# Configurer l'accès LAN local pour le client sécurisé

### Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Configurer configuration FMC Configuration du client sécurisé Vérifier Client sécurisé CLI FTD Dépannage

### Introduction

Ce document décrit comment configurer Cisco Secure Client pour accéder au LAN local tout en maintenant une connexion sécurisée à la tête de réseau.

### Conditions préalables

#### Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Secure Client (CSC)

#### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance virtuelle Cisco Secure Firewall Management Center version 7.3
- Appareil virtuel de défense contre les menaces Cisco Firepower version 7.3
- Client sécurisé Cisco version 5.0.02075

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

### Informations générales

La configuration décrite dans ce document permet au client sécurisé Cisco d'avoir un accès complet au LAN local tout en maintenant une connexion sécurisée à la tête de réseau et aux ressources de l'entreprise. Cela peut être utilisé pour permettre au client d'imprimer ou d'accéder à un serveur d'accès réseau (NAS).

## Configurer

#### configuration FMC

Dans ce document, il est supposé que vous avez déjà une configuration VPN d'accès à distance opérationnelle.

Pour ajouter la fonctionnalité d'accès LAN local, accédez à Devices > Remote Access et cliquez sur le bouton Edit sur la stratégie d'accès à distance appropriée.

Firewall Management Center Devices / VPN / Remote Access	Overview A	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	• 3	≎ 0	admin ~ 🔤	SECURE
												Add
Name		Status				Last Modified						
AC-Policy		Targeting Up-to-dat	1 devices le on all target			2023-07-18 11:55:56 Modified by "admin"					§/\$	

Accédez ensuite à Avancé > Stratégies de groupe.

AC-Policy Enter Description       Cancel         Enter Description       Cancel         Policy Assignments (1)       Cocal Realm: LOCAL       Dynamic Access Policy: None         Connection Profile       Access Interfaces       Advanced         Secure Client Images       Group Policies       Group Policies         Secure Client Customization       Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.         GUI Text and Messages       Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Scripts       Name       Protocol       DNS Servers       VPN Filter         Name       Protocol       DNS Servers       VPN Filter       Images         Address Assignment Policy       RedGP       SSL,IKEV2       Images       Images         RedGP       SSL,IKEV2       Images       Images       Images       Images       Images	Devices / VPN / Edit Advanced	Overview	Analysis Policies	Devices Objects	Integration	Deploy	९ 🔮 🌣	⑦ admin ∨	cisco SECURE
Binaries       Coalized Installer Transforms       Name       Protocol       DNS Servers       VPN Filter         Name       Sci, IKEV2       Image: Si, IKEV2	AC-Policy								Save Cancel
Connection Profile       Access Interfaces       Advanced         Secure Client Images       Secure Client Customization       Group Policies       Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.       Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         GUI Text and Messages       Group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Scripts       Name       Protocol       DNS Servers       VPN Filter         Icoalized Installer Transforms       Localized Installer Transforms       IcoalLAN       SL,IKEV2       Image: Coalized Installer Transforms         Address Assignment Policy       RedGP       SL,IKEV2       Image: Coalized Installer Transforms       Image: Coalized Installer Transforms	Enter Description							Polic	v Assignments (1)
Connection Profile       Access Interfaces       Advanced         Secure Client Images       Group Policies       Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.         GUI Text and Messages       Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.         Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Name       Protocol       DNS Servers       VPN Filter         Name       SL,IKEV2       Image:         Localized Installer Transforms       BlueGP       SL,IKEV2       Image:         RedGP       SL,IKEV2       Image:						Local Realm: LO	CAL	Dynamic Ac	ccess Policy: None
Secure Client Images       Group Policies         Secure Client Customization       Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.         GUI Text and Messages       Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Icons and Images       Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Name       Protocol       DNS Servers       VPN Filter         Icoalized Installer Transforms       LocalizAN       SSL_IKEV2       Image: SSL_IKEV2         Address Assignment Policy       RedGP       SSL_IKEV2       Image: SSL_IKEV2	Connection Profile Access Interfaces A	dvanced							
Secure Client Customization       Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.         GUI Text and Messages       Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Icons and Images       Name       Protocol       DNS Servers       VPN Filter         Binaries       LocalLAN       SSL,IKEV2       Images         Address Assignment Policy       RedGP       SSL,IKEV2       Images	Secure Client Images Group Po	licies							
GUI Text and Messages loons and Images       Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.         Scripts       Name       Protocol       DNS Servers       VPN Filter         Binaries       Localized Installer Transforms       Localized Installer Transforms       BilueGP       SSL,IKEV2       Image: SSL,IKEV2         Address Assignment Policy       RedGP       SSL,IKEV2       Image: SSL,IKEV2       Image: SSL,IKEV2	Secure Client Customization Group policy	can be assigned to VP	N user through connection	profile or by RADIUS server	during authentication	ı.			
Icons and Images       Protocol       DNS Servers       VPN Filter         Binaries       IcoalLAN       SSL,IKEV2       Image: Custom Installer Transforms         Localized Installer Transforms       IncoalLAN       SSL,IKEV2       Image: Custom Installer Transforms         Address Assignment Policy       RedGP       SSL,IKEV2       Image: Custom Installer Transforms	GUI Text and Messages Following an	e the group policies that	t are associated with this R	temote Access VPN configura	ation. Add a group p	olicy if it is required to be	assigned by R	ADIUS server during	g authentication.
Scripts     Name     Protocil     DNS Servers     VPN Filter       Binaries     LocalLAN     SSL,IKEV2     Image: SSL,IKEV2       Localized Installer Transforms     BlueGP     SSL,IKEV2       Address Assignment Policy     RedGP     SSL,IKEV2	Icons and Images								+
Binaries     LocalLAN     SSL,IKEV2       Localized Installer Transforms     BlueGP     SSL,IKEV2       Address Assignment Policy     RedGP     SSL,IKEV2	Scripts Name		Protocol		DNS Servers		VPN Filter		
Custom Installer Transforms     LocalLAN     SSL,IKEV2       Localized Installer Transforms     BlueGP     SSL,IKEV2       Address Assignment Policy     RedGP     SSL,IKEV2	Binaries								
Localized Installer Transforms         BlueGP         SSL,IKEV2         Image: Contribution of the second data and t	Custom Installer Transforms LocalLAN		SSL,IKEV2						/ 🖬
Address Assignment Policy Certificate Mans	Localized Installer Transforms BlueGP		SSL,IKEV2						/ 🖬
Certificate Mans	Address Assignment Policy		SSI IKEV/2						/ =
	DedOD		SSL,IKEVZ						<ul> <li>•</li> </ul>
Group Policies	Certificate Maps								
LDAP Attribute Mapping	Certificate Maps Group Policies								
Load Balancing	Certificate Maps Group Policies LDAP Attribute Mapping								

Cliquez sur le bouton Edit sur la stratégie de groupe où vous voulez configurer l'accès au réseau

local et naviguez jusqu'à l'onglet Split Tunneling.

Edit Group Policy		Ø
Name:* LocalLAN Description: General Secure	Client Advanced	
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	IPv4 Split Tunneling: Allow all traffic over tunnel  IPv6 Split Tunneling: Allow all traffic over tunnel  Split Tunnel Network List Type: Standard Access List  Extended Access List Standard Access List  INS Request Split Tunneling DNS Requests: Send DNS requests as per split t Domain List:	
	Cancel	ve

Dans la section Fractionnement de tunnel IPv4, sélectionnez l'option Exclure les réseaux spécifiés ci-dessous. Vous êtes alors invité à sélectionner une liste d'accès standard.

### Edit Group Policy

Name:*	
LocalLAN	
Description:	
General Secu	ire 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:
	Standard Access List
	▼ +
	DNS Request Split Tunneling
	DNS Requests:
	Send DNS requests as per split t▼
	Domain List:
	Cancer

Cliquez sur le bouton + pour créer une nouvelle liste d'accès standard.

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

Cliquez sur le bouton Add pour créer une entrée de liste d'accès standard. L'action de cette entrée doit être définie sur Autoriser.

Add Standard Access List Ent	ry		0
Action:	] - ]	Selected Network	
PC2828 Router-1 Router-2 Routersub10 Sub1 Sub2 Sub3	Add		
Subint50		Enter an IP address	Add
		Cancel	Add

Cliquez sur le bouton + pour ajouter un nouvel objet réseau. Assurez-vous que cet objet est défini en tant qu'hôte sur la section Réseau et entrez 0.0.0.0 dans la zone.

Edit Network Object		•
Name LocalLAN		
Description		
Network <ul> <li>Host</li> <li>Range</li> <li>Network</li> </ul> 0.0.0.0 Allow Overrides	⊖ FQDN	
	Cancel	Save

Cliquez sur le bouton Save et sélectionnez l'objet nouvellement créé.

Add Standard Access List Ent	ry		0
Action: Allow ▼ Network: Available Network C + Q Search	] - ]	Selected Network	T
NS-GW NS1 NS2 NS3 PC2828 Router-1	Add		
Router-2 Routersub10		Enter an IP address	Add
		Cancel	Add

Cliquez sur le bouton Add pour enregistrer l'entrée Standard Access List.

Edit Standard Access List Object				8
Name LocalLAN-Access				
▼ Entries (1)				
				Add
Sequence No	Action	Network		
1	🚭 Allow	LocalLAN		11
Allow Overrides				
			Cancel	Save

Cliquez sur le bouton Save et la liste d'accès standard nouvellement créée est automatiquement sélectionnée.

#### 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	Allow all traffic over turnel
DNS/WINS	
Split Tunneling	Split Tunnel Network List Type:
	Standard Access List LocalLAN-Access
	Send DNS requests as per split t▼
	Domain List:
	Cancel

Cliquez sur le bouton Save et déployez les modifications.

#### Configuration du client sécurisé

Par défaut, l'option Local LAN Access est définie sur User Controllable. Pour activer cette option, cliquez sur l'icône Gear (Engrenage) dans l'interface utilisateur graphique Secure Client.

8

S Cisco Secur	e Client	-		×
	AnyConnect VPN: Ready to connect. Testing-Deploy	~	Connect	
<b>\$</b> ()				-1 1-1 1- CISCO

Accédez à Préférences et vérifiez que l'option Autoriser l'accès local (LAN) lors de l'utilisation du VPN (si configuré) est activée.



### Vérifier

#### Client sécurisé

Connectez-vous à la tête de réseau à l'aide du client sécurisé.

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

Cliquez sur l'icône d'engrenage et accédez à Détails de la route. Ici, vous pouvez voir que le LAN local est automatiquement détecté et exclu du tunnel.



CLI FTD

Pour vérifier si la configuration a été correctement appliquée, vous pouvez utiliser l'interface de ligne de commande du FTD.

<#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

### Dépannage

Afin de vérifier si la fonctionnalité d'accès LAN local a été appliquée, vous pouvez activer ces débogages :

debug webvpn anyconnect 255

Voici un exemple de résultat de débogage réussi :

#### <#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): MEQCICzX1yDWLXQHnlOhOXV+/OI1/OlLjBic/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(dtlshdr) - 16(dtlsiv) = 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

#### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.