Configurer le tunnel VPN de gestion d'AnyConnect sur l'ASA

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Fonctionnement du tunnel de gestion
Limites
Configurer
Configuration sur ASA via ASDM/CLI
Création du profil VPN de gestion AnyConnect
Méthodes de déploiement pour profil VPN de gestion AnyConnect
(Facultatif) Configurez un attribut personnalisé pour prendre en charge la configuration de tous les tunnels
<u>Vérifier</u>
<u>Dépannage</u>
Informations connexes

Introduction

Ce document décrit la configuration de l'ASA comme passerelle VPN accepte les connexions du client AnyConnect Secure Mobility via le tunnel VPN de gestion.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN via Adaptive Security Device Manager (ASDM)
- Configuration de base de l'interface de ligne de commande ASA
- Certificats X509

Composants utilisés

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

• Logiciel Cisco ASA version 9.12(3)9

- Logiciel Cisco ASDM version 7.12.2
- Windows 10 avec Cisco AnyConnect Secure Mobility Client version 4.8.03036

Remarque : téléchargez le package de déploiement Web AnyConnect VPN (anyconnect-win*.pkg or anyconnect-macos*.pkg) à partir de la page Cisco <u>Software Download</u> (clients enregistrés uniquement). Copiez le client VPN AnyConnect dans la mémoire flash de l'ASA qui doit être téléchargé sur les ordinateurs des utilisateurs distants pour établir la connexion VPN SSL avec l'ASA. Référez-vous à la section <u>Installation du client AnyConnect</u> du guide de configuration ASA pour plus d'informations.

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

Un tunnel VPN de gestion assure la connectivité au réseau d'entreprise chaque fois que le système client est mis sous tension, et pas seulement lorsqu'une connexion VPN est établie par l'utilisateur final. Vous pouvez effectuer la gestion des correctifs sur les terminaux hors du bureau, en particulier les périphériques qui sont rarement connectés par l'utilisateur, via un VPN, au réseau du bureau. Les scripts de connexion au système d'exploitation des terminaux qui nécessitent une connectivité réseau d'entreprise bénéficient également de cette fonctionnalité.

AnyConnect Management Tunnel permet aux administrateurs de connecter AnyConnect sans intervention de l'utilisateur avant la connexion de l'utilisateur. Le tunnel de gestion AnyConnect peut fonctionner en association avec la détection de réseau sécurisé et n'est donc déclenché que lorsque le terminal est hors site et déconnecté d'un VPN initié par l'utilisateur. Le tunnel de gestion AnyConnect est transparent pour l'utilisateur final et se déconnecte automatiquement lorsque l'utilisateur lance le VPN.

SE/Application	Version minimale requise
ASA	9.0.1
ASDM	7.10.1
Version de Windows AnyConnect	4.7.00136
Version de macOS AnyConnect	4.7.01076
Linux	Non Pris En Charge

Fonctionnement du tunnel de gestion

Le service d'agent VPN AnyConnect est automatiquement démarré au démarrage du système. Il détecte que la fonctionnalité de tunnel de gestion est activée (via le profil VPN de gestion), par conséquent il lance l'application cliente de gestion pour initier une connexion de tunnel de gestion. L'application cliente de gestion utilise l'entrée d'hôte du profil VPN de gestion pour initier la

connexion. Ensuite, le tunnel VPN est établi comme d'habitude, à une exception près : aucune mise à jour logicielle n'est effectuée pendant une connexion de tunnel de gestion puisque le tunnel de gestion est censé être transparent pour l'utilisateur.

L'utilisateur lance un tunnel VPN via l'interface utilisateur AnyConnect, ce qui déclenche la fin du tunnel de gestion. À la fin du tunnel de gestion, l'établissement du tunnel utilisateur se poursuit comme d'habitude.

L'utilisateur déconnecte le tunnel VPN, ce qui déclenche le rétablissement automatique du tunnel de gestion.

Limites

- Interaction utilisateur non prise en charge
- L'authentification basée sur les certificats via le magasin de certificats de l'ordinateur (Windows) est uniquement prise en charge
- Vérification stricte du certificat du serveur
- Un proxy privé n'est pas pris en charge
- Un proxy public n'est pas pris en charge (la valeur ProxyNative est prise en charge sur les plates-formes où les paramètres du proxy natif ne sont pas récupérés du navigateur)
- Les scripts de personnalisation AnyConnect ne sont pas pris en charge

Remarque : pour plus d'informations, reportez-vous à <u>A propos du tunnel VPN de gestion.</u>

Configurer

Cette section décrit comment configurer Cisco ASA en tant que passerelle VPN pour accepter les connexions des clients AnyConnect via le tunnel VPN de gestion.

Configuration sur ASA via ASDM/CLI

Étape 1. Créez la stratégie de groupe AnyConnect. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > Group Policies. Cliquez surAdd.

Remarque : il est conseillé de créer une nouvelle stratégie de groupe AnyConnect qui est utilisée pour le tunnel de gestion AnyConnect uniquement.



Étape 2. Fournissez uneNamebase pour la stratégie de groupe. Attribuer/Créer unAddress Pool. ChoisissezTunneling ProtocolsasSSL VPN Clientet/OUIPsec IKEv2, comme illustré dans l'image.

• • • • • • • • • • • • • • • • • • • •	·····	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	Name: AnyConnect_MGMT_1	funnel	
Advanced	Banner: 🗹 Inherit		
	SCEP forwarding URL: 🗹 Inherit		
	Address Pools: Inherit VPN_Po	ol	Select
	IPv6 Address Pools: 🗹 Inherit		Select
	More Options		*
	Tunneling Protocols:	Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPse	ю
	Filter:	✓ Inherit	Manage
	Access Hours:	✓ Inherit	Manage
e e e e e e e e e e e e e e e e e e e	Simultaneous Logins:	C Inherit	
	Restrict access to VLAN:	☑ Inherit 0	
	Connection Profile (Tunnel Group) Lock:	☑ Inherit 0	
	Maximum Connect Time:	✓ Inherit Unlimited minutes	
	Idle Timeout:	✓ Inherit None minutes	
	Security Group Tag (SGT):	✓ Inherit None (2 - 65519)	
	On smart card removal:	☑ Inherit O Disconnect Keep the connection	
	Timeout Alerts		
	Maximum Connect Time Alert Interval:	✓ Inherit Default minutes	
	Periodic Certificate Authentication Interval	: 🔽 Inherit 🗌 Unlimited hours	
Find:	Next	Previous	
		Help Cancel OK	

Étape 3. Accédez àAdvanced > Split Tunneling. Configurez lePolicyen tant queTunnel Network List Belowet choisissez leNetwork List, comme illustré dans l'image.

• • •		Edit Internal G	Froup Policy: AnyConnect_MGMT_	Tunnel	
General Servers	The VPN client makes split tunneling dee fields.	cisions on the	basis of a network list that can	be specified below by providing the proper parameters to 'Policy	' and 'Networl
Split Tunneling	DNS Names:	🗹 Inherit			
Browser Proxy ► AnyConnect Client ► IRsec(/(Sv1) Client	Send All DNS Lookups Through Tunnel:	Inherit	🔿 Yes 💿 No		
P IFSec(IKEV1) Client	Policy:	Inherit	Tunnel Network List Below		3
	IPv6 Policy:	🗹 Inherit		<	
	Network List:	Inherit	VPN-Split		Manag
•	Pressing this button to set up split exlus Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	ion for Web S ty	Security proxies.		
Find:	Next 🔘	Previous			
		Help	Cancel OK	1	

Remarque : si une adresse de client n'est pas transmise pour les deux protocoles IP (IPv4 et IPv6), le paramètre doit êtreclient Bypass Protocolenabled défini de sorte que le trafic correspondant ne soit pas perturbé par le tunnel de gestion. Pour configurer, reportez-vous à l'étape 4.

Étape 4. Accédez àAdvanced > AnyConnect Client. DéfiniClient Bypass ProtocolSurEnable. Cliquez surOKSave (Enregistrer), comme illustré dans l'image.

•		Add Internal Group Policy	
General	Keep Installer on Client System:	✓ Inherit Yes No	
Servers Advanced	Datagram Transport Layer Security (DTLS):	✓ Inherit	
Split Tunneling	DTLS Compression:	✓ Inherit	
Browser Proxy AnyConnect Client	SSL Compression:	☑ Inherit O Deflate O LZS O Disable	
IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	✓ Inherit ○ Enable ○ Disable	
	Client Bypass Protocol:	Inherit O Enable Disable	
	FQDN of This Device:	V FQDN	
	MTU:	✓ Inherit	
	Keepalive Messages:	✓ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	☑ Inherit	
	• Always-On VPN:	☑ Inherit O Disable O Use AnyConnect Profile setting 0	
	Client Profiles to Download:	🗹 Inherit	
		Add 1 Delete	
		Profile Name Profile Usage/Type	
			_
			_
nd:	Next 🔘	Previous	

Étape 5. Comme le montre cette image, cliquez surApplypour transmettre la configuration à l'ASA.

🐔 Home 🎭 Configuration 🝺 Monitoring 识	Save 🔇 Refresh 🔇 Back 🔘 Forw	rard ? Help Type topic Go			diala cisco
000 Remote Access VPN	○ ○ ○ Configuration > Remote Acc	cess VPN > Network (Client) Acces	s > Group Policies		
Introduction Introduction Network (Client) Access AnyConnect Connection Profiles MayConnect Customization/Localizati AnyConnect Client Profile MayConnect Client Profile	Manage VPN group policies.A VPN gr policy information is referenced by V To enforce authorization attributes f � Add • @ Edit @ Delete X As:	roup is a collection of user-oriented VPN connection profiles and user ac from an LDAP server you must use a sign	authorization attribute/value pairs that may be stored in counts. n LDAP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The gro	φ
Anyconnect Clerin Solution	Name	Type	Tunneling Protocol	Connection Profiles / Users	
Group Policies	Am Connect	Internal	cel ellens	Assigned To	_
IPsec(IKEv1) Connection Profiles	DftrCrnPolicy (System Default)	Internal	ikav1:ikav2:12to_insec	DefaultRACroup Default 21 Group DefaultADMINGroup De	aultWF
Psec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2:ssl-client	AnyConnect MGMT Tunnel	
 > m Address Assignment > m Address Assignment > m Advanced > m Contentions SSL VPN Access > m Advanced Uters M Advanced Uters > m Advanced Uters > m Advanced Uters > m Secure Desktop Manager > m Contificate Manager > m Content Conte					
Device Setup					
Remote Access VPN					
Site-to-Site VPN	Find:	Match Case			
Device <u>M</u> anagement			Reset		

Configuration CLI pour la stratégie de groupe :

<#root>

ip local pool

VPN_Pool

192.168.10.1-192.168.10.100 mask 255.255.255.0 !

access-list

VPN-Split

standard permit 172.16.0.0 255.255.0.0
!
group-policy

AnyConnect_MGMT_Tunnel

internal group-policy

AnyConnect_MGMT_Tunnel

attributes vpn-tunnel-protocol

ikev2 ssl-client

split-tunnel-network-list value

VPN-Split

```
client-bypass-protocol enable
address-pools value
VPN_Pool
```

Étape 6. Créez le profil de connexion AnyConnect. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Cliquez surAdd.

Remarque : il est conseillé de créer un nouveau profil de connexion AnyConnect, utilisé uniquement pour le tunnel de gestion AnyConnect.



Étape 7. Fournissez un_{Name}pour le profil de connexion et définissez-le_{Authentication Method}Sur_{Certificate} only. Sélectionnez la_{Group} Policycomme celle créée à l'<u>étape 1</u>.

Basic Advanced	Name:	AnyConnect_MGMT_Tunnel	
Advanced	Aliases:		
	Authentication		
	Method:	Certificate only	
	AAA Server Group:	LOCAL	S Manage
		Use LOCAL if Server Group fails	
	SAML Identity Provider		
	SAML Server :	None	S Manage
	Client Address Assignment		
	DHCP Servers:		
		• None OHCP Link OHCP Subnet	
	Client Address Pools:		Select
	Client IPv6 Address Pools	:	Select
	Default Group Policy		
	Group Policy:	AnyConnect_MGMT_Tunnel	Manage
	(Following fields are linke	ed to attribute of the group policy selected above.)	
	🗹 Enable SSL VPN clie	ent protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
et a la			
Find:		Wext Previous	

Remarque : assurez-vous que le certificat racine de l'autorité de certification locale est présent sur l'ASA. Accédez àConfiguration > Remote Access VPN > Certificate Management > CA Certificatespour ajouter/afficher le certificat.

Remarque : vérifiez qu'un certificat d'identité émis par la même autorité de certification locale existe dans le magasin de certificats de l'ordinateur (pour Windows) et/ou dans la chaîne de clés système (pour macOS).

Étape 8. Accédez àAdvanced > Group Alias/Group URL. CliquezAddsousGroup URLset ajoutez unURL. Assurezvous queEnabledest coché. Cliquez surokSave (Enregistrer), comme illustré dans l'image. Add AnyConnect Connection Profile

Basic V Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securld messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Celete (The table is in-line editable.) Alias
	Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel Cancel OK
Find:	Next Previous Help Cancel OK

Si IKEv2 est utilisé, assurez-vous queIPsec (IKEv2) Accessest activé sur l'interface utilisée pour AnyConnect.

O O Remote Access VPN	Config	uration > Remot	e Access VPN > N	letwork (Client) A	ccess > AnyConnect Co	nnection Profiles
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	appliance automa rts IPsec (IKEv2) tu	tically deploys the innel as well as SS	Cisco AnyConnec L tunnel with Data	ct VPN Client to remote us agram Transport Layer Sec	ers upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN urity (DTLS) tunneling options.
AnyConnect Customization/Local AnyConnect Client Profile AnyConnect Client Software	Enable C SSL access m	es isco AnyConnect \ ust be enabled if !	VPN Client access you allow AnyCon	on the interfaces :	selected in the table below	/ /eb Launch) .
Group Policies Precikevity Connection Profiles	Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acce Allow Access	Enable Client Services	Device Certificate
IPsec(IKEv2) Connection Profiles Secure Mobility Solution Address Assignment	inside		Ő	- Ö	Ö	Port Settings

Étape 9. Cliquez sur_{Apply}pour transmettre la configuration à l'ASA.



Configuration CLI pour le profil de connexion (tunnel-group) :

```
<#root>
tunnel-group
AnyConnect_MGMT_Tunnel
type remote-access
tunnel-group
AnyConnect_MGMT_Tunnel
general-attributes
default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
authentication certificate
group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Étape 10. Assurez-vous qu'un certificat sécurisé est installé sur l'ASA et lié à l'interface utilisée pour les connexions AnyConnect. Accédez à pourConfiguration > Remote Access VPN > Advanced > SSL settingsajouter/afficher ce paramètre.

Remarque : reportez-vous à Installation of Identity Certificate on ASA.

Remote Access VPN	Configuration > Remote Access VP	N > Advanced > SSL Settings				
Introduction	[
Network (Client) Access AnyConnect Connection Pr	Configure SSL parameters. These parameter	rs affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization	The minimum SSL version for the security	appliance to negotiate as a "server":	TLS V1	🖸 💿 DTLS	W1 OTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the security	appliance to negotiate as a "client":	TLS V1	٥		
Group Policies	Diffie-Hellman group to be used with SSL:		Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	0		
Secure Mobility Solution	Encountion					
Sp Address Assignment	cheryption				hele c	
Advanced	Cipher version	Cipher Security Level		Cipher Algorithms/ Custom:	string	Edit
Clientless SSL VPN Access	Default	Medium		DES-CBC3-SHA AES128-SH	IA DHE-RSA-AES128-SHA AES256-SHA DHE-RSA	
AAA/Local Urerr	TLSV1	Medium		DHE-RSA-AES256-SHA AE	S256-SHA DHE-RSA-AES128-SHA AES128-SHA	
With the Comment	TLSV1.1	Medium		DHE-RSA-AES256-SHA AE	S256-SHA DHE-RSA-AES128-SHA AES128-SHA	
Novi Server Groups	TLSV1.2	Medium		ECDHE-ECDSA-AES256-G	CM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
LDAP Attribute Map	DTLSV1	Medium		DHE-RSA-AES256-SHA AE	S256-SHA DHE-RSA-AES128-SHA AES128-SHA	
Cocal Users	DTLSV1.2	Medium		ECDHE-ECDSA-AES256-G	CM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing						
DHCP Server	Server Name Indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						
Consection Consection						Edit
Connection Gateway						Cont
SSL Settings						Delete
B Reference Identity						Delete
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
Crypto Engine						
a a the sudare						
	Carlificator					
	Certificates					
	Specify which certificates, if any, should	be used for SSL authentication on ea	ch interface. The fallback certificate	will be used on interfaces not as	sociated with a certificate of their own.	
	Interface	Primary Certificate	Load Balancing Certificate	Kev-T	VDF	C.dia
evice Setup	inside		construction of the second sec	Nep -		Ealt
	mananament					
rewall	Inutride	POOT_CA:bostonme_ASA_evample	(A)	Prima	or PCA (2049 bits) Load Palancing: none	
and a second second	louside	IKOO1+CA:nostname=ASA.example	S0m	Prima	ry, Kak (2046 bits), Load Balancing, none	
emote Access VPN						
te-to-Site VPN						
evice Management						

Configuration CLI pour le point de confiance SSL :

<#root>

ssl trust-point ROOT-CA outside

Création du profil VPN de gestion AnyConnect

Étape 1. Créez le profil client AnyConnect. Accédez àConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Cliquez surAdd, comme illustré dans l'image.

🔥 Hon	ne 🔏 Configuration 📴 Monitori	ng 🔚 Save 🔇 Refresh 🔇 Back 🔘	Forward 💡 Help Type topic Go			cisco
0	Remote Access VPN	○ ○ ○ Configuration > Remote Acces	ss VPN > Network (Client) Access > AnyCo	nnect Client Profile		
Bookmarks	Introduction Network (Client) Access MayConnect Connection Profil MayConnect Customization/Lc MayConnect Client Profile AnyConnect Client Software AnyConnec	This panel is used to manage AnyCom button to add a new profile. Pressing t The profile Usage field is introduced w HostScan configuration can be perform Add Edir [25] Change Group Pol	nect Client Profiles and perform group assign he Import or Export button is for upload and ith the Secure Mobility Solution. This field co ned by going to Secure Desktop Manager/Ho (cy) Delete 3 Import 3 Export 3 Valida	ment for AnyConnect version 2.5 or later. You can select download of client profiles between local machine and du ontains different profile usage in AnyConnect version 3.0 stScan. If 'HostScan' is not visible under 'Secure Desktop te	x profile to edit, change group or to delete. You can select the 'Add' vice. and later. Manager', you will need to restart ASDM.	
	IPsec(IKEv1) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
) 	Psec(IXEV2) Connection Profil Psec(IXEV2) Connection Profil Psecure Mobility Solution Pa Address Assignment Advanced Clenties SSL VPN Access Advanced Clenties SSL VPN Access Advanced Charles SSL VPN Access Consection Consection Profile Control Consection Consection Advanced Connection Cateway SSL Settings	T UNE NAITE	rione usage	Lindų Folky	Prome Location	
	Reference Identity Reference Identity Crificate to AryConnect and HTTP Reference Identity Crypto Engine Crypto Engine Perice Setup Firewall Ster-to-Site VPN Device Management					
	*			Reset Apply		

Étape 2. Fournissez unProfile Name. Sélectionnez leProfile UsageCommeAnyConnect Management VPN profile. Sélectionnez leGroup Policyqui a été créé à l<u>'étape 1</u>. Cliquez surok, comme illustré dans l'image.

Profile Name		Profile Usage	Group Policy	Profile Location
	• • •	Add AnyConnect Client Pro	file	
	Profile Name	AnyConnect_MGMT_Profile		
	Profile Usage	AnyConnect Management VPN Profile	0	
	Enter a device f created if it doe	ile path for an xml file, ie. disk0:/ac_profile. The file wi s not exist.	II be automatically	
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Browse Flash	
			Upload	
	Group Policy	AnyConnect_MGMT_Tunnel	©	
		Enable 'Always On VPN' for selected group		
		Help Cancel	ОК	
			Reset Apply	

Étape 3. Choisissez le profil créé et cliquez sur Edit, comme indiqué dans l'image.



Étape 4. Accédez à Server List. CliquezAdd pour ajouter une nouvelle entrée de liste de serveurs, comme illustré dans l'image.

	Any	Connect Client Profile Ec	litor - AnyConnect_MGI	MT_Profile				
Profile: AnyConnect_MG	MT_Profile					About		
VPN Preferences (Part 1) Preferences (Part 2) Backup Servers Certificate Pinning Certificate Matching Server List	Server List							
	Hostname	Host Address	User Group	Backup Server List	Certificate Pins			
•	Note: at most o	ne server can be define	d in a management VP	N profile. Add Edit	Delete Details			
		Help	ancel OK					

Étape 5. Fournissez unDisplay Name. Ajoutez leFQDN/IP addressde l'ASA. Fournissez leUser Groupcomme nom du groupe de tunnels.Group URLest automatiquement renseigné avec leFQDNet leUser Group. Cliquez surok.

Server	Certificate Pinning
Primary Server Display Name (required) AnyConnect_MGMT_Tunnel FQDN or IP Addr User Group (required) asa.example.com / AnyConnect_MGMT. Group URL asa.example.com/AnyConnect_MGMT_Tunnel	Connection Information Primary Protocol SSL 🗘 ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect 🗘 IKE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up Move Down Delete
ок ок Nemarque : le nom de domaine complet/	^{Cancel} adresse IP + groupe d'utilisateurs doit être

identique à l'URL du groupe mentionnée lors de la configuration du profil de connexion AnyConnect à l'<u>étape 8</u>.

Remarque : AnyConnect avec IKEv2 en tant que protocole peut également être utilisé pour établir un VPN de gestion vers ASA. Assurez-vousPrimary Protocolque est défini surIPsecà l'étape <u>5</u>.

Étape 6. Comme le montre l'image, cliquez surokEnregistrer.

8 🕘 🖶	AnyC	connect Client Profile Edit	or - AnyConnect_MGM	T_Profile	
Profile: AnyConnect_MG	MT_Profile				Abo
VPN Preferences (Part 1) Preferences (Part 2)	Server List				
Backup Servers	Hostname AnyConnect_MGMT	Host Address _T asa.example.com	User Group AnyConnect_MGMT	Backup Server List T Inherited	Certificate Pins
	Note: at most on	e server can be defined	in a management VPN	profile. Add	Delete Details
e					
		Help Ca	ncel OK]	

Étape 7. Cliquez sur_{Apply}pour envoyer la configuration à l'ASA, comme illustré dans l'image.



Configuration CLI après l'ajout du profil VPN de gestion AnyConnect.

<#root>

```
webvpn
 enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
ļ
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

webvpn

Profil VPN de gestion AnyConnect sur la machine cliente AnyConnect :

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
```

true

<ShowPreConnectMessage>false</ShowPreConnectMessage>

Machine

System

true

<ProxySettings>IgnoreProxy</ProxySettings> <AllowLocalProxyConnections>true</AllowLocalProxyConnections> <AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---

<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover> <AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>

AnyConnect_MGMT_Tunnel

asa.example.com

</AnyConnectProfile>

Remarque : si le protocole TND (Trusted Network Detection) est utilisé dans le profil VPN AnyConnect de l'utilisateur, il est conseillé de faire correspondre les mêmes paramètres dans le profil VPN de gestion pour une expérience utilisateur cohérente. Le tunnel VPN de gestion est déclenché en fonction des paramètres TND appliqués au profil de tunnel VPN utilisateur. En outre, l'action TND Connect dans le profil VPN de gestion (appliquée uniquement lorsque le tunnel VPN de gestion est actif), s'applique toujours au tunnel VPN de l'utilisateur, afin de garantir que le tunnel VPN de gestion est transparent pour l'utilisateur final.

Remarque : sur tout PC d'utilisateur final, si les paramètres TND sont activés sur le profil VPN de gestion et si le profil VPN d'utilisateur est manquant, il considère les paramètres de préférences par défaut pour le TND (il est désactivé sur les préférences par défaut dans l'application cliente AC) à la place du profil VPN d'utilisateur manquant. Cette noncorrespondance peut conduire à un comportement inattendu/indéfini.

Par défaut, les paramètres TND sont désactivés dans les préférences par défaut. Pour surmonter les préférences par défaut des paramètres codés en dur dans l'application client AnyConnect, l'ordinateur de l'utilisateur final doit avoir deux profils VPN, un profil VPN utilisateur et un profil VPN de gestion AC, et les deux doivent avoir les mêmes paramètres TND.

La logique derrière la connexion et la déconnexion du tunnel VPN de gestion est que pour établir un tunnel VPN de gestion, l'agent AC utilise les paramètres TND du profil VPN utilisateur et pour la déconnexion du tunnel VPN de gestion, il vérifie les paramètres TND du profil VPN de gestion.

Méthodes de déploiement pour profil VPN de gestion AnyConnect

• Une connexion VPN utilisateur réussie est établie avec le profil de connexion ASA afin de télécharger le profil VPN de gestion AnyConnect à partir de la passerelle VPN.



connexion doit être établie via SSL (afin de télécharger le profil VPN de gestion AnyConnect depuis l'ASA).

 Le profil VPN de gestion AnyConnect peut être téléchargé manuellement sur les ordinateurs clients, soit par diffusion d'un objet de stratégie de groupe, soit par installation manuelle (assurez-vous que le nom du profil estvpnMgmtTunProfile.xml).

Emplacement du dossier où le profil doit être ajouté : Fenêtres: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun macOS : /opt/cisco/anyconnect/profile/mgmttun/

(Facultatif) Configurez un attribut personnalisé pour prendre en charge la configuration de tous les tunnels

Le tunnel VPN de gestion nécessite un fractionnement qui inclut la configuration du tunneling, par défaut, pour éviter un impact sur la communication réseau initiée par l'utilisateur. Cela peut être remplacé lorsque vous configurez l'attribut personnalisé dans la stratégie de groupe utilisée par la connexion du tunnel de gestion.

Étape 1. Accédez à Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Cliquez sur , comme illustré dans l'image.

	Home 😵 Configuration 📴 Monitoring	, sa	ave 🚱 Refresh 🔇 Back 💭 Forward 🦻 Help Type topic Go	isco
5	Remote Access VPN		O Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes	
Device L	Introduction Network (Client) Access AnyConnect Connection Profiles		Declarations of custom attribute types and these attributes are enforced in <u>AnyConnect group policy</u> , <u>AnyConnect dynamic access policy</u> and <u>AnyConnect custom attribute names</u>	
	AnyConnect Customization/Localizati		Add E Edit Delete	
	AnyConnect Client Profile		Type Description	
ark	AnyConnect Client Software			
-ke	Population of the second secon			
8	Group Policies			
	Psec(KEv2) Connection Profiles			
	Secure Mobility Solution			
	Address Assignment			
	V 🗟 Advanced			
	AnyConnect Essentials			
	AnyConnect Custom Attributes			
	IPsec			
	ACL Manager			
	Clientless SSL VPN Access			
	AAA/Local Users			
	AAA Server Groups			
	CDAP Attribute Map			
	A Secure Desktop Manager			
	E Certificate Management			
	language Localization			
	Sector Contracting			
	P DHCP Server			
	Advanced			
	Device Setup			
	Firewall			
	Cal Remote Access VPN			
	Conde Access And			
	Site-to-Site VPN			
	Device Management		L	_
	×		Reset Apply	
	-			

Étape 2. Définissez l'attribut personnalisé Type surManagementTunnelAllAllowed et fournissez un Description. Cliquez surok, comme illustré dans l'image.

OOO Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes

			Description		
	Create Custo	om Attribute Type			
•••	Create Custo	om Attribute Type			
• • Type:	Create Custo	om Attribute Type			
• • • Type:	Create Custo ManagementTunnelAllAllowed ManagementTunnelAllAllowed	om Attribute Type			
Type: Description	Create Custo ManagementTunnelAllAllowed ManagementTunnelAllAllowed	om Attribute Type d			
Type: Description	Create Custo ManagementTunnelAllAllowed ManagementTunnelAllAllowed	om Attribute Type d			
Type: Description	Create Custo ManagementTunnelAllAllowed ManagementTunnelAllAllowed	om Attribute Type	1		

Étape 3. Accédez à Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Cliquez sur , comme illustré dans l'image.



Étape 4. Sélectionnez le type ManagementTunnelAllAllowed. Définissez le nom surtrue. CliquezAddpour fournir une valeur d'attribut personnalisée, comme illustré dans l'image.

0 O Configuration > Re	mote Access VPN > Network (Client) Access > Ad	vanced > AnyConnect Custom Attribute Names
eclarations of custom att	ribute names and these attributes are enforced in An	yConnect group policy and AnyConnect dynamic access polic
🕈 Add 🗹 Edit 📋 Delete		
ype Name Values		
	Croate Custom Attribute N	2770
	Cleate Custom Attribute N	ane
Type:	ManagementTunnelAllAllowed	ᅌ Manage
Name:	true	
	Value	bbA
		Edit
		Delete
Configure Value	s:	
	Help Cancel	ОК

Étape 5. Définissez la valeur surtrue. Cliquez surok, comme illustré dans l'image.

	Management l'unnel	AllAllowed	\$	Manage
Name:	true			
	Value		Add	
			e tra	
•		Add Value		
true				
lue:				

Étape 6. Accédez à Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Sélectionnez la stratégie de groupe. Cliquez sur Edit , comme illustré dans l'image.

1) Home 🔩 Configuration 📴 Monitoring 🔓	Save 🔇 Refresh 🔇 Back 🔘 Fo	rward 💡 Help Type topic Go)		cisco
	O O Remote Access VPN	CONTINUE Configuration > Remote A	ccess VPN > Network (Client) /	Access > Group Policies		
Introduction Introduction Introduction Introduction AryConnett Connection Profiles SynConnett Customization/Localization GaryConnett Client Profile GaryConnett Client Software By Concent Client Software		Manage VPN group policies.A VPN server. The group policy informati To enforce authorization attribute Add C Edit Delete	group is a collection of user-or on is referenced by VPN connect s from an LDAP server you must Assign	iented authorization attribute/value pairs that ma ion profiles and user accounts. use an LDAP attribute map.	y be stored internally on the device or externally on a RADIUS	/LDAP
sk	Dynamic Access Policies	Name	Туре	Tunneling Protocol	Assigned To	
8	Group Policies	AnyConnect	Internal	ssl-client	AnyConnect	
	Psec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGr	oup;Def
	IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
	Address Assignment Address Assignment Address Assignment Address Assignment AnyConnect Essentials AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attribute Names Address St. VPN Access Address St. VPN Access Address St. VPN Access Address St. VPN Access Address Add					
	Bevice Setup					
	🕄 Firewall					
	Kemote Access VPN					
	Site-to-Site VPN	Find:	O O Match Case			
	Device Management			Reset Apply		

Étape 7. Comme le montre cette image, accédez àAdvanced > Split Tunneling. Configurez la stratégie en tant queTunnel All Networks.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network fields.	i:
▼ Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	DNS Names: Inherit Inherit Yes No Policy: Inherit Tunnel All Networks S IPv6 Policy: Inherit Inherit Tunnel All Networks I Network List: Inherit Inher	
Find:	Next O Previous	
	Help Cancel OK	

Étape 8. Accédez à Advanced > Anyconnect Client > Custom Attributes. Cliquez surAdd, comme illustré dans

l'image.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel
General Servers V Advanced Split Tunneling Browser Proxy AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes IPsec(IKEv1) Client	Configuration of custom policy attributes. Image: Configuration of custom policy attributes. Type Name of Value
Find:	Next Previous
	Help Cancel OK

Étape 9. Sélectionnez le type d'attribut_{ManagementTunnelAllAllowed} et sélectionnez Valeur true. Cliquez OKSUR, comme illustré dans l'image.

Name of Value	
Name of Value	
Create Custom Attribute	
Management lunnel All Allowed	age
ue	
true 🕥 Mana	age
Help Cancel OK	
L	Create Custom Attribute ManagementTunnelAllAllowed I I I I I I I I I I I I I I I I I I I

Étape 10. Cliquez sur_{Apply}pour transmettre la configuration à l'ASA, comme illustré dans l'image.



Configuration CLI après l'ajout de l'attribut personnalisé Management Tunnel All Allowed:

<#root>

webvpn

```
enable outside
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
I
anyconnect-custom-data ManagementTunnelAllAllowed true true
I
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
```

vpn-tunnel-protocol ikev2 ssl-client

```
split-tunnel-policy tunnelall
client-bypass-protocol enable
address-pools value VPN_Pool
anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Vérifier

Vérifiez la connexion du tunnel VPN de gestion sur l'interface de ligne de commande ASA avec lashow vpn-sessiondb detail anyconnect commande.

```
<#root>
ASA#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username
           :
vpnuser
               Index
                           : 10
Assigned IP :
192.168.10.1
Public IP : 10.65.84.175
Protocol
            :
AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License
            : AnyConnect Premium
Encryption
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
            : 17238
                                                 : 1988
Bytes Tx
                                     Bytes Rx
            : 12
                                     Pkts Rx
                                                  : 13
Pkts Tx
Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
Duration
            : 0h:11m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                     VLAN
                                                  : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
DTLS-Tunnel:
  Tunnel ID : 10.3

        Assigned IP
        : 192.168.10.1
        Public IP
        : 10.65.84.175

        Encryption
        : AES-GCM-256
        Hashing
        : SHA384

  Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2
                                               UDP Src Port : 57053
  UDP Dst Port : 443
Auth Mode : Certificate
  Idle Time Out: 30 Minutes
                                    Idle TO Left : 18 Minutes
  Client OS : Windows
  Client Type : DTLS VPN Client
  Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036
  Bytes Tx : 17238
Pkts Tx : 12
                                                     Bytes Rx : 1988
Pkts Rx : 13
  Pkts Tx Drop : 0
                                                     Pkts Rx Drop : 0
```

--- Output Omitted ---

Vérifiez la connexion du tunnel VPN de gestion sur ASDM.

Accédez à Monitoring > VPN > VPN Statistics > Sessions. Filter By AnyConnect Client pour afficher la session client.

ổ Home 🦓 Configuration [M	onitoring 📊 Save (🔇 Refresh 🔇 Ba	ck 🔘 Forward 🖁	Help Type topic Go				cisco
Device List Bookmarks	OOO Monitoring	> VPN > VPN Stati	stics > Sessions					
O O O Device List								
🕈 Add 📋 Delete 🚿 Connect	Туре	Active		Cumulative	Peak Concurrent	Inact	ive	
Find: Go	AnyConnect Client		1		19	1		0
A 10.106.39.196	SSL/TLS/DTLS		1		19	1		0
A 10.106.64.230								
10.197.227.47								
10.106.51.99:444								
OOO VPN								
VPN Statistics	Filter By AnyCo	nnect Client	🔾 All S	Sessions ᅌ	Filter			
VPN Cluster Loads	Username	Group Policy Connection Profile	Assigned IP Address	Protocol	Login Time Duration	Bytes Tx Inactivity	Audit !	Details
Crypto Statistics	vpnuser	AnyConnect_MGMT.	192.168.10.1	AnyConnect-Parent	10:52:25 UTC	34688 0h:00m:00s	c0a80	
Compression Statistics		AnyConnect_MGMT.	10.65.84.175	AnyConnect-Parent: (1))none 0h:01m:31s	33954		Logout
Clobal IKE //Broc Statistics	L							Ding
								Fing
VLAN Mapping Sessions								
Clientless SSL VPN								
Shared SSL VPN								
VPN Connection Graphs								
SA Sessions								
Interfaces								
C ^A , VPN								
	To sort VPN session	ns, right-click on th	e above table and	elect Table Sort Order fr	om popup menu.			
Routing								
Sa Properties	Logout By: A	an Sessio 🖸		Logout Sessions				

Vérification de la connexion du tunnel VPN de gestion sur l'ordinateur client :

Scisco AnyConnect Secure Mobility Client		- 🗆 X	
cisco AnyCon	nect Secure Mobility Cli	ent	
Virtual Private Network (VPN)		Diagnostics	
Preferences Statistics Route Details Firewall Message History			
Connection Information	Disconnected	· ^	
Tunnel Mode (IPv4):	Not Available	Sisco AnyConnect Secure Mobility Client –	×
Tunnel Mode (IPv6): Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available Not Available 00:00:00 None Connected (asa.example.com)	VPN: Ready to connect.	nect
Address Information		-	
Client (IPv4): Client (IPv6):	Not Available Not Available	\$ ()	alialia cisco
Bytes		~ •	
	Reset	t Export Stats	

Dépannage

La nouvelle ligne UI Statistics (Management Connection State) peut être utilisée pour résoudre les problèmes de connectivité du tunnel de gestion. Voici les états d'erreur courants :

Déconnecté (désactivé) :

- La fonctionnalité est désactivée.
- Assurez-vous que le profil VPN de gestion a été déployé sur le client, via une connexion de tunnel utilisateur (nécessite que vous ajoutiez le profil VPN de gestion à la stratégie de groupe de tunnels utilisateur) ou hors bande par le biais du téléchargement manuel du profil.
- Assurez-vous que le profil VPN de gestion est configuré avec une seule entrée d'hôte qui inclut un groupe de tunnels.

Déconnecté (réseau approuvé) :

• TND a détecté un réseau approuvé et le tunnel de gestion n'est donc pas établi.

Déconnecté (tunnel utilisateur actif) :

• Un tunnel VPN utilisateur est actuellement actif.

Déconnecté (échec du lancement du processus) :

• Une erreur de lancement de processus a été rencontrée lors de la tentative de connexion au tunnel de gestion.

Déconnecté (échec de la connexion) :

- Une défaillance de connexion s'est produite lors de l'établissement du tunnel de gestion.
- Assurez-vous que l'authentification du certificat est configurée dans le groupe de tunnels, qu'aucune bannière n'est présente dans la stratégie de groupe et que le certificat du serveur doit être approuvé.

Déconnecté (configuration VPN non valide) :

- Une configuration de tunnel partagé ou de protocole de contournement de client non valide a été reçue du serveur VPN.
- Vérifiez votre configuration dans la politique de groupe de tunnels de gestion par rapport à la documentation.

Déconnecté (mise à jour logicielle en attente) :

• Une mise à jour du logiciel AnyConnect est actuellement en attente.

Déconnecté :

• Le tunnel de gestion est sur le point d'être établi ou ne peut pas l'être pour une autre raison.

Collectez le DART pour un dépannage plus approfondi.

Informations connexes

- <u>Configuration du tunnel VPN de gestion</u>
- Dépannage du tunnel VPN de gestion
- <u>Assistance et documentation techniques Cisco Systems</u>

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.