# AnyConnect Secure Mobility Client met splittunneling op een ASA configureren

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Informatie over AnyConnect-licenties Configureren Netwerkdiagram ASDM AnyConnect-configuratiewizard Configuratie van split-tunneling AnyConnect-client downloaden en installeren Webimplementatie Standalone-implementatie **CLI-configuratie** Verifiëren Problemen oplossen **DART** installeren **DART** uitvoeren Gerelateerde informatie

# Inleiding

In dit document wordt beschreven hoe u de Cisco AnyConnect Secure Mobility Client configureert via de Cisco Adaptive Security Device Manager (ASDM) op een Cisco adaptieve security applicatie (ASA) waarop softwareversie 9.3(2) draait.

# Voorwaarden

### Vereisten

Het pakket voor de webimplementatie van Cisco AnyConnect Secure Mobility Client moet worden gedownload naar het lokale bureaublad waarop de ASDM-toegang tot de ASA aanwezig is. Ga naar de webpagina <u>Cisco AnyConnect Secure Mobility Client</u> om het pakket te downloaden. De webimplementatiepakketten voor verschillende besturingssystemen kunnen tegelijkertijd worden geüpload naar de ASA.

Dit zijn de bestandsnamen voor de verschillende besturingssystemen:

• Microsoft Windows-besturingssystemen: AnyConnect-win-<version>-k9.pkg

- Apple-besturingssystemen (macOS): AnyConnect-macosx-i386-<version>-k9.pkg
- Linux-besturingssystemen: AnyConnect-linux-<version>-k9.pkg

### Gebruikte componenten

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

- ASA versie 9.3(2)
- ASDM versie 7.3(1)101
- AnyConnect versie 3.1

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 de potentiële impact van elke opdracht begrijpen.

# Achtergrondinformatie

Dit document bevat gedetailleerde informatie over het gebruik van de Cisco AnyConnectconfiguratiewizard via de ASDM om de AnyConnect-client te configureren en split-tunneling mogelijk te maken.

Split-tunneling wordt gebruikt wanneer alleen specifiek verkeer moet worden getunneld, in tegenstelling tot gevallen waarbij alle door het clientapparaat gegenereerde verkeersstromen via het verbonden VPN lopen. Het gebruik van de AnyConnect-configuratiewizard leidt automatisch tot de configuratie *tunnel-all* op de ASA. Split-tunneling moet apart worden geconfigureerd. Dit wordt in dit document nader uitgelegd.

De bedoeling van dit configuratievoorbeeld is om verkeer voor subnet 10.10.10.0/24 (het LANsubnet achter de ASA) via de VPN-tunnel te verzenden. Al het andere verkeer van het clientapparaat wordt via het eigen internetcircuit doorgestuurd.

### Informatie over AnyConnect-licenties

Hier is een aantal links naar nuttige informatie over de Cisco AnyConnect Secure Mobility Clientlicenties:

- Raadpleeg het document <u>AnyConnect Secure Mobility Client functies, licenties en</u> <u>besturingssystemen, release 3.1</u> om te weten te komen welke licenties vereist zijn voor de AnyConnect Secure Mobility Client en bijbehorende functies.
- Raadpleeg de <u>Cisco Bestelgids voor AnyConnect</u> voor informatie over AnyConnect Apex- en Plus-licenties.
- Raadpleeg het document <u>Welke ASA-licentie is er nodig voor IP-telefoon- en mobiele VPN-</u> <u>verbindingen?</u> voor informatie over de extra licentievereisten voor IP-telefoon- en mobiele

verbindingen.

# Configureren

In dit gedeelte wordt beschreven hoe u de Cisco AnyConnect Secure Mobility Client op de ASA kunt configureren.

### Netwerkdiagram

Dit is de topologie die voor de voorbeelden in dit document wordt gebruikt:



### ASDM AnyConnect-configuratiewizard

De AnyConnect-configuratiewizard kan worden gebruikt om de AnyConnect Secure Mobility Client te configureren. Zorg ervoor dat een AnyConnect-clientpakket is geüpload naar de flash/schijf van de ASA-firewall voordat u verdergaat.

Volg de volgende stappen om de AnyConnect Secure Mobility Client te configureren met de configuratiewizard:

1. Log in bij ASDM, open de Configuration Wizard en klik op Next:

Cisco ASDM 7.3 for	r ASA - 10.106.44.21	The second second	NAME OF TAXABLE PARTY.
<u>File View Tools</u>	Mizards Window Help		
🍊 Hame 🗞 ConFig	Startup Wizard	C Forward 2 Help	
Device List	VPN Wizards	Site-to-site VPN Wizard	
🏶 Add 📋 Delete 💡	High Availability and Scalability Wizard	AnyConnect VPN Wizard	board
Find:	Unified Communication Wizard	Clientless SSL VPN Wizard	
- 🔠 10.106.44.3 - 🔊 10.106.44.21	ASDM Identity Certificate Wizard	IPsec (IKEv1) Remote Access VPN Wizard	
-	Packet Capture Wizard	Host Name: EdgeASA-4	
		ASA Version: 9.3(2) C ASDM Version: 7.3(1)101 C Firewall Mode: Routed C Environment Status: • 0K T	Xerice Uptime: 0d 16h 15m 5s Xerice Type: ASA 5525 Xontext Mode: Single Yotal Flash: 8102 MB

2. Voer de *Connection Profile Name* in, kies de interface waarop het VPN wordt beëindigd in het keuzemenu van de *VPN Access Interface* en klik op **Next**:

AnyConnect VPN Connect	ection Setup Wizard		-	X
Steps	Connection Profile Identific	ation		
1. Introduction	This step allows you to cor	nfigure a Connection Profile Nam	ne and the Inte	rface the remote access users will
2. Connection Profile Identification	access for VPN connection	s.		
3. VPN Protocols	Connection Profile Name:	SSLClient		
4. Client Images	VPN Access Interface;	outside	-	
5. Authentication Meth		•		

3. Vink het SSL-vakje aan om Secure Sockets Layer (SSL) in te schakelen. Het apparaatcertificaat kan een door een betrouwbare externe certificeringsinstantie (CA, zoals Verisign of Entrust) uitgegeven certificaat of een zelf-ondertekend certificaat zijn. Als het certificaat al op de ASA is geïnstalleerd kan het worden geselecteerd via het keuzemenu. Opmerking: Dit certificaat is het certificaat van de serverzijde dat zal worden verstrekt. Als er nog geen certificaten op de ASA zijn geïnstalleerd en er een zelf-ondertekend certificaat moet worden gegenereerd, klikt u op Manage.Om een certificaat van een externe partij te installeren moet u de stappen volgen die zijn beschreven in het Cisco-document <u>ASA 8.x:</u> voorbeeld van handmatige installatie van certificaten van een externe leverancier voor gebruik bij een WebVPN-configuratie.

AnyConnect VPN Connect VPN	ection Setup Wizard
Steps	VPN Protocols
1. Introduction	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol
2. Connection Profile	or protocols you would like this connection profile to support.
Identification	V SSL
3. VPN Protocols	
4. Client Images	IPsec
5. Authentication Meth	Device Certificate
6. Client Address Assignment	Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.
7. Network Name Resolution Servers	Device Certificate: None
8. NAT Exempt	
0 AnyConnect Client	

#### 4. Klik op **Add**:

Manage Ider	ntity Certificat	tes				X
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
						Delete
						Export
						Install

5. Typ de juiste naam in het veld *Trustpoint Name* en klik op het keuzerondje Add a new identity certificate. Als er geen RSA-sleutelparen (Rivest-Shamir-Addleman) op het apparaat aanwezig zijn, klik dan op **New** om er een te genereren:

🔄 Add Identity Certificate	
Trustpoint Name:	SelfsignedCert
Import the identity certific	cate from a file (PKCS12 format with Certificate(s)+Private Key):
Decryption Passphrase:	
File to Import From:	Browse
Add a new identity certific	cate:
Key Pair:	<default-rsa-key> ▼ Show New</default-rsa-key>
Certificate Subject DN:	CN=anyconnect.cisco.com Select
Generate self-signed	certificate
🗌 Act as local certi	ficate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Cer	tificate Cancel Help

6. Klik op het keuzerondje **Use default key pair name** of klik op het keuzerondje **Enter new key pair name** en voer een nieuwe naam in. Selecteer het formaat van de sleutels en klik vervolgens op **Generate Now**:

<b>E</b>	Add Key F	Pair	<b>X</b>
	Кеу Туре:	RSA	© ECDSA
	Name:	🔘 Use default key pair name	
		Enter new key pair name:	ssicert
	Size:	2048 🗸 🗸	
	Usage:	<ul> <li>General purpose</li> </ul>	🔘 Special
		Generate Now Cancel	Help

7. Nadat het RSA-sleutelpaar is gegenereerd kiest u de sleutel en vinkt u het vakje **Generate** self-signed certificate aan. Voer het gewenste domeinnaam onderwerp (DN) in bij *Certificate Subject DN* en klik vervolgens op Add Certificate:

Add Identity Certificate	×
Trustpoint Name:	SelfsignedCert
Import the identity certific	cate from a file (PKCS12 format with Certificate(s)+Private Key):
Decryption Passphrase:	
File to Import From:	Browse
Add a new identity certification	cate:
Key Pair:	ssicert   Show New
Certificate Subject DN:	CN=anyconnect.cisco.com Select
Generate self-signed	certificate
🔲 Act as local certi	ficate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Cer	tificate Cancel Help

8. Klik nadat de inschrijving is voltooid op OK, OK en Next:

📴 Ar	nyConnect VPN Connection Setup Wizard			
Ste	Manage Identity Certificates			X
1.	Testied To Testied By Evoliny Date Associate	d Trustopints - Lisage	Public Key Type	Add
2.	hostname hostname 16:39:40 M Selfsigne	dCert Gener	RSA (2048 bits)	Show Details
3.				Delete
4. 5.				Export
6				Install
0.	Eind: 🛛 🛇 🕅 Match	Case		
7.	Public CA Enrollment			
8.	Get your Cisco ASA security appliance up and runn Entrust, Entrust offers, Cisco qustomers, a special pr	ing quickly with an SSL A comptional price for certi	dvantage digital certificates and trial certifi	ficate from
9.	Enroll ASA	SSL certificate with Entru	ist	cause for testing.
10	Using a previously saved certificate signing reques	t, enroll with Entrust.		
	ОК	Cancel	Help	

9. Klik op Add om de image van de AnyConnect-client (het .pkg-bestand) toe te voegen vanaf de pc of het flash-geheugen. Klik op Browse Flash om de image toe te voegen vanaf het flashstation of klik op Upload om de image direct vanaf de hostcomputer toe te voegen:

5. Authentication Meth	Add Replace To Delete 🕈 🗸
6. Client Address Assignment	Add AnyConnect Client Image
7. Network Name Resolution Servers	AnyConnect Image: Browse Flash
8. NAT Exempt	Upload
<ol> <li>AnyConnect Client Deployment</li> </ol>	Regular expression to match user-agent
10. Summary	OK Cancel Help

Browse Flash				x
Folders	Files			
disk0:	FileName	Size (	Date	
crypto_archive     coredumpinfo     for coredumpinfo     for coredumpinfo	anyconnect-win-3.1.05152-k9.pkg	35,167,	12/17/	
	anyconnect-win-3.1.06073-k9.pkg	38,048,	01/02/	
	asa932-smp-k8.bin	63,479,	01/02/	
	and a real sector bits	10.004	11/00/	

10. Klik op Next nadat de image is toegevoegd:

🕈 Add 🗹 Replace 📋 Delete 🛧 🗲	
Image	Regular expression to match user-agent
disk0:/anyconnect-win-3.1.06073-k9.pkg	
You can download AnyConnect Client packages from <u>C</u> <u>here</u> ,	iisco by searching 'AnyConnect VPN Client' or <u>click</u>
< Back Next >	Cancel Help

11. De gebruikersverificatie kan worden voltooid via de AAA-servergroepen (verificatie, autorisatie en accounting). Als de gebruikers al zijn geconfigureerd, kiest u LOCAL en klikt u op Next. Opmerking: In dit voorbeeld wordt LOKALE verificatie geconfigureerd. Dit betekent dat de lokale gebruikersdatabase op de ASA gebruikt zal worden voor verificatie.

AnyConnect VPN Co	nnection Setup Wizard	
Steps 1. Introduction	Authentication Methods This step lets you specify the location of the authentication server.	_
2. Connection Profile Identification	You can click on the "New" button to create a new server group.	
<ol> <li>VPN Protocols</li> <li>Client Images</li> </ol>	Local User Database Details	
5. Authentication Methods	cisco	
6. Client Address Assignment	User to be Added User1	
<ol> <li>Network Name Resolution Servers</li> </ol>	Password:	
8. NAT Exempt	Confirm Password: ••••	
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel Help	]

12. De adresgroep voor de VPN-client moet worden geconfigureerd. Als er al een is geconfigureerd, selecteert u deze in het keuzemenu. Zo niet, klik dan op **New** om een nieuwe te configureren. Klik na voltooiing op **Next**:

D. VENTER OLOCOIS							
4. Client Images	IP v4 A	IP v4 Address Pool IP v6 Address Pool					
5. Authentication Meth	Address Poo	l: [ Select 🔻 Nev	H				
6. Client Address Assignment	Details of	Add IPv4 Pool		×			
7. Network Name Resolution Servers		Name:	SSL-Pool				
3. NAT Exempt		Starting IP Address:	10.10.11.1	-			
<ol> <li>AnyConnect Client Deployment</li> </ol>		Ending IP Address:	10.10.11.20				
10. Summary		Subnet Mask:	255.255.255.0	•			
		ОК	Cancel	Help			

13. Voer de DNS-servers (Domain Name System) en DN's correct in bij de velden *DNS* en *Domain Name* en klik vervolgens op **Next**:

Steps	Network Name R	Network Name Resolution Servers					
1. Introduction	This step lets you	This step lets you specify how domain names are resolved for the remote user when accessing the internal					
2. Connection Profile	network.						
3 VPN Protocols	DNS Servers:	10.10.10.23					
4. Client Images	WINS Servers:						
5. Authentication Meth	Domain Name:	Cisco.com					

14. In dit geval is het doel om de toegang via het VPN te beperken tot het netwerk 10.10.0/24 dat als *Inside*-subnet (of LAN) achter de ASA is geconfigureerd. Het verkeer tussen de client en het inside-subnet moet zijn vrijgesteld van iedere dynamische Network Address Translation (NAT).

Vink het vakje **Exempt VPN traffic from network address translation** aan en stel de LAN- en WAN-interfaces in die voor de vrijstelling gebruikt gaan worden:

<ul> <li>3. VPN Protocols</li> <li>4. Client Images</li> <li>5. Authentication Metho</li> <li>6. Client Address Assignment</li> <li>7. Network Name Resolution Servers</li> <li>8. NAT Exempt</li> <li>9. AnyConnect Client</li> </ul>	2. Connection Profile Identification	Exempt VPN traffic from network address translation				
<ul> <li>4. Client Images Inside Interface: Inside </li> <li>5. Authentication Metho</li> <li>6. Client Address Assignment Local Network is the network address(es) of the internal network that client can access. Local Network: any </li> <li>7. Network Name Resolution Servers</li> <li>8. NAT Exempt The traffic between AnyConnect client and internal network will be exempt from network address translation.</li> <li>9. AnyConnect Client</li> </ul>	3. VPN Protocols	Inside Interface is the interface directly connected to your internal network.				
<ul> <li>5. Authentication Metho</li> <li>6. Client Address Assignment</li> <li>7. Network Name Resolution Servers</li> <li>8. NAT Exempt</li> <li>9. AnyConnect Client</li> </ul>	4. Client Images	Inside Interface: Inside 🔹				
<ul> <li>6. Client Address Assignment</li> <li>7. Network Name Resolution Servers</li> <li>8. NAT Exempt</li> <li>9. AnyConnect Client</li> </ul>	5. Authentication Metho	Local Network is the network address(es) of the internal network that client				
Assignment Local Network: any 7. Network Name Resolution Servers 8. NAT Exempt 9. AnyConnect Client 4. Cocal Network: any The traffic between AnyConnect client and internal network will be exempt from network address translation.	6. Client Address	can access.				
<ul> <li>Network Name Resolution Servers</li> <li>NAT Exempt</li> <li>AnyConnect Client</li> </ul>	Assignment	Local Network: any				
8. NAT Exempt       The traffic between AnyConnect client and internal network will be exempt from network address translation.         9. AnyConnect Client       Image: stranslation internal network address translation.	<ol> <li>Network Name Resolution Servers</li> </ol>					
9. AnyConnect Client	8. NAT Exempt	The traffic between AnyConnect client and internal network will be exempt from network address translation.				
	9. AnyConnect Client					

15. Kies de lokale netwerken die moeten worden vrijgesteld:

Filter:				Filter Clea
Name 1	IP Address	Netmask	Description	Object NAT Addr
- IPv4 Network	Objects			
- 🏈 any				
🔤 🛃 Inside.	. 10.10.10.0	255.255.255.0		
- 📑 outsid.	. 10.106.44.0	255.255.255.0		
- 🚅 10.0.0.	0 10.0.0.0	255.0.0.0		
- 🛃 10.1.2.	10.1.232.192	255.255.255		
- IPv4 Network	Object Groups			
🗈 🞆 ANY				
🕀 🎆 OBJ_L				
🗄 🎆 OBJ_S.				
Interfaces				
TI ISICIB				
outside				
Selected Local Ne	etwork			
Selected Local Netwo	etwork rk -> Inside-r	network/24		
Selected Local Netwo	etwork rk -> Inside-r	network/24		OK Cance
Selected Local Netwo	etwork rk -> Inside-r	hetwork/24 k is the network addr	ess(es) of the internal net	OK Cance
Authentication Meth	etwork rk -> Inside-r	hetwork/24	ess(es) of the internal net	OK Cance
Authentication Meth Client Address Assignment	etwork wrk -> Inside-r Local Networ can access. Local Networ	hetwork/24 k is the network addr k: 10.10.10.0/24	ess(es) of the internal net	OK Cance work that client
Authentication Meth Client Address Assignment Network Name Resolution Servers	etwork rk -> Inside-r Local Networ Local Networ	hetwork/24 k is the network addr k: 10.10.10.0/24	ess(es) of the internal net	OK Cance work that client
Authentication Metho Client Address Assignment Network Name Resolution Servers NAT Exempt	etwork rk -> Inside-r Local Networ can access. Local Networ The traffic be	hetwork/24 k is the network addr k: 10.10.10.0/24 etween AnyConnect cl	ess(es) of the internal net	OK Cance work that client
Authentication Meth Client Address Assignment Network Name Resolution Servers NAT Exempt AnyConnect Client Deployment	etwork rk -> Inside-r	k is the network addr k: 10.10.10.0/24 etween AnyConnect cl k address translation.	ess(es) of the internal net	OK Cance work that client

#### 16. Klik op Next, Next en vervolgens op Finish.

De configuratie van de AnyConnect-client is nu voltooid. Wanneer u AnyConnect echter via de configuratiewizard instelt, wordt het *Split Tunnel*-beleid standaard ingesteld op **Tunnelall**. Om alleen specifiek verkeer te tunnelen, moet *split-tunneling* worden geïmplementeerd.

Opmerking: Als split-tunneling niet is geconfigureerd zal het Split Tunnel-beleid gebaseerd

zijn op het standaard groepsbeleid (DfltGrpPolicy). Deze is standaard ingesteld op **Tunnelall.** Dit betekent dat al het verkeer (inclusief het internetverkeer) via de tunnel wordt verzonden zodra de client via VPN is verbonden.

Alleen het verkeer dat bestemd is voor het IP-adres van het WAN van de ASA (of *outside*) zal de tunneling op het clientapparaat omzeilen. Dit kunt u zien in de output van de opdracht **route print** op Microsoft Windows-computers.

### Configuratie van split-tunneling

Split-tunneling is een functie die u kunt gebruiken om te definiëren welk verkeer bestemd voor de subnetten of hosts moet worden versleuteld. Dit betreft de configuratie van een toegangscontrolelijst (ACL) die aan deze functie wordt gekoppeld. Het verkeer voor de subnetten of de hosts dat op deze ACL wordt gedefinieerd zal via de tunnel vanaf de kant van de client worden versleuteld. De routes voor deze subnetten worden geïnstalleerd op de routingtabel van de pc.

Voltooi deze stappen om de Tunnel-all-configuratie te wijzigen in de Split-tunnel-configuratie:

1. Ga naar Configuration > Remote Access VPN > Group Policies:



 Klik op Edit en gebruik de navigatiestructuur om naar Advanced > Split Tunneling te gaan. Zet het vakje Inherit uit in het gedeelte *Policy* en selecteer Tunnel Network List Below in het keuzemenu:

Edit Internal Group Policy	r: GroupPolicy_SSLClient	7-	
General	The VPN client makes split tunne	ling decisions on the	basis of a network list that can be specifie
Advanced	DNS Names:	📝 Inherit	
Browser Proxy	Send All DNS Lookups Through T	funnel: 📝 Inherit	O Yes O No
_ 、 ,	Policy:	📃 Inherit	Tunnel Network List Below
	Network List:	📝 Inherit	

3. Zet het vakje **Inherit** uit in het gedeelte *Network List* en klik op **Manage** om de ACL te selecteren die een of meerdere LAN-netwerken specificeert waartoe de client toegang nodig

#### heeft:

Network List:	🔲 Inherit	inside_access_in	•]	Manage
Pressing this button to set up split extu: Set up Split Exclusion for Web Secur	sion for Web ⊆ ity	curity proxies.		

4. Klik op Standard ACL, Add, Add ACL en typ vervolgens in het vak ACL Name:

General	The VPN	lient makes split tunneling decisions on the basis of a network list that can be specif				
Advanced	DNS N	ACL Manager				
Browser Proxy	Send	Standard ACL Extended ACL				
IPsec(IKEv1) Client	/1) Client 🕂 🕹 Add - 🗹 Edit 👚 Delete 🛧 - 🐇 ங 🕮 -					
	Policy	No Address Action Description				
	Netwo					
		Add ACL				
	Pressi	ACL Name: Split-ACL				
	Set	ACL Name: Spin-ACL				
	Inte	OK Cancel Help				

5. Klik op Add ACE om de regel toe te voegen:

ACL Man	lager	_						
Standard ACL Extended ACL								
🗣 Add 🕶 🗹 Edit <u>î</u> Delete   🛧 🗲   👗 🐚 🏙 -								
No	Address	Action	Description					
Split-A	CL							
Add ACE								
Action: O Permit O Deny								
Address: 10.10.10.0/24								
Descrin	tion:							

6. Klik op **OK**.

Edit Internal Group Policy	GroupPolicy_SSLCient	7-		×
-Ceneral -Cenvers	The VPN client makes split to realing de	istorie on the	base of a network ust that can be specified below by providing the proper carameters to Yokoy' and Network tool' fe	e des
É-Advanced —Split Tunne Ing	DNE Names:	🟹 Inherit		
→Browser Frowy → AnyConnect Client → Psec(0(Byt)) Client	Send All DRS Loci ups Through Tunnel:	🔽 Interit	⊙ ves ⊙No	
	Poloy:	<ul> <li>Inherit</li> </ul>	Turnel Network List Selow 🔻	
	Notwork List:	🔲 Inherit	9515-401 · · · · · · · · · · · · · · · · · · ·	Manage
	Pressing this burson to set up to it eaks Earlup Split Estlusion for Web Secur	ion for web s	iecunity provides	
	Intercept DHEP Configuration Mes	sage from N	ficrosoft Clienta	*

#### 7. Klik op Apply (Toepassen).

Zodra er verbinding is, worden de routes voor de subnetten of hosts op de gesplitste ACL toegevoegd aan de routingtabel van het clientapparaat. Op Microsoft Windows-computers kan dit worden bekeken in de output van de opdracht **route print**. De volgende hop voor deze routes zal een IP-adres van het subnet van de IP-adresgroep van de client zijn (doorgaans het eerste IP-adres van het subnet):

C:\Users\admin>route print IPv4 Route Table Active Routes: Network Destination Netmask Gateway Interface Metric 0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261 10.10.10.0 255.255.255.0 10.10.11.2 10.10.11.1 2

*!!* This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261 172.16.21.1 255.255.255 On-link 10.106.44.243 6

*!! This is the route for the ASA Public IP Address.* Voer op macOS-computers de opdracht **netstat -r** in om de routingtabel van de computer te bekijken:

\$ netstat -r Routing tables Internet: Destination Gateway Flags Refs Use Netif Expire default hsrp-64-103-236-1. UGSc 34 0 enl 10.10.10/24 10.10.11.2 UGSc 0 44 utun1 !! This is the split tunnel route. 10.10.11.2/32 localhost UGSc 1 0 lo0 172.16.21.1/32 hsrp-64-103-236-1. UGSc 1 0 en1 !! This is the route for the ASA Public IP Address.

### AnyConnect-client downloaden en installeren

Er zijn twee methoden die u kunt gebruiken om Cisco AnyConnect Secure Mobility Client op de computer van de gebruiker te implementeren:

- Webimplementatie
- Standalone-implementatie

Beide methoden worden in de volgende secties nader toegelicht.

#### Webimplementatie

Om de implementatiemethode via het web te gebruiken moet u de URL https://<ASA's IP> of <ASA's FQDN> in een browser op het clientapparaat invoeren. Deze brengt u naar de pagina van de *WebVPN*-portal.

**Opmerking:** Als u Internet Explorer (IE) gebruikt, wordt de installatie meestal voltooid via ActiveX, tenzij u Java moet gebruiken. Alle andere browsers gebruiken Java.

Na het inloggen op de pagina begint de installatie op het clientapparaat. De client zou verbinding moeten maken met de ASA nadat de installatie is voltooid.

**Opmerking:** Mogelijk wordt u gevraagd om toestemming voor het uitvoeren van ActiveX of Java. Geef toestemming om verder te kunnen gaan met de installatie.

Logon						
Group	SSLClient V					
Username						
Password						
	Logon					

🖕 🍚 🕑 🚺 🖉 🖉 🖉 🖉 🖉

cisco AnyConnect Secure Mobility Client							
🔦 WebLaunch	Attempting to use Java for Installation						
<ul> <li>Platform</li> <li>Detection</li> <li>- ActiveX</li> </ul>	Sun Java applet has started. This could take up to 60 seconds. <b>Please wait</b>						
Java Detection							
🗌 - Java							
Download							
Connected							
	Help Download						

#### Standalone-implementatie

Volg de volgende stappen om de standalone-implementatiemethode te gebruiken:

- Download de image van de AnyConnect-client van de Cisco-website. Raadpleeg de webpagina <u>Cisco AnyConnect Secure Mobility Client</u> om te zien welke image moet worden gedownload. Op deze pagina staat een downloadlink. Ga naar de downloadpagina en selecteer de juiste versie. Zoek naar Full installation package - Windows/standalone installer (ISO). Opmerking: Vervolgens wordt er een ISO-image met het installatieprogramma gedownload (zoals *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
- 2. Gebruik *WinRar* of *7-Zip* om het ISO-pakket uit te pakken:

Development win 21,070				
anyconnect-win-5.1.070		Burn disc image		
	7-Zip Edit with Notepad++ Open with		÷	Open archive
				Open archive
			•	Extract files
		Share with	•	Extract Here
				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

3. Nadat het pakket is uitgepakt, opent u het bestand **Setup.exe** en kiest u de modules die samen met Cisco AnyConnect Secure Mobility Client moeten worden geïnstalleerd.

**Tip**: Om extra instellingen voor VPN te configureren raadpleegt u de sectie <u>AnyConnect</u> <u>VPN-clientverbindingen configureren</u> van de *Configuratiehandleiding voor de Cisco ASA 5500 Series met behulp van de CLI, 8.4 en 8.6*.

### **CLI-configuratie**

Deze sectie bevat de CLI-configuratie voor Cisco AnyConnect Secure Mobility Client ter referentie.

```
ASA Version 9.3(2)
1
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
1
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224
access-list all extended permit ip any any
!********Split ACL configuration*********
access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
```

no pager logging enable logging buffered debugging mtu outside 1500 mtu inside 1500 mtu dmz 1500 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-721.bin no asdm history enable arp timeout 14400 no arp permit-nonconnected !This will exempt traffic from Local LAN(s) to the !Remote LAN(s) from getting NATted on any dynamic NAT rule. nat (inside,outside) source static NETWORK\_OBJ\_10.10.10.0\_24 NETWORK\_OBJ\_10.10.10.0\_24 destination static NETWORK OBJ 10.10.11.0 27 NETWORK OBJ 10.10.11.0 27 no-proxy-arp route-lookup access-group all in interface outside route outside 0.0.0.0 0.0.0.0 172.16.21.2 1 timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 dynamic-access-policy-record DfltAccessPolicy user-identity default-domain LOCAL aaa authentication ssh console LOCAL http server enable http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact !\*\*\*\*\*\*\*\* Trustpoint for Selfsigned certificate\*\*\*\*\*\*\*\*\* !Genarate the key pair and then configure the trustpoint !Enroll the trustpoint genarate the self-signed certificate crypto ca trustpoint SelfsignedCert enrollment self subject-name CN=anyconnect.cisco.com keypair sslcert crl configure crypto ca trustpool policy crypto ca certificate chain SelfsignedCert certificate 4748e654 308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105 0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e 170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0 55a975ec alf2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4 ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0 7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c 75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93 5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7 53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34 03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36

```
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-shal
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-shal 3des-shal aes128-shal aes256-shal
!******* Bind the certificate to the outside interface*******
ssl trust-point SelfsignedCert outside
!******Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable
!*****Group Policy configuration*******
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.
group-policy GroupPolicy SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com
username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
!*****Tunnel-Group (Connection Profile) Configuration****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
class-map inspection_default
match default-inspection-traffic
!
1
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
```

```
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

# Verifiëren

Volg de volgende stappen om de clientverbinding en de verschillende parameters die bij die verbinding horen te controleren:

1. Ga naar Monitoring > VPN op de ASDM:



2. U kunt de **Filter By**-optie gebruiken om op het type VPN te filteren. Selecteer **AnyConnect Client** in het keuzemenu en alle AnyConnect-clientsessies. **Tip**: De sessies kunnen verder worden gefilterd met behulp van andere criteria, zoals *gebruikersnaam* en *IPadres*.



3. Dubbelklik op een sessie om meer te weten te komen over die specifieke sessie:

essio	n Details								
Username		Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Login Time Encryption Duration			Bytes Tx Bytes Rx	Inactivity	
isco		GroupPolicy_SSLClien 10.10.11.1 SSLClient 172.16.21.1		AnyConnect-Parent SSL-Tunnel . 16:58:56 UTC 1147 AnyConnect-Parent: (1)none S. Oh:21m:09s 2665			1472 6653	0h:DDm:DDs	
eta	Type	Local Addr. / Subnet N	Ask / Protocol / Port	Encryption	Other		Bytes Tx		Mor
	AnyConn		Maak, ( Product) / Port	none	Tunnel ID: 14.1 Public IP: 172.16.2 Hashing: none TCP Src Port 5782 TCP Dst Port 443 Authentication Mo Idle Time Out: 30 Idle TO Left: 9 Mir Client OS Type: W Client Tunn: Arro	21.1 28 de : userPassword Minutas Tutes Vindows accord	5954 1046	• 11	

 Voer de opdracht show vpn-sessiondb anyconnect in op de CLI om de gegevens van de sessie te zien:

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1 Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. U kunt de andere filteropties gebruiken om de resultaten te verfijnen:

#### ${\ensuremath{\tt \#}}$ show vpn-sessiondb detail any connect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 11036 Bytes Rx : 4977 Pkts Tx : 8 Pkts Rx : 60 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy\_SSLClient Tunnel Group : SSLClient Login Time : 20:33:34 UTC Mon Apr 6 2015 Duration : 0h:01m:19s

```
AnyConnect-Parent Tunnels: 1
```

SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 19.1 Public IP : 10.106.44.243 Encryption : none Hashing : none TCP Src Port : 58311 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 5518 Bytes Rx : 772 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel TD : 19.2 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Encryption : 3DES Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 58315 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 5518 Bytes Rx : 190 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 19.3 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Encryption : DES Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 58269 UDP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 0 Bytes Rx : 4150 Pkts Tx : 0 Pkts Rx : 59 Pkts **Tx Drop** : 0 Pkts **Rx Drop** : 0

## Problemen oplossen

U kunt de AnyConnect Diagnostics en Reporting Tool (DART) gebruiken om gegevens te verzamelen die handig zijn bij het troubleshooten van problemen met de AnyConnect configuratiewizard of de verbinding. De DART-wizard kan worden gebruikt op een computer met AnyConnect. DART verzamelt de logboeken, status en diagnostische informatie voor analyse door de Cisco Technical Assistance Center (TAC) en heeft geen beheerdersbevoegdheden nodig om op het clientapparaat te werken.

### **DART** installeren

Volg de volgende stappen om DART te installeren:

1. Download de image van de AnyConnect-client van de Cisco-website. Raadpleeg de

webpagina <u>Cisco AnyConnect Secure Mobility Client</u> om te zien welke image moet worden gedownload. Op deze pagina staat een downloadlink. Ga naar de downloadpagina en selecteer de juiste versie. Zoek naar **Full installation package - Windows/standalone installer** (ISO). Opmerking: Vervolgens wordt er een ISO-image met het installatieprogramma gedownload (zoals *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).

2. Gebruik *WinRar* of *7-Zip* om het ISO-pakket uit te pakken:

anvennast vin 21.070	· · · · · · · · · · · · · · · · · · ·			
anyconnect-win-5.1.070.		Burn disc image		
		7-Zip	×	Open archive
	2	Edit with Notepad++		Open archive
		Open with	•	Extract files
		Share with	•	Extract Here
				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

- 3. Ga naar de map waarin de inhoud is uitgepakt.
- 4. Open het bestand Setup.exe en selecteer alleen AnyConnect Diagnostic and Reporting Tool:



### DART uitvoeren

Dit is belangrijke informatie die u in overweging moet nemen voordat u DART uitvoert:

- De kwestie moet minstens één keer worden gereproduceerd voordat u DART uitvoert.
- De datum en de tijd op de computer van de gebruiker moeten worden genoteerd wanneer het probleem wordt gereproduceerd.

Open DART vanuit het menu Start op het clientapparaat:



U kunt de optie *Default* of Custom *selecteren*. Cisco raadt u aan om DART in de Default-modus te draaien zodat alle informatie in één overzicht kan worden vastgelegd.

Cisco DART 3.1.05170	X							
Bundle Creation Option	lulu isco							
Select "Default" to include the typical log files and diagnostic informa the bundle. Select "Custom" to choose the list of log files and diagno information to be included in the bundle.	tion in ostic							
<ul> <li>Default (Bundle will be saved to Desktop)</li> </ul>								
Custom								
Clear logs after DART finshes								
Back Next	Cancel							

Na voltooiing slaat de tool het .zip-bestand van de DART-bundel op het bureaublad van de client

op. De bundel kan dan naar de TAC worden gemaild (nadat u een TAC-case heeft geopend) voor nadere analyse.

# Gerelateerde informatie

- Probleemoplossingsgids AnyConnect VPN-client veelvoorkomende problemen
- Java 7 problemen met AnyConnect, CSD/HostScan en WebVPN: Probleemoplossingsgids
- <u>Technische ondersteuning en documentatie Cisco Systems</u>

#### 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.