow Overrides						
			Cancel	Save		

按一下Add按鈕以建立標準訪問清單條目。此條目的Action必須設定為Allow。

Add Standard Access List Ent	try		8
Action: Allow ▼ Network: Available Network C ↓ Q Search PC2828 Router-1 Router-2 Routersub10 Sub1 Sub2 Sub3 Subint50	Add	Selected Network	
		Enter an IP address	Add
		Cancel	Add

按一下+按鈕新增新的網路對象。確保在Network 部分將此對象設定為Host,並在框中輸入 0.0.0.0。

Edit Network Object		9
Name LocalLAN Description Network Network 0.0.0.0 Allow Overrides	O FQDN	
	Cancel	Save

按一下Save按鈕並選擇新建立的對象。

Add Standard Access List Ent	ry		0
Action: Allow  Allow  Action: Network: Available Network C  Available Network Network Network C  Available Network	Add	Selected Network LocalLAN	
Router-2 Routersub10		Enter an IP address	Add
		Cancel	Add

按一下Add按鈕儲存Standard Access List條目。

Edit Standard Access List Object					
Name LocalLAN-Access					
▼ Entries (1)					
				Add	
Sequence No	Action	Network			
1	🔁 Allow	LocalLAN		/1	
Allow Overrides					
			Cancel	Save	

按一下Save按鈕,系統會自動選擇新建立的標準訪問清單。

## Edit Group Policy

Name:*	
LocalLAN	
Description:	
General Secure	Client Advanced
VPN Protocols IP Address Pools	IPv4 Split Tunneling: Exclude networks specified belo <sup>,</sup> ▼
Banner	IPv6 Split Tunneling:
DNS/WINS	Allow all traffic over tunnel
Split Tunneling	Split Tunnel Network List Type: <ul> <li>Standard Access List</li> <li>Extended Access List</li> </ul> Standard Access List: <ul> <li>LocalLAN-Access</li> <li>+</li> </ul>
	DNS Request Split Tunneling
	DNS Requests:
	Send DNS requests as per split t▼
	Domain List:
	Cancel

按一下Save按鈕並部署更改。

### 安全客戶端配置

預設情況下,本地LAN訪問選項設定為使用者可控。要啟用該選項,請按一下安全客戶端GUI上的 「齒輪」圖示。

8

S Cisco Secu	re Client	-		×
	AnyConnect VPN: Ready to connect. Testing-Deploy	~	Connect	
\$ ①				-1 1-1 1- CISCO

導覽至Preferences,並確保啟用Allow local(LAN)access when using VPN(if configured)選項。

S Cisco Secure Client	-		×			
Secure Client			1			
Virtual Private Network (VPN)	Diagnost	tics				
Preferences Statistics Route Details Firewall Message History						
<ul> <li>Minimize Cisco Secure Client on VPN connect</li> <li>Allow local (LAN) access when using VPN (if configured)</li> <li>Disable Captive Portal Detection</li> <li>Block connections to untrusted servers</li> </ul>						

## 驗證

安全使用者端

使用安全客戶端連線到頭端。

S Cisco Secure Client		-	
	AnyConnect VPN: Connected to FTD		Disconnect
00:00:20			IPv4
<b>\$</b> ()			-thata cisco

按一下齒輪圖示並導航至工藝路線詳細資訊。您可以看到,系統會自動檢測本地LAN並將其從隧道 中排除。



FTD CLI

若要確認組態是否成功套用,可以使用FTD的CLI。

<#root>

firepower#

show running-config group-policy LocalLAN

group-policy LocalLAN internal group-policy LocalLAN attributes banner value Local LAN Access is allowed wins-server none dns-server none dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ikev2 ssl-client split-tunnel-policy excludespecified ipv6-split-tunnel-policy tunnelall split-tunnel-network-list value LocalLAN-Access default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools value AC\_Pool webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

## 疑難排解

若要驗證是否已應用本地LAN存取功能,您可以啟用以下調試:

debug webvpn anyconnect 255

以下是成功偵錯輸出的範例:

<#root>

firepower# debug webvpn anyconnect 255 Validating the session cookie... Processing CSTP header line: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' Found WebVPN cookie: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' WebVPN Cookie: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' Cookie validation successfull, session authenticated http\_parse\_cstp\_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn\_cstp\_parse\_request\_field() ...input: 'Host: ftdv-cehidalg.cisco.com' Processing CSTP header line: 'Host: ftdv-cehidalg.cisco.com' webvpn\_cstp\_parse\_request\_field() ...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 5.0.02075' Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 5.0.02075' Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 5.0.02075' webvpn\_cstp\_parse\_request\_field() ...input: 'Cookie: webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05' Processing CSTP header line: 'Cookie: webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31B Session already authenticated, skip cookie validation webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line: 'X-CSTP-Version: 1' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Hostname: DESKTOP-LPMOG6M' Processing CSTP header line: 'X-CSTP-Hostname: DESKTOP-LPMOG6M' Setting hostname to: 'DESKTOP-LPMOG6M' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-MTU: 1399' Processing CSTP header line: 'X-CSTP-MTU: 1399' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Address-Type: IPv6, IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv6, IPv4' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Local-Address-IP4: 10.28.28.7' Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 10.28.28.7' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Base-MTU: 1500' Processing CSTP header line: 'X-CSTP-Base-MTU: 1500' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Remote-Address-IP4: 10.28.28.10' Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 10.28.28.10' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Full-IPv6-Capability: true' Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true' webvpn\_cstp\_parse\_request\_field() ...input: 'X-AnyConnect-STRAP-Pubkey: MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDKz/zLa3Yz+QJDHOYWfT6 Processing CSTP header line: 'X-AnyConnect-STRAP-Pubkey: MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDK Setting Anyconnect STRAP rekey public key(len: 124): MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDKz/zL webvpn\_cstp\_parse\_request\_field() ...input: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHnl0hOXV+/0I1/0lLjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj Processing CSTP header line: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHn10h0XV+/0I1/01LjBic/Nu/K2+N6E Setting Anyconnect STRAP client signature(len: 96): MEQCICzX1yDWLXQHnl0h0XV+/0I1/0lLjBic/Nu/K2+N6E5GAiA webvpn\_cstp\_parse\_request\_field() ...input: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942B75DF9A97C709325C3E Processing CSTP header line: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942 webvpn\_cstp\_parse\_request\_field() ...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-GCM-SHA25 Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-R Skipping cipher selection using DTLSv1 since a higher version is set in ssl configuration webvpn\_cstp\_parse\_request\_field() ...input: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AE Processing CSTP header line: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM- Selecting cipher using DTLSv1.2 webvpn\_cstp\_parse\_request\_field() ...input: 'X-DTLS-Accept-Encoding: lzs' Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs' webvpn\_cstp\_parse\_request\_field() ... input: 'X-DTLS-Header-Pad-Length: 0' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Accept-Encoding: lzs,deflate' Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate' webvpn\_cstp\_parse\_request\_field() ...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.' Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.' cstp\_util\_address\_ipv4\_accept: address asigned: 172.16.28.15 cstp\_util\_address\_ipv6\_accept: No IPv6 Address np\_svc\_create\_session(0xF36000, 0x000014d37b17c080, TRUE) webvpn\_svc\_np\_setup SVC ACL Name: NULL SVC ACL ID: -1 No SVC ACL Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406 tcp-mss = 1460path-mtu = 1460(mss)TLS Block size = 16, version = 0x304mtu = 1460(path-mtu) - 0(opts) - 5(ssl) = 1455mod-mtu = 1455(mtu) & 0xfff0(complement) = 1440 tls-mtu = 1440(mod-mtu) - 8(cstp) - 32(mac) - 1(pad) = 1399 DTLS Block size = 16 mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dt]shdr) - 16(dt]siv) = 1443 mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440 dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 48(mac) - 1(pad) = 1390 computed tls-mtu=1399 dtls-mtu=1390 conf-mtu=1406 DTLS enabled for intf=2 (outside) tls-mtu=1399 dtls-mtu=1390 SVC: adding to sessmgmt Sending X-CSTP-Split-Exclude msgs: for ACL - LocalLAN-Access: Start Sending X-CSTP-Split-Exclude: 0.0.0.0/255.255.255.255 Sending X-CSTP-MTU: 1399 Sending X-DTLS-MTU: 1390 Sending X-DTLS12-CipherSuite: ECDHE-ECDSA-AES256-GCM-SHA384 Sending X-CSTP-FW-RULE msgs: Start Sending X-CSTP-FW-RULE msgs: Done Sending X-CSTP-Quarantine: false Sending X-CSTP-Disable-Always-On-VPN: false Sending X-CSTP-Client-Bypass-Protocol: false

#### 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)。