Beheerde AnyConnect VPN-tunnel op ASA configureren

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Werken met beheertunnels Beperkingen Configureren Configuratie op ASA via ASDM/CLI VPN-profiel voor AnyConnect-beheer maken Implementatiemethoden voor AnyConnect Management VPN-profiel (Optioneel) Configureer een aangepast kenmerk om de configuratie van alle tunnels te ondersteunen Verifiëren Problemen oplossen Gerelateerde informatie Inleiding

Dit document beschrijft hoe u een ASA kunt configureren als de VPN-gateway verbindingen accepteert vanuit de Cisco AnyConnect Secure Mobility Client via de VPN-tunnel voor beheer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- VPN-configuratie via Adaptieve Security Device Manager (ASDM)
- CLI-configuratie voor basis adaptieve security applicatie (ASA)
- X509-certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA softwareversie 9.12(3)9
- Cisco ASDM-softwareversie 7.12.2
- Windows 10 met Cisco AnyConnect Secure Mobility-clientversie 4.8.03036

Opmerking: download het AnyConnect VPN-webimplementatiepakket (anyconnect-win*.pkg or anyconnect-macos*.pkg) vanuit de Cisco <u>Software Download</u> (alleen geregistreerde klanten). Kopieer de AnyConnect VPN-client naar het flitsgeheugen van de ASA dat moet worden gedownload naar de externe gebruikerscomputers om de SSL VPN-verbinding met de ASA tot stand te brengen. Raadpleeg <u>het</u> gedeelte <u>AnyConnect-client installeren</u> in de ASA-configuratiehandleiding voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een VPN-tunnel voor beheer zorgt voor verbinding met het bedrijfsnetwerk wanneer het clientsysteem is ingeschakeld, niet alleen wanneer een VPN-verbinding tot stand is gebracht door de eindgebruiker. U kunt patchbeheer uitvoeren op out-of-the-office endpoints, met name apparaten die niet vaak door de gebruiker, via VPN, worden verbonden met het kantoornetwerk. Endpoint OS login scripts die zakelijke netwerkconnectiviteit vereisen, profiteren ook van deze functie.

AnyConnect Management Tunnel stelt beheerders in staat om AnyConnect verbonden te hebben zonder tussenkomst van de gebruiker voordat de gebruiker zich aanmeldt. AnyConnectbeheertunnel kan werken in combinatie met Trusted Network Detection en wordt daarom alleen geactiveerd wanneer het eindpunt niet op de locatie beschikbaar is en is losgekoppeld van een door de gebruiker geïnitieerde VPN. AnyConnect-beheertunnel is transparant voor de eindgebruiker en wordt automatisch losgekoppeld wanneer de gebruiker VPN initieert.

Besturingssysteem/toepassing

ASA ASDM Windows AnyConnect versie MacOS AnyConnect versie Linux

Minimale versievereisten

9.0.1 7.10.1 4.7.00136 4.7.01076 Niet ondersteund

Werken met beheertunnels

De AnyConnect VPN-agentservice wordt automatisch gestart nadat het systeem is opgestart. Het detecteert dat de beheerstunnelfunctie is ingeschakeld (via het VPN-profiel voor beheer) en start daarom de beheerclienttoepassing om een beheertunnelverbinding te starten. De toepassing van de beheersclient gebruikt de hostingang van het VPN-beheerprofiel om de verbinding te starten. Dan is de VPN-tunnel zoals gebruikelijk, met één uitzondering: er wordt geen software-update uitgevoerd tijdens een beheertunnelverbinding, omdat de beheerstunnel bedoeld is om transparant te zijn voor de gebruiker.

De gebruiker initieert een VPN-tunnel via de AnyConnect UI, die de beëindiging van de beheerstunnel activeert. Op de beëindiging van de beheerstunnel, gaat de inrichting van de gebruikerstunnel verder zoals gebruikelijk.

De gebruiker verbreekt de VPN-tunnel, waardoor de beheerstunnel automatisch wordt hersteld.

Beperkingen

- · Gebruikersinteractie wordt niet ondersteund
- Op certificaat gebaseerde verificatie via het machinecertificaat Store (Windows) wordt alleen
 ondersteund
- Er wordt strikte controle van servercertificaten uitgevoerd
- Een particuliere proxy wordt niet ondersteund
- Een openbare proxy wordt niet ondersteund (ProxyNative waarde wordt ondersteund op platforms waar Native Proxy-instellingen niet worden opgehaald van de browser)
- AnyConnect-aanpassingsscripts worden niet ondersteund

Opmerking: Raadpleeg Info over de VPN-tunnelleiding voor beheer voor meer informatie.

Configureren

In deze sectie wordt beschreven hoe u Cisco ASA kunt configureren als de VPN-gateway voor het accepteren van verbindingen van AnyConnect-clients via de VPN-tunnel voor beheer.

Configuratie op ASA via ASDM/CLI

Stap 1. Maak het AnyConnect-groepsbeleid. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Klik Add.

Opmerking: het is aan te raden om een nieuw AnyConnect-groepsbeleid te maken dat alleen voor de AnyConnect-beheerstunnel wordt gebruikt.



Stap 2. Een Name voor het groepsbeleid. Een bestand toewijzen/maken Address Pool.

Kiezen Tunneling Protocols als SSL VPN Client en/of IPsec IKEv2, zoals aangegeven in de afbeelding.

SCEP forwarding URL: SCEP forwarding URL: Inherit Address Pools: Inherit VPN_Pool IPv6 Address Pools: Inherit Clientless SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec Filter: C Inherit Clientless SSL VPN Client IPsec IKEv2 L2TP/IPsec Filter: C Inherit Clientless SSL VPN Client IPsec IKEv2 L2TP/IPsec Filter: C Inherit Clientless SSL VPN Client IPsec IKEv2 L2TP/IPsec Filter: C Inherit Clientless SSL VPN Client IPsec IKEv2 L2TP/IPsec Filter: C Inherit Clienters Simultaneous Logins: C Inherit Restrict access to VLAN: Connection Profile (Tunnel Group) Lock: Inherit Unlimited minutes Ide Timeout: Venter Inherit None (2 - 65519) On smart card removal: Inherit Disconnect Keep the connection	
ScLer forwarding Okc. Inherit Address Pools: Inherit IPv6 Address Pools: Inherit More Options Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv2 L2TP/IPsec Filter: Inherit Cinneting Protocols: Inherit Connection Profile (Tunnel Group) Lock: Inherit Inherit Unlimited Maximum Connect Time: Inherit Ide Timeout: Inherit None (2 - 65519) On smart card removal: Inherit	
Nutress Pools: IPv6 Address Pools: Inherit More Options Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv2 L2TP/IPsec Filter: Inherit Consection Profile (Tunnel Group) Lock: Inherit Inherit Maximum Connect Time: Inherit Inherit None Idle Timeout: Security Group Tag (SGT): Inherit Disconnect Keep the connection	Select
More Options Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec Filter: Inherit Inherit Inherit Imsec IKEv1 IPsec IKEv2 L2TP/IPsec Simultaneous Logins: Inherit Imsec IKEv1 Imsec IKEv2 L2TP/IPsec Simultaneous Logins: Inherit Imsec IKEv1 Imsec IKEv2 Imsec IKEv2 Imsec IKEv2 Connection Profile (Tunnel Group) Lock: Inherit Imsec IKEv2 Imsec IKEv2 Imsec IKEv2 Imsec IKEv2 Idle Timeout: Inherit Inherit Imsec IKEv2 Imsec IKEv2 </th <th>Select</th>	Select
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec Filter: Inherit Inherit Inherit Inherit Imperit Imperit Imperit Access Hours: Inherit Inherit Imperit Imperit Imperit Imperit Imperit Simultaneous Logins: Inherit Inherit Imperit Imperit Imperit Imperit Imperit Connection Profile (Tunnel Group) Lock: Inherit Imperit Imperit Imperit Imperit Imperit Maximum Connect Time: Inherit Inherit Inherit Imperit Imperit Imperit Imperit Idle Timeout: Inherit Inherit None Imperit Imperit Imperit Imperit Security Group Tag (SGT): Inherit Inherit Inherit Imperit Imperit Imperit On smart card removal: Imperit Disconnect Keep the connection Imperit	
Filter: Inherit Inherit Inherit Access Hours: Inherit Inherit Inherit Simultaneous Logins: Inherit Inherit Inherit Restrict access to VLAN: Inherit Inherit Inherit Connection Profile (Tunnel Group) Lock: Inherit Inherit Inherit Maximum Connect Time: Inherit Unlimited Inherit Idle Timeout: Inherit None Inherit Security Group Tag (SGT): Inherit None (2 - 65519) On smart card removal: Inherit Disconnect Keep the connection	
Access Hours: Inherit Simultaneous Logins: Inherit Restrict access to VLAN: Inherit Connection Profile (Tunnel Group) Lock: Inherit Maximum Connect Time: Inherit Idle Timeout: Inherit Security Group Tag (SGT): Inherit Inherit None Inherit None Inherit Inherit	Manage
* Simultaneous Logins: Inherit Restrict access to VLAN: Inherit Connection Profile (Tunnel Group) Lock: Inherit Maximum Connect Time: Inherit Idle Timeout: Inherit Security Group Tag (SGT): Inherit Inherit None On smart card removal: Inherit	Manage
Restrict access to VLAN: Inherit <	
Connection Profile (Tunnel Group) Lock: Inherit Inherit Inherit Maximum Connect Time: Inherit Unlimited minutes Idle Timeout: Inherit None minutes Security Group Tag (SGT): Inherit None (2 – 65519) On smart card removal: Inherit Disconnect Keep the connection	
Maximum Connect Time: Inherit Unlimited minutes Idle Timeout: Inherit None minutes Security Group Tag (SGT): Inherit None (2 – 65519) On smart card removal: Inherit Disconnect Keep the connection	
Idle Timeout: Inherit None minutes Security Group Tag (SGT): Inherit None (2 - 65519) On smart card removal: Inherit Disconnect Keep the connection	
Security Group Tag (SGT): Inherit None (2 - 65519) On smart card removal: Inherit Disconnect Keep the connection	
Security Group Tag (SGT): Inherit None (2 - 65519) On smart card removal: Inherit Disconnect Keep the connection	
On smart card removal:	
Timeout Alerts	
Maximum Connect Time Alert Interval: 🗹 Inherit 🔹 Default minutes	
Periodic Certificate Authentication Interval: 🗹 Inherit 🗌 Unlimited hours	
Find: O Next O Previous	

Stap 3. Naar navigeren Advanced > Split Tunneling. Configureer de Policy als Tunnel Network List Below en kies de Network List, zoals aangegeven in de afbeelding.

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

Opmerking: Als een clientadres niet voor beide IP-protocollen (IPv4 en IPv6) wordt ingedrukt, wordt het Client Bypass Protocol instelling moet enabled zodat het overeenkomstige verkeer niet door de beheerstunnel wordt verstoord. Raadpleeg voor het configureren stap 4.

Stap 4. Naar navigeren Advanced > AnyConnect Client. instellen Client Bypass Protocol in Enable. Klik OK om op te slaan, zoals in de afbeelding.

• •		Add Internal Group Policy	
General	Keep Installer on Client System:	☑ Inherit O Yes O No	٦
Servers Advanced	Datagram Transport Layer Security (DTLS):	✓ Inherit ○ Enable ○ Disable	
Split Tunneling	DTLS Compression:	🗹 Inherit 🔷 Enable 🔷 Disable	
Browser Proxy	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 오 Enable 🔿 Disable	
	FQDN of This Device:	V FQDN	
	MTU:	🗹 Inherit	
	Keepalive Messages:	☑ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	🛛 Inherit 🗘	
0	Always-On VPN:	☑ Inherit O Isable O Use AnyConnect Profile setting 0	
	Client Profiles to Download:	🗹 Inherit	
		🛧 Add 📋 Delete	
		Profile Name Profile Usage/Type	
			1
			4
Find:	💿 Next 🔘	Previous	
		Help Cancel OK	

Stap 5. Zoals in deze afbeelding, klikt u op Apply om de configuratie naar de ASA te duwen.

🔥 Home 🍫 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	rard ? Help Type topic Go		cisco
000 Remote Access VPN	Configuration > Remote Acc	cess VPN > Network (Client) Acces	s > Group Policies	
Pintroduction Pintro	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes Add C C Edit Delete 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 <u>LDAP attribute map</u> .	ternally on the device or externally on a RADIUS/LDAP server. The group
E Dynamic Access Policies	Name	Type	Tuppeling Protocol	Connection Profiles/Users
Group Policies	An Connect	- ppe	cel elione	Assigned To
IPsec(IKEv1) Connection Profiles	DftCroPolicy (System Default)	Internal	ikev1:ikev2:l2tn=inser	DefaultRACroup: Defaulti 21 Croup: DefaultADMINCroup: DefaultWE
IPsec(IKEv2) Connection Profiles	AnyConnect MGMT_Tunnel	Internal	ikev2:ssl-client	AnyConnect MGMT Tunnel
Secure Mobility Solution				
Address Assignment				
Advanced				
Clientless SSL VPN Access				
AAA/Local Users				
Ma AAA Server Groups				
Mar LDAP Attribute Map				
B Gorean Declare Manager				
Gattificate Manager				
Certificate Management				
Se Load Balancing				
A DNS				
Advanced				
Device Setup				
Eirewall				
Remote Access VPN				
Site-to-Site VPN	Find:	Match Case		
Device Management				
			Reset Apply	
•				

CLI-configuratie voor groepsbeleid:

```
! 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
```

Stap 6. Maak het AnyConnect-verbindingsprofiel. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Klik Add.

Opmerking: aanbevolen wordt om een nieuw AnyConnect-verbindingsprofiel te maken dat alleen voor de AnyConnect-beheertunnel wordt gebruikt.



Stap 7. Een Name voor het verbindingsprofiel en instellen Authentication Method als Certificate only. Kies de Group Policy als degene die in <u>Stap 1</u> is gemaakt.

Basic	Name:	AnyConnect_MGMT_Tunnel		
Advanced	Aliases:			
	Authentication			
	Method:	Certificate only		
	AAA Server Group:	LOCAL	0	Manage
		Use LOCAL if Server Group fails		
	SAML Identity Provider			
	SAML Server :	None	0	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	٥	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:			
Finals		Next Previous		

Opmerking: Zorg ervoor dat het basiscertificaat van Local CA op de ASA aanwezig is. Naar navigeren Configuration > Remote Access VPN > Certificate Management > CA Certificates om het certificaat toe te voegen/weer te geven.

Opmerking: zorg ervoor dat een door dezelfde lokale certificeringsinstantie afgegeven identiteitsbewijs bestaat in de machinecertificaatwinkel (voor Windows) en/of in de systeemsleutelhanger (voor macOS).

Stap 8. Naar navigeren Advanced > Group Alias/Group URL. Klik Add onder Group URLs en voeg een URL. verzekeren Enabled wordt gecontroleerd. Klik OK om op te slaan, zoals in de afbeelding.

Add AnyConnect Connection Profile

 Enable the display of Securid 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 Delete (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 Add Group URL URL: https://asa.example.com/AnyConnect_MGMT_Tunnel @ Enabled Help Cancel OK

Als IKEv2 wordt gebruikt, zorg dan voor IPsec (IKEv2) Access is ingeschakeld op de interface die wordt gebruikt voor AnyConnect.

O O Remote Access VPN	Config	uration > Remot	e Access VPN > I	Network (Client) A	Access > AnyConnect Co	onnection Profiles
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	appliance automa orts IPsec (IKEv2) to	tically deploys the unnel as well as S	e Cisco AnyConnec SL tunnel with Data	ct VPN Client to remote u agram Transport Layer Se	sers upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN curity (DTLS) tunneling options.
AnyConnect Customization/Local	Enable C	ces Cisco AnyConnect	VPN Client access	on the interfaces	selected in the table belo	w
AnyConnect Client Software Population Access Policies	SSL access r	nust be enabled if	you allow AnyCor	nect client to be li	aunched from a browser (Web Launch) .
Group Policies Psec(IKEv1) Connection Profiles	Interface	Allow Access	Enable DTLS	IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate
IPsec(IKEv2) Connection Profiles Secure Mobility Solution Address Assignment	inside			L ő		Port Settings

Stap 9. Klik Apply om de configuratie naar de ASA te duwen.



CLI-configuratie voor verbindingsprofiel (tunnelgroep):

```
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
```

Stap 10. Zorg ervoor dat een betrouwbaar certificaat is geïnstalleerd op de ASA en is gebonden aan de interface die wordt gebruikt voor AnyConnect-verbindingen. Naar navigeren Configuration > Remote Access VPN > Advanced > SSL Settings om deze instelling toe te voegen/weer te geven.

Opmerking: Raadpleeg Installatie van identiteitsbewijs op ASA.

Remote Access VPN	○ ○ ○ Configuration > Remote Acces	s VPN > Advanced > SSL Settings				
Introduction	r					
Network (Client) Access	Configure SSL parameters. These para	meters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization AnyConnect Client Profile	The minimum SSL version for the second	urity appliance to negotiate as a "server":	TLS V1	0	O DTLSV1 O DTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the second	urity appliance to negotiate as a "client":	TLS V1	0		
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	Encryption					
Sp Address Assignment	cheryption				10.00.001	
Advanced	Cipher version	Cipher Security Level		Cipher Algorithm	s/ custom string	Edit
Clientless SSL VPN Access	Default	Medium		DES-CBC3-SHA	AES128-SHA DHE-KSA-AES128-SHA AES256-SHA DHE-KSA	
AAA/Local Users	TLSV1	Medium		DHE-RSA-AESZS	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
AAA Server Grouns	TLSV1.1	Medium		DHE-RSA-AESZ	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
Se LDAR Ancibude Man	TLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
	DTLSV1	Medium		DHE-RSA-AES2	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
I Local Users	DTLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-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						
Connection Gateway						Edit
Reference Identity						Delete
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Certificates					
	Specify which contificator if any of	ould be used for SSL authentication on ea	ch interface. The fallback contificate u	uill be used on interfs	car not prescipted with a cartificate of their own	
	specify which certificates, if any, si	iouid be used for SSL authentication on ea	ich interface. The fanback certificate v	vill be used on interra	ces not associated with a certificate of their own.	
under Cature	Interface	Primary Certificate	Load Balancing Certificate		Key-Type	Edit
evice Setup	inside					
innuall	management					
ineman.	outside	ROOT-CA:hostname=ASA.example	.co		Primary: RSA (2048 bits), Load Balancing: none	
emote Access VPN						
ite-to-Site VPN						
Device Management						
			(Charles) (Charles			

CLI-configuratie voor SSL Trustpoint:

ssl trust-point ROOT-CA outside

VPN-profiel voor AnyConnect-beheer maken

Stap 1. Maak het AnyConnect-clientprofiel. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Klik Add, zoals aangegeven in de afbeelding.

	Home 🔏 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 Back 🌘	Forward 💡 Help Type topic Go			cisco
	O O Remote Access VPN	○ ○ ○ Configuration > Remote Ac	cess VPN > Network (Client) Access > AnyCon	nect Client Profile		
Bookmarks	Introduction I	This panel is used to manage AnyC button to add a new profile. Pressin The profile Usage field is introduce HostScan configuration can be perf	onnect Client Profiles and perform group assignm ig the Import or Export button is for upload and d d with the Secure Mobility Solution. This field con ormed by going to Secure Desktop Manager/Host Policy Delete I import & Export A Validate	ent for AnyConnect version 2.5 or later.You can select ownload of client profiles between local machine and tains different profile usage in AnyConnect version 3. Scan. If 'HostScan' is not visible under 'Secure Desktop	a profile to edit, change group or to delete. You can select the 'Add' device.) and later. Manager', you will need to restart ASDM.	
	Psec(IKEv1) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	PsectitKEv2 Connection Profil Secure Mobility Solution Secure Mobility Solution Madress Assignment Badvanced Address Assignment Madress SSL VPM Access Address SSL VPM Access Add/Local Users Address SSL VPM Access Add/Local Users Address Could Users Contal Users Could Users Could Users Ded Salancing DHCP Server DHCP Server DHCP Server DHS Secure Connection Gateway Advanced Secure					
	Certificate to AnyConnect and HTTP Redirect Maximum VPN Sessions Crypto Engine					
	<u>D</u> evice Setup Firewall <u>Remote Access VPN</u>					
	Site-to-Site VPN			Recet Anniu		
	*			Reset Apply		

Stap 2. Een Profile Name. Kies de Profile Usage als AnyConnect Management VPN profile. Kies de Group Policy gemaakt in <u>Stap 1</u>. Klik OK , zoals aangegeven in de afbeelding.

Name		Profile Usage	Group Policy		Profile Location
	• • •	Add AnyConnect Clier	nt Profile		
	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 fi s not exist.	ile will be automatically		
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Bro	wse Flash	
				Jpload	
	Group Policy	AnyConnect_MGMT_Tunnel	0		
	_	Enable 'Always On VPN' for selected group			
		Help Cancel	ОК		
			Reset Apply		

Stap 3. Kies het profiel dat u hebt gemaakt en klik op Edit, zoals aangegeven in de afbeelding.

Name	Profile Usage	Group Policy	Profile Location
nnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

Stap 4. Naar navigeren Server List. Klik Add om een nieuwe serverlijst toe te voegen, zoals in de afbeelding wordt getoond.

	(
Preferences (Part 1)	Server List				
Preferences (Part 2)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Matching					
Server List					
					_
	Note: at most o	one server can be define	d in a management VP	N profile. Add	Delete
				Edit	Details

Stap 5. Een Display Name. Voeg het FQDN/IP address van de ASA. Geef de User Group als naam van de tunnelgroep. Group URL wordt automatisch ingevuld met de FQDN en User Group. Klik OK.

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 KE Identity (IOS gateway only)
Backup Servers	
Host Address	Add
	Move Up Move Down
	Delete
ОК	Cancel

Opmerking: de FQDN/IP-adres + gebruikersgroep moet gelijk zijn aan de URL van de groep die wordt vermeld tijdens de configuratie van het AnyConnect-verbindingsprofiel in <u>stap 8</u>.

Opmerking: AnyConnect met IKEv2 als protocol kan ook worden gebruikt om Management VPN naar ASA te implementeren. verzekeren Primary Protocol is ingesteld op IPsec in <u>stap 5</u>.

Stap 6. Zoals in de afbeelding, klikt u op ок Opslaan.

8 🔵 🖶	AnyC	onnect Client Profile Edit	or - AnyConnect_MGM1	_Profile	
Profile: AnyConnect_MC	GMT_Profile				Abou
VPN Preferences (Part 1) Preferences (Part 2)	Server List				
Backup Servers	Hestname	Heat Address	llear Crown	Paslue Conver List	Costificato Ding
Certificate Pinning	AnyConnect MGMT	T asa.example.com	AnyConnect MGMT	F Inherited	Certificate Pins
Certificate Matching					
	Note: at most on	e server can be defined	in a management VPN	profile. Add	Delete
				Edit	Details
	•				
		Help	ncel OK		

Stap 7. Klik Apply tOm de configuratie naar de ASA te duwen, zoals in de afbeelding.

	Home 🔩 Configuration 📴 Monito	ring 🔚 Save 🔇 Refresh 🔇 Back 🔘 F	forward 💡 Help Type topic Go			cisco
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote Access	s VPN > Network (Client) Access > AnyConnect Client	ent Profile		
Bookmarks	Introduction Imroduction Imroduc	This panel is used to manage AnyConn button to add a new profile. Pressing th The profile Usage field is introduced wi HostScan configuration can be perform	ect Client Profiles and perform group assignment for le Import or Export button is for upload and download th the Secure Mobility Solution. This field contains di ed by going to Secure Desktop Manager/HostScan. If () Delete Jimport Secure Desktop Manager/HostScan.	AnyConnect version 2.5 or later.You can select a pro d of client profiles between local machine and device (ferent profile usage in AnyConnect version 3.0 and 'HostScan' is not visible under 'Secure Desktop Man	lie to edit, change group or to delete. You can select the 'Add' ater. ger', you will need to restart ASDM.	
	IPsec(IKEv1) Connection Profil	Profile Name	Profile Usane	Group Policy	Profile Location	
	 IPsec(IKEv2) Connection Profil Secure Mobility Solution Address Assignment 	AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm	
	► Solution Advanced Controls SSL VPA Access Advanced Advanced Advanced Advanced Advanced Advanced Control Users Decometion Cateway SSL Settings Reference Identity Controls Access					
	The HTTP Redirect The Redirect Crypto Engine Crypto Engine Crypto Engine Crypto Esclup Crypto Setup Crypto					
	Remote Access VPN					
	*			Reset Apply		

CLI-configuratie na toevoeging van AnyConnect Management VPN-profiel.

```
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
1
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
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

AnyConnect Management VPN-profiel op AnyConnect-clientmachine:

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

<ShowPreConnectMessage>false</ShowPreConnectMessage>

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

--- Output Omitted ---

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

Opmerking: als Trusted Network Detection (TND) wordt gebruikt in het VPN-profiel van AnyConnect, is het raadzaam dezelfde instellingen in het VPN-profiel voor beheer aan te passen voor een consistente gebruikerservaring. De VPN-tunnel voor beheer wordt geactiveerd op basis van de TND-instellingen die zijn toegepast op het tunnelprofiel van de gebruiker VPN. Bovendien is de TND Connect-actie in het VPN-beheerprofiel (alleen afgedwongen wanneer de VPN-tunnel voor beheernetwerken actief is) altijd van toepassing op de VPN-tunnel van de gebruiker om ervoor te zorgen dat de VPN-tunnel voor beheernetwerken transparant is voor de eindgebruiker.

Opmerking: op elke eindgebruiker-pc, als de TND-instellingen in het VPN-profiel voor beheer zijn ingeschakeld en als het VPN-profiel van de gebruiker ontbreekt, worden de standaardinstellingen voor de TND (het is uitgeschakeld op de standaardvoorkeuren in de AC-clienttoepassing) in plaats van het ontbrekende VPN-profiel van de gebruiker bekeken. Deze mismatch kan leiden tot onverwacht/niet gedefinieerd gedrag.

In de standaardinstellingen worden de TND-instellingen standaard uitgeschakeld. Om de standaardvoorkeuren voor hardgecodeerde instellingen in de AnyConnectclienttoepassing te overwinnen, moet de eindgebruiker-pc twee VPN-profielen hebben, een VPN-profiel voor gebruikers en een VPN-profiel voor AC Management, en moeten beide dezelfde TND-instellingen hebben.

De logica achter de VPN-tunnelverbinding en ontkoppeling van het beheer is dat om een VPN-tunnel voor het beheer tot stand te brengen, de AC-agent de TND-instellingen van het VPN-profiel van de gebruiker gebruikt en voor het ontkoppelen van de VPN-tunnel voor het beheer controleert op TND-instellingen voor het VPN-profiel van het beheer.

Implementatiemethoden voor AnyConnect Management VPN-profiel

• Een succesvolle VPN-verbinding van de gebruiker is voltooid met het ASA-verbindingsprofiel om het AnyConnect Management VPN-profiel te downloaden van de VPN-gateway.

Opmerking: als het protocol voor de VPN-tunnel voor beheer IKEv2 is, moet de eerste verbinding tot stand worden gebracht via SSL (om het AnyConnect Management VPN-profiel van de ASA te downloaden).

• Het AnyConnect Management VPN-profiel kan handmatig naar de clientmachines worden geüpload via een GPO-push of via een handmatige installatie (Controleer of de naam van het profiel juist is VpnMgmtTunProfile.xml).

Locatie van map waarin het profiel moet worden toegevoegd: Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun macOS: /opt/cisco/anyconnect/profile/mgmttun/

(Optioneel) Configureer een aangepast kenmerk om de configuratie van alle tunnels te ondersteunen

Een VPN-tunnel voor beheer vereist standaard een splitsing die tunnelconfiguratie omvat om gevolgen voor de door de gebruiker geïnitieerde netwerkcommunicatie te voorkomen. Dit kan worden overschreven wanneer u het aangepaste kenmerk configureert in het groepsbeleid dat

wordt gebruikt door de beheertunnelverbinding.

Stap 1. Naar navigerenConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Klik Add, zoals aangegeven in de afbeelding.

1	Home 🖧 Configuration [Monitoring	🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help Type topic Go	cisco
	O O O Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes	
E I	2 Introduction	Declarations of custom attribute types and these attributes are enforced in Am/Connect group policy. Am/Connect dynamic access policy and Am/Connect custom attribute names	
š	Network (Client) Access	become don't extern activates are enored in any connect group pones, any connect group pones, and enored any any connect cortained external activates are enored in any connect group pones.	
å	AnyConnect Connection Profiles		
	AnyConnect Customization/Localizati		
	AnyConnect Client Profile	Type Description	
ark	AnyConnect Client Software		
- S	Subscription of the second sec		
ĝ	Group Policies		
	IPsec(IKEv1) Connection Profiles		
	IPsec(IKEv2) Connection Profiles		
	B Secure Mobility Solution		
	Address Assignment		
	V ES Advanced		
	Anys onner Lessentials		
	AnyConnect Custom Attributes		
	b IB iProc		
	an ACI Manager		
	Clientless SSL VPN Access		
	T AAA/Local Users		
	I AAA Server Groups		
	Se LDAP Attribute Map		
	5 Local Users		
	▶ A Secure Desktop Manager		
	El Certificate Management		
	language Localization		
	See Load Balancing		
	P DHCP Server		
	JANS DNS		
	Advanced		
	_		
	Device Setup		
	Eirewall		
	Stateman .		
	Remote Access VPN		
	CA Site-to-Site VPN		
	2 2ne-to-site vrit		
	Device Management		
		Reset Apply	
	•		

Stap 2. Stel het aangepaste attribuut Type in op ManagementTunnelAllAllowed en bieden een Description. Klik OK, zoals aangegeven in de afbeelding.

	Delete	
e		Description
	• • •	Create Custom Attribute Type
	• • • Type:	Create Custom Attribute Type ManagementTunnelAllAllowed
	• • • Type:	Create Custom Attribute Type ManagementTunnelAllAllowed ManagementTunnelAllAllowed
	Type: Descriptio	Create Custom Attribute Type ManagementTunnelAlIAllowed m:
	Type: Description	Create Custom Attribute Type ManagementTunnelAllAllowed mn:

Stap 3. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Klik Add, zoals aangegeven in de afbeelding.



Stap 4. Kies het type als ManagementTunnelAllAllowed . Stel de naam in op true. Klik Addom een waarde voor eigen kenmerken te bepalen, zoals in de afbeelding.

lame Values		
	Create Custom Attribute Na	ame
Type:	ManagementTunnelAllAllowed	ᅌ Manage
Name:	true	
	Value	Add
		Edit
		Delete
Configure Value	s:	

Stap 5. Stel de waarde in op true. Klik OK, zoals aangegeven in de afbeelding.

ManagementTunnelAllAl	lowed	\$	Manage		
true	true				
Value		Add			
	Add Value				
	true Value	true Value Add Value	true Add		

Stap 6. Naar navigeren Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Kies het groepsbeleid. Klik Edit , zoals aangegeven in de afbeelding.

1	Home 🍫 Configuration 📴 Monitoring 识	Save 🔇 Refresh 🔇 Back 🚫 Fo	rward 🦻 Help Type topic (io	cisco
	CO Remote Access VPN	Configuration > Remote A	ccess VPN > Network (Client)	Access > Group Policies	
cmarks	Introduction Introduction Introduction Introduction Intervent (Collent) Access Introduction Profiles Introduction Profiles Introduction Profile AnyConnect Clustomization/Localization Intervent Profile Intervent Intervent Profile Intervent Intervent Intervent InterventInte	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-o on is referenced by VPN connec s from an LDAP server you mus Assign	riented authorization attribute/value pairs that ma tion profiles and user accounts. t use an LDAP attribute map.	y be stored internally on the device or externally on a RADIUS/LDAP
ook	Crown Policies	Name	Туре	Tunneling Protocol	Assigned To
	Psec(KEv1) Connection Profiles	AnyConnect	Internal	ssl-client	AnyConnect
-	IPsec(IKEv2) Connection Profiles	DfitGrpPolicy (System Default)	Internal	ikev1;ikev2;iZtp-ipsec	DefaultRAGroup;DefaultL2EGroup;DefaultADMINGroup;Def
	Secure Mobility Solution	[AnyConnect_MGM1_Lunnel	Internal	ikev2;ssl-client	AnyConnect_MGM1_Lunnel
	Address Assignment Address Assignment Address Assignment AnyConnect Essentials AnyConnect Custom Attributes AnyConnect C				
	Bevice Setup				
	🚺 Firewall				
	Remote Access VPN				
	Site-to-Site VPN	Find:	Match Case		
	Device Management			Reset Apply	

Stap 7. Zoals in deze afbeelding wordt getoond, navigeer naar Advanced > Split Tunneling. Het beleid configureren als Tunnel All Networks.

• •		Edit Intern	nal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	The VPN client makes split tunneling dec fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List:	Edit Interr cisions on the Inherit Inherit Inherit Inherit	mal Group Policy: AnyConnect_MGMT_Tunnel the basis of a network list that can be specified below by providing the proper parameters to 'Policy' an Yes • No Tunnel All Networks	d 'Network Lit
Find:	Pressing this button to set up split exlus Set up Split Exclusion for Web Securit Intercept DHCP Configuration Message	sion for Web S ty from Microso	Security proxies. oft Clients	
	- NEXT	- rievious	Help Carrel OK	
			help cancer on	

Stap 8. Naar navigeren Advanced > Anyconnect Client > Custom Attributes. Klik Add, zoals aangegeven in de afbeelding.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers Y Advanced Split Tunneling Browser Proxy Y AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Customization For 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	

Stap 9. Type kenmerk kiezen als ManagementTunnelAllAllowed en kies de Waarde als true. Klik OK, zoals aangegeven in de afbeelding.

	Name o	f Value
	Create Custom Attribute	
Attribute type:	ManagementTunnelAllAllowed	Manage
Omit the value		_
• Select Value:	true	Manage
		-

Stap 10. Klik Apply om de configuratie naar de ASA te duwen, zoals in de afbeelding wordt getoond.

ا 🏀	Home 🍕 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	ard 💡 Help Type topic Go			cisco
	O O Remote Access VPN	Configuration > Remote Acc	ess VPN > Network (Client) Acce	ss > Group Policies		
u Device Lis	Pintroduction AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile	Manage VPN group policies.A VPN gr policy information is referenced by To enforce authorization attributes f Add C C the C the C As	oup is a collection of user-oriente /PN connection profiles and user a from an LDAP server you must use : sign	d authorization attribute/value pairs that may be stored ir ccounts. an LDAP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The gro	ир
mark	AnyConnect Client Software	Name	Tune	Turneling Protocol	Connection Profiles/Users	_
Book	Group Policies	AmConnect	Internal	ssi-client	Assigned To AnyConnect	_
	Psec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def	aultWE
	Psec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
	 ≥ and Advanced > En Advanced > Energies SSL VPN Access > Advanced Users > Energies SSL VPN Access > Advanced Users > Energies SSL VPN Access > Energies Stever Groups > Energies Users > Secure Desktop Manager > Enginge Loalization > Enginge Loalization > Enginge Server > DNS > Advanced 					
	A Device Setup					
	🚯 Firewall					
	Remote Access VPN					
	Site-to-Site VPN	Find:	Match Case			
	Device Management			Reset		

CLI-configuratie na de ManagementTunnelAllAllowed Aangepaste eigenschap wordt toegevoegd:

```
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
1
anyconnect-custom-data ManagementTunnelAllAllowed true true
1
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
```

Verifiëren

Controleer de VPN-tunnelverbinding van beheer op ASA CLI met de show vpn-sessiondb detail anyconnect uit.

ASA# show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
```

```
Username
           : vpnuser
                                    Index
                                                : 10
                                    Public IP : 10.65.84.175
Assigned IP : 192.168.10.1
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
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
Bytes Tx
           : 17238
                                    Bytes Rx
                                               : 1988
           : 12
                                                : 13
Pkts Tx
                                    Pkts Rx
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
           : 0h:11m:36s
Duration
Inactivity : 0h:00m:00s
                                    VLAN
                                               : none
VLAN Mapping : N/A
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
--- Output Omitted ---
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 A	gent for Windows	s 4.8.03036
Bytes Tx :	17238	Bytes Rx	: 1988
Pkts Tx :	12	Pkts Rx	: 13
Pkts Tx Drop :	0	Pkts Rx Dro	op : 0

Controleer de VPN-tunnelverbinding van het beheer op ASDM.

Navigeer naar **Monitoring > VPN > VPN-statistieken > Sessies** . Filteren op **AnyConnect-client** om de clientsessie te bekijken.

									cisco
Device List Bookmarks	000 <u>Monitoring</u>	> VPN > VPN Stati	istics > <u>Sessions</u>						
Add 1 Delete & Connect	-								
	Type AnyConnect Client	Active	,	Cumulative	Peak Concurr	ent	Inactive	e	0
Go Go	SSL/TLS/DTLS		1		19		1		0
A 10.106.39.196	552,125,012								
■ 10.106.64.230 ■ 10.107.227.47									
■ 10.197.227.47 ■ 10.106.51.99.444									
VPN Statistics	Filter Pr	nnect Client	All 5	assions 🔼		Iter			
	Filter by AllyCo	meet chent	■ All .			itei			
VPN Cluster Loads	Username	Group Policy	Assigned IP Address	Protocol	Login Time	Bytes Tx	Inactivity	Audit !	Details
Crypto Statistics	vonuser	AnyConnect MGMT.	192,168,10,1	AnyConnect-Parent	10:52:25 UT	34688	0h:00m:00s	c0a80	
E Compression Statistics	(pridoci	AnyConnect_MGMT.	10.65.84.175	AnyConnect-Parent	: (1)none 0h:01m:31s	33954			Logout
Encryption Statistics								_	
Global IKE/IPsec Statistics									Ping
Protocol Statistics									
VLAN Mapping Sessions									
Shared SSL VPN									
VPN Connection Graphs									
WSA Sessions									
_									
Interfaces									
C T 1 mil									
VPN VPN	Townshipstown					,			
4 Routing	To sort VPN sessio	ns, right-click on th	he above table and s	select Table Sort Orde	er from popup menu.				
4 Louing									

Verificatie van de VPN-tunnelverbinding van beheer op de clientmachine:

Sisco AnyConnect Secure Mobili	ty Client	- 🗆 🗙	
cisco AnyCon	nect Secure Mobility Clie	ent	
Virtual Private Network (VPN	۷)	Diagnostics	
Preferences Statistics Route Detail	s Firewall Message History		
Connection Information State: Tunnel Mode (IPv4): Tunnel Mode (IPv6):	Disconnected Not Available Not Available	Cisco AnyConnect Secure Mobility Client –	×
Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available 00:00:00 None Connected (asa.example.com)	VPN: Ready to connect.	nect
Address Information		-	
Client (IPv4): Client (IPv6): Server:	Not Available Not Available Not Available	¢ (j)	uluulu cisco
Bytes		^	
	Reset	Export Stats	

Problemen oplossen

De nieuwe UI Statistics-lijn (Management Connection State) kan worden gebruikt om problemen op te lossen met de connectiviteit van de beheerstunnel. Dit zijn de meest voorkomende fouttoestanden:

Verbinding verbroken (uitgeschakeld):

- Deze optie is uitgeschakeld.
- Zorg ervoor dat het VPN-beheerprofiel is geïmplementeerd op de client, via een verbinding met een gebruikerstunnel (u moet het VPN-beheerprofiel toevoegen aan het beleid van de gebruikerstunnel-groep) of buiten de band via de handmatige upload van het profiel.
- Zorg ervoor dat het VPN-beheerprofiel is geconfigureerd met één hostingang die een tunnelgroep omvat.

Verbroken (vertrouwd netwerk):

• TND heeft een vertrouwd netwerk gedetecteerd zodat de beheerstunnel niet tot stand is gebracht.

Verbroken (gebruikerstunnel actief):

• Een VPN-tunnel voor gebruikers is momenteel actief.

Verbinding verbroken (proces is niet gestart):

• Een fout bij de start van het proces is opgetreden wanneer de verbinding met de

beheerstunnel wordt geprobeerd.

Verbinding verbroken (verbinding mislukt):

- Een verbindingsmislukking werd ontmoet toen de beheerstunnel wordt gevestigd.
- Zorg ervoor dat de certificaatverificatie is geconfigureerd in de tunnelgroep, dat er geen banner aanwezig is in het groepsbeleid en dat het servercertificaat moet worden vertrouwd.

Verbroken (ongeldige VPN-configuratie):

- Een ongeldige gesplitste tunnelconfiguratie is ontvangen van de VPN-server.
- Controleer de configuratie van gesplitste tunnels in het beleid van de beheertunnelgroep.

Verbinding verbroken (software-update in behandeling):

• Een AnyConnect-software-update is momenteel in behandeling.

Verbroken:

• De beheerstunnel staat op het punt te worden opgezet of kan om een andere reden niet worden opgezet.

Verzamel DART voor verdere probleemoplossing.

Gerelateerde informatie

- Configuratie van VPN-tunnelbeheer
- <u>VPN-tunnel voor probleemoplossing</u>
- Technische ondersteuning en documentatie Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.