# AnyConnect VPN-clientomzettingsverkeer op ASA 9.X configureren

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Configureer omgekeerd extern toegangsverkeer AnyConnect VPN-client voor openbaar internet en VPN op een configuratievoorbeeld van een stick Netwerkdiagram ASA release 9.1(2) configuraties met ASDM release 7.1(6) ASA release 9.1(2) configuratie in de CLI Communicatie tussen AnyConnect VPN-clients met de TunnelAll-configuratie toestaan op zijn plaats Netwerkdiagram ASA release 9.1(2) configuraties met ASDM release 7.1(6) ASA release 9.1(2) configuratie in de CLI Communicatie tussen AnyConnect VPN-clients met splitter-tunnel toestaan Netwerkdiagram ASA release 9.1(2) configuraties met ASDM release 7.1(6) ASA release 9.1(2) configuratie in de CLI Verifiëren Problemen oplossen Gerelateerde informatie

# Inleiding

Dit document beschrijft hoe u een Cisco adaptieve security applicatie (ASA) release 9.x kunt instellen om VPN-verkeer om te keren. Het behandelt dit configuratiescenario: U-draai verkeer van verre toegangsclients.

**Opmerking:** Om een overlapping van IP-adressen in het netwerk te voorkomen, wijst u een volledig andere pool van IP-adressen toe aan de VPN-client (bijvoorbeeld 10.x.x.x, 172.16.x.x en 192.168.x.x). Deze IP-adresregeling is handig om problemen met uw netwerk op te lossen.

### haarspeld of bocht

Deze eigenschap is nuttig voor VPN verkeer dat een interface ingaat, maar dan uit die zelfde interface gerouteerd. Als je bijvoorbeeld een hub-and-spoke VPN-netwerk hebt waar het security

apparaat de hub is en de externe VPN-netwerken spokes zijn, moet men, om te communiceren met een ander spoke-verkeer, naar het security apparaat gaan en dan weer naar de andere spoke.

Voer het same-security-traffic bevel om verkeer toe te staan om de zelfde interface in te gaan en te verlaten.

ciscoasa(config)#same-security-traffic permit intra-interface

# Voorwaarden

### Vereisten

Cisco raadt u aan aan deze vereisten te voldoen voordat u deze configuratie probeert:

- De hub ASA security applicatie moet release 9.x uitvoeren.
- Cisco AnyConnect VPN-client 3.xOpmerking: Het AnyConnect VPN-clientpakket downloaden (anyconnect-win\*.pkg) vanuit de Cisco <u>Software Download</u> (alleen geregistreerde klanten). Kopieer de AnyConnect VPN-client naar het Cisco ASA-flitsgeheugen, dat moet worden gedownload naar de externe gebruikerscomputers om de SSL VPN-verbinding met de ASA tot stand te brengen. Raadpleeg het gedeelte <u>AnyConnect VPN-clientverbindingen</u> van de ASAconfiguratiehandleiding voor meer informatie.

### Gebruikte componenten

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

- Cisco 5500 Series ASA waarin softwareversie 9.1(2) wordt uitgevoerd
- Cisco AnyConnect SSL VPN-clientversie voor Windows 3.1.05152
- PC die een ondersteund besturingssysteem uitvoert per de <u>ondersteunde VPN-platforms</u>, <u>Cisco ASA Series</u>.
- Cisco Adaptive Security Device Manager (ASDM), versie 7.1(6)

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

De Cisco AnyConnect VPN-client biedt beveiligde SSL-verbindingen met het security apparaat voor externe gebruikers. Zonder een eerder geïnstalleerde client voeren externe gebruikers het IP-adres in in hun browser van een interface die is geconfigureerd om SSL VPN-verbindingen te accepteren. Tenzij het security apparaat is geconfigureerd om te worden omgeleid http://verzoeken aan https://moeten gebruikers de URL in het formulier invoeren https://

.Nadat de URL is ingevoerd, maakt de browser verbinding met die interface en geeft het inlogscherm weer. Als de gebruiker voldoet aan de login en authenticatie, en het security apparaat identificeert de gebruiker als in behoefte van de client, het downloadt de client die overeenkomt met het besturingssysteem van de externe computer. Na de download installeert en configureert de client zichzelf, maakt een beveiligde SSL-verbinding en blijft of verwijdert zichzelf (dit is afhankelijk van de configuratie van het security apparaat) wanneer de verbinding wordt beëindigd. In het geval van een eerder geïnstalleerde client, wanneer de gebruiker authenticeert, onderzoekt het security apparaat de revisie van de client en upgrades de client indien nodig.Wanneer de client een SSL VPN-verbinding met het security apparaat onderhandelt, maakt hij verbinding met Transport Layer Security (TLS) en gebruikt hij ook Datagram Transport Layer Security (DTLS). DTLS vermijdt latentie- en bandbreedteproblemen die aan sommige SSLverbindingen zijn gekoppeld en verbetert de prestaties van realtime toepassingen die gevoelig zijn voor pakketvertragingen. De AnyConnect-client kan worden gedownload van het security apparaat of de systeembeheerder kan de client handmatig op de externe pc installeren. Raadpleeg de beheerdershandleiding voor Cisco AnyConnect Secure Mobility Client voor meer informatie over het handmatig installeren van de client. Het security apparaat downloadt de client op basis van het groepsbeleid of de gebruikersnaam van de gebruiker die de verbinding tot stand brengt. U kunt het beveiligingstoestel configureren om automatisch de client te downloaden, of u kunt het configureren om de externe gebruiker te vragen of hij de client moet downloaden. In het laatste geval, als de gebruiker niet reageert, kunt u het security apparaat configureren om de client na een tijdelijke periode te downloaden of de login pagina te presenteren **Opmerking:** De voorbeelden die in dit document worden gebruikt, maken gebruik van IPv4. Voor IPv6-bochtverkeer zijn de

stappen hetzelfde, maar gebruik de IPv6-adressen in plaats van IPv4. **Configureer** 

**Omgekeerd extern toegangsverkeer**Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.Opmerking: Gebruik de handleidingen <u>Opdrachtreferenties</u> om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.AnyConnect VPN-client voor openbaar internet en VPN op een configuratievoorbeeld van een stickNetwerkdiagramHet netwerk in dit document is als volgt



ASA release 9.1(2) configuraties met ASDM release 7.1(6)Dit document gaat ervan uit dat de basisconfiguratie, zoals de interfaceconfiguratie, al is voltooid en correct werkt.Opmerking: Raadpleeg <u>Management Access configureren</u> om de ASA door de ASDM te kunnen configureren.Opmerking: In release 8.0(2) en hoger ondersteunt de ASA zowel clientloze SSL VPN (WebVPN)-sessies als ASDM-beheersessies tegelijkertijd op poort 43 van de buiteninterface. In versies eerder dan release 8.0(2) kunnen WebVPN en ASDM niet op dezelfde ASA-interface worden ingeschakeld, tenzij u de poortnummers wijzigt. Raadpleeg <u>ASDM en Web VPN Enabled</u>

# op dezelfde interface van de ASA voor meer informatie.Voltooi deze stappen om SSL VPN op een stok in ASA te configureren:

1. Kiezen Configuration > Device Setup > Interfaces *en controleer de* Enable traffic between two or more hosts connected to the same interface *controledoos om SSL VPN verkeer toe te staan om de zelfde interface in te gaan en te verlaten. Klik* Apply.

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Туре	Add 🔻
igabitEthemet0/0	outside	Enabled	0	172.16.1.1	255,255,255,0		Hardware	Edit
igabitEthernet0/1	inside	Enabled	100	10.77.241.142	255.255.255.192		Hardware	00010
igabitEthernet0/2		Disabled					Hardware	Delete
igabitEthernet0/3		Disabled					Hardware	
lanagement0/0	mgmt	Disabled	0				Hardware/Ma	
•	m						4	

#### Equivalente CLI-configuratie:

ciscoasa(config)#same-security-traffic permit intra-interface

2. Kiezen Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add om een IP-adresgroep te maken vpnpool.

Name:	vpnpool	
Starting IP Address:	192.168.10.1	
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	•

#### 3. Klik Apply. Equivalente CLI-configuratie:

ciscoasa(config) #ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

4. Web VPN inschakelen. Kiezen Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles *en onder* Access Interfaces *klikt u op de selectievakjes* Allow Access *en* Enable DTLS voor de buiteninterface. Controleer ook het Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below *controledoos om SSL VPN op de buiteninterface toe te laten*.

options. cess Interfaces C Enable Osc 59. acress mus	grits: The Cisco AnyCon	access on the interfac	is IPsec (IKEv2) tunnel a es selected in the table l e launched from a brows	is well as SSL tunnel with Datagram below ser (Web Launch) ,	Transport Layer Security (DTLS) tunnelin
access mas	c be enabled if you alone				
	SSL Access		IPsec (IKEv2) Acc	855	
Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate
Interface outside	SSL Access Allow Access	Enable DTLS	IPsec (JKEv2) Accord	Enable Client Services	Device Certificate

Klik Apply.Kiezen Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add om het Cisco AnyConnect VPN-clientbeeld uit het flitsgeheugen van ASA toe te voegen zoals aangegeven op de afbeelding.

Local File Parb:	Ct)Users) insemed) Deskton) any connect-win-3, 1, 05152-k9, nkg	Browse Local Files
Elach File Suctem Dath	dick0:/apycoppect.wip.3.1.05152.k9.pkg	Browce Elach
Add AnvConne	ct Client Image	×
<u> </u>		
AnyConnect Image	anyconnect-win-3.1.05152-k9.pkg	Browse Flash
	(	Upload

#### Equivalente CLI-configuratie:

ciscoasa(config)#**webvpn** 

ciscoasa(config-webvpn)#enable outside ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1 ciscoasa(config-webvpn)#tunnel-group-list enable ciscoasa(config-webvpn)#anyconnect enable

5. Groepsbeleid configureren. Kiezen Configuration > Remote Access VPN > Network (Client) Access > Group Policies om een intern groepsbeleid te creëren clientgroup. In het General tabblad selecteert

u de SSL VPN Client vink dit selectievakje aan om WebVPN als tunnelprotocol in te schakelen.

are re-	flare:	hgroup	
Nances Barner:	Barrer:	net	
	SCEP forwarding URL	then:	
	Address Pools	ne:	Ered
	3PV6 Address Pools	ne:	Seed
	More Options		
	Turneling Protocoku	Thread Electronics service is service and the service in the servi	ve 🗏 Latentese

In het Advanced > Split Tunneling tabblad kiest u Tunnel All Networks van de vervolgkeuzelijst Beleid van het Beleid om alle pakketten van de verre PC door een veilige tunnel te maken.

General Sciences	The VEN client makes split humaling decisions on the basis of a network list that can be specified below by providing the proper parameters to Policy and Vetwork list Reids.	
Ateaned	DNS Name (iii) Lifent	
BRONGLETTYCEY	Polog: I'l Ishani.  Famil Al Notourla	[]
H Prec(REv1) Clent	Pactwork Luci: 10/ Infunt	+ Panaga

#### Equivalente CLI-configuratie:

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policyclientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelall

6. Kiezen Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add OM een nieuwe

gebruikersaccount aan te maken ssluser1. Klik ok en vervolgens Apply.

PN Policy	Therease wheel					
	VALUE					
	Pastword and a second s					
	Garfin Passend *******					
	FIGer automicated using MSCH8P					
	Factors reactions Section at this profiles below to reduct AVDM, VOI, Tablet and Console acress.					
	Note: Allocers have individe access, reporties of these settings.					
	B Difference/CON, 731, Television (console)					
	Privilege levels used with command authorization.					
	Privlege (evel: 2 👻					
	💮 OL Kingin prompt han 55H, Telefet and console (ino (630H access)					
	This setting is effective only if "ase authentication http:console LOCAL" command is configured.					
	() No ASDA, 33H, Telnet or Consele access					
	The setting is offsective only if "ass authentication http:conside LOCK." and "ass authentication excert converte are configured.					

#### Equivalente CLI-configuratie:

ciscoasa(config)#username ssluser1 password asdmASA@

7. Tunnelgroep configureren. Kiezen Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add *om een nieuwe tunnelgroep te creëren* ssigroup. *In het* Basic tabblad kunt u de lijst met configuraties uitvoeren zoals aangegeven: Geef de tunnelgroep een naam als ssigroup. Onder Client Address Assignment, kies de adrespool vpnpool van de Client Address Pools (Functie). Onder Default Group Policy, kies het groepsbeleid clientgroup van de Group Policy (Functie).

asic	Name: sslgroup	
dvanced	Aliases:	
	Authentication	
	Method: 💿 AAA 💿 Certific	ate 🖱 Both
	AAA Server Group: LOCAL	✓ Manage
	Use LOCAL if Ser	ver Group fails
	Client Address Assignment	
	DHCP Servers:	
	None O DHCP	Link 💿 DHCP Subnet
	Client Address Pools: vpnpcol	Select
	Client IPv6 Address Pools:	Select
	IPv6 address pool is o	inly supported for SSL.
	Default Group Policy	
	Group Policy: Clientgroup	✓ Manage

In het Advanced > Group Alias/Group URL tabblad specificeert u de naam van de groep als ssigroup\_users en klik op OK. Equivalente CLI-configuratie:

ciscoasa (config) **#tunnel-group** sslgroup type remote-access ciscoasa (config) **#tunnel-group** sslgroup general-attributes ciscoasa (config-tunnel-general) **#address-pool** vpnpool ciscoasa (config-tunnel-general) **#default-group-policy** clientgroup ciscoasa (config-tunnel-general) **#exit** ciscoasa (config) **#tunnel-group** sslgroup webvpn-attributes ciscoasa (config) **#tunnel-group** sslgroup webvpn-attributes ciscoasa (config-tunnel-webvpn) **#group-alias** sslgroup\_users enable NAT configureren Kiezen Configuration > Firewall > NAT Rules > Add "Network

8. NAT configureren Kiezen Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule zodat het verkeer dat van het binnennetwerk komt met buiten IP adres 172.16.1.1 kan worden vertaald.

File View Tools Wizards Wind	low Help				
Home 🗞 Configuration 🔯 Mo	nitaring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 He	de l			
Device List di 4 X	Configuration > Firewall > NAT Rules				D
🗣 Add 📋 Delete 🚿 Connect	🗣 Add - 🕑 Edt 👔 Delete 🎓 🗳 👗 📴 📖 - 🔍 Fix	i 🖽 Diagram 🯹 i	Padiet Trace		
Find: Go	Add NAT Rule Before "Network Object" NAT Rules		Action: Translated Packet		
172.31.245.74:8443	Add "Network Object" NAT Rule	Service	Source	Destination	Service
	Add NAT Rule After "Network Object" NAT Rules	Stany	Original (5)	Original	Original
	👲 Insert	i any	Original (5)	Original	Original
firewall ਰ P	🐺 Insert After	-			
Control of the second s					

lame:	obj-inside	
Туре:	Network	•
P Address:	10.77.241.128	
Vetmask:	255.255.255.192	•
Description:		
NAT	۸	Ŋ
NAT Add Auto Type:	omatic Address Translation Rules	
NAT Add Auto Type: Translated	omatic Address Translation Rules          Dynamic <ul> <li>Addr:</li> <li>outside</li> <li> </li></ul>	

*Kiezen* Configuration >

Firewall > NAT Rules > Add "Network Object" NAT Rule zodat het verkeer dat VPN-verkeer dat van het buitennetwerk komt, met het buitenste IP-adres 172.16.1.1 kan worden vertaald.

Network	1
	<b>T</b>
192.168.10.0	
255.255.255.0	-
matic Address Translation Rules	
Addr: outside	
ough to interface PAT(dest intf): inside	
Advanced	
	192.168.10.0         255.255.255.0         matic Address Translation Rules         Dynamic PAT (Hide) ↓         Addr:       outside         output to interface PAT(dest intf):       inside         Advanced

#### configuratie:

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

#### ASA release 9.1(2) configuratie in de CLI

```
ciscoasa(config)#show running-config
```

```
: Saved
.
ASA Version 9.1(2)
1
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
```

security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address

#### !

passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate 3:00:00 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 uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list class-map inspection\_default match default-inspection-traffic 1 1 policy-map type inspect dns preset\_dns\_map parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns preset\_dns\_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global\_policy global webvpn enable outside

!--- Enable WebVPN on the outside interface

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

tunnel-group sslgroup general-attributes
address-pool vpnpool

!--- Associate the address pool vpnpool created

default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup\_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#

Communicatie tussen AnyConnect VPN-clients met de TunnelAll-configuratie toestaan op zijn plaatsNetwerkdiagram



Als communicatie tussen AnyConnect Clients vereist is en de NAT voor Public Internet op een Stick aanwezig is; een handmatige NAT is ook nodig om bidirectionele communicatie mogelijk te maken.Dit is een veelvoorkomend scenario wanneer AnyConnect Clients telefoonservices gebruiken en elkaar moeten kunnen bellen.ASA release 9.1(2) configuraties met ASDM release 7.1(6)Kiezen Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules dus het verkeer dat afkomstig is van het buitennetwerk (AnyConnect Pool) en bestemd is voor een andere AnyConnect-client uit dezelfde pool wordt niet vertaald met het buitenste IP-adres 172.16.1.1.

File View Tools Wizards Window	w Help				
Home Configuration 👩 Moni	taring 🔲 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help	1			
Device List 🗗 🖗 🗡	Configuration > Firewall > NAT Rules				0
🌩 Add 🗻 Delete 🚿 Connect	🗣 Add 🔹 📑 Edk 🗻 Delete   🕈 🗲   👗 🗞 🛝 -   Q, Find	🖭 Diagram 🏹	Packet Trace		
Find: Go	Add NAT Rule Before "Network Object" NAT Rules	Action: Translated Packet			
	Add "Network Object" NAT Rule         Add NAT Rule After "Network Object" NAT Rules	Service	Source	Destination	Service
		any any	Original (S)	Original	Original
	👷 Insert	any	Original (5)	Original	Original
Firewall - 4	This Insert After	. 🏟 any	Original (S)	- Original	- Original

Source Interface:	outside	Destination Interface:	outside	-
Source Address:	obj-AnyconnectPool (	Destination Address:	obj-AnyconnectPool	[
		Service:	any	
Action: Translated	Packet			
Source NAT Type:	Static	•		
Source Address:	obj-AnyconnectPool (		obj-AnyconnectPool	
Fall through to	interface PAT	Service:	Original	
Options				
📝 Enable rule				
Translate DNS	replies that match this rule			
)irection: Both				

#### Equivalente CLI-configuratie:

nat (outside, outside) source static obj-AnyconnectPool obj-AnyconnectPool destination static obj-AnyconnectPool obj-AnyconnectPool ASA release 9.1(2) configuratie in de CLI ciscoasa(config)#show running-config : Saved

```
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
```

no ip address

passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined to another Client within the same pool does not get translated.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
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 uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
1
class-map inspection_default
match default-inspection-traffic
1
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
1
service-policy global_policy global
webvpn
enable outside
```

```
!--- Enable WebVPN on the outside interface
```

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

```
group-policy clientgroup internal
```

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients. username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

tunnel-group sslgroup general-attributes
address-pool vpnpool

!--- Associate the address pool vpnpool created

default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup\_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end ciscoasa(config)# Communicatie tussen AnyConnect VPN-clients met splitter-tunnel toestaanNetwerkdiagram



Als communicatie tussen AnyConnect-clients is vereist en een Split-Tunnel wordt gebruikt; geen handmatige NAT is vereist om bidirectionele communicatie toe te staan tenzij er een NAT-regel is die dit geconfigureerde verkeer beïnvloedt. De AnyConnect VPN-pool moet echter worden opgenomen in de ACL van de splitter-tunnel.Dit is een veelvoorkomend scenario wanneer AnyConnect Clients telefoonservices gebruiken en elkaar moeten kunnen bellen.ASA release 9.1(2) configuraties met ASDM release 7.1(6)

1. Kiezen Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add om een IP-adresgroep te maken vpnpool.

Name:	vpnpool	
Starting IP Address:	192.168.10.1	
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	•

- 2. Klik Apply. Equivalente CLI-configuratie:
- ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
- 3. Web VPN inschakelen. Kiezen Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles en onder Access Interfaces klikt u op de selectievakjes Allow Access en Enable DTLS voor de buiteninterface. Controleer ook het Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below controledoos om SSL VPN op de buiteninterface toe te laten.

The security ap administrative r options. cess Interfaces Interfaces SSL access mus	plance automatically dep ights. The Cisco AnyCon	oloys the Cisco AnyCon nect VPN Client support t access on the interfac AnyConnect client to b	ect VPN Client to remot s IPsec (IKEv2) tunnel a es selected in the table i e launched from a brows	e users upon connection. The initial s well as SSL tunnel with Datagram pelow ser (Web Launch) .	dient deployment requires end-user Transport Layer Security (DTLS) tunneling
	SSI Access		IPsec (IKEv2) Acce	155	
	JUL MUL635				
Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate
Interface outside	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate

Klik Apply.Kiezen Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add om het Cisco AnyConnect VPN-clientbeeld uit het flitsgeheugen van ASA toe te voegen zoals aangegeven op de afbeelding.

Jpload a file from local o Please wait for the oper	computer to flash file system on the device. The upload process min ation to finish.	ght take a few minutes.
Local File Path:	C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg	Browse Local Files
Flash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash

AnyConnect Image:	anyconnect-win-3.1.05152-k9.pkg			Browse Flash
				Upload
Regular express	on to match use	er-agent		*

### Equivalente CLI-configuratie:

ciscoasa(config)# <b>webvpn</b>
ciscoasa(config-webvpn)# <b>enable outside</b>
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)# <b>tunnel-group-list enable</b>
ciscoasa(config-webvpn)# <b>anyconnect enable</b>

4. Groepsbeleid configureren. Kiezen Configuration > Remote Access VPN > Network (Client) Access > Group Policies om een intern groepsbeleid te creëren clientgroup. In het General tabblad selecteert u de SSL VPN Client vink dit selectievakje aan om WebVPN als toegestane tunnelprotocol in te schakelen.

	flars:	intgroup	
hances	Barrer:	(imen:	
	SCEP forwarding URL)	(Ime:	
	Address Pools	gene:	Eest
	3PV6 Address Pools	()mex	 Seet

In het Advanced > Split Tunneling tabblad kiest u Tunnel Network List Below van de vervolgkeuzelijst Beleid om alle pakketten te maken van de externe pc via een beveiligde tunnel.

Ment -	365Nenes: 💽 Intert		
Browerer Proof	Elityi Elitterit Tunna Nativatis	List Delon	-
'y Connect Client Sep(IREv1) Client	Network List: 1 Interit SPLID-ACL		<ul> <li>✓ Mar</li> </ul>
	Presing Unstance to set up split on Law	🖬 ACI Manager —	22
	Set up Oplit Curtier on for Web Cenadry	burnland 4. Terrested and	
	Intercept DHCP Configuration Mea	● Add + 図 tok 目 Debte + 4   5 % (8 - )	
		No Address Action Description	
		[1] 2015-07     [2] 2017-0210.0[29	

#### Equivalente CLI-configuratie:

ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policy clientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL

5. Kiezen Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add Om een nieuwe

gebruikersaccount aan te maken ssluser1. Klik OK en vervolgens Apply.

VPN Policy	linemane: echaer1				
	Factored message				
	Carline Research				
	F User automicated using MSCHAP				
	Aucos Kolinduar				
	Select one of the optime below to reduct 2.500, 750, Televilla errors.				
	Note: All users have indoned actions, regardless of these solutions.				
	Bullaccess(JSDN, 524, Tehet and Console)				
	Privlage level sugget with command authorization.				
	Privlege lowel: 2				
	O Lliogin prompt for 594, Telet and console (no ASDPI access)				
	This setting is effective only it "ase suthenlikation http:consile LOCIA." command is configured.				
	🛞 Na ASDA, 334, Tulnat or Connels accass				
	This setting is effective only if "ana authentication http:conede.LOCAL" and "ana authentication ecce."commands are configured.				

#### Equivalente CLI-configuratie:

ciscoasa(config)#username ssluser1 password asdmASA@

6. Tunnelgroep configureren. Kiezen Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add *Om een nieuwe tunnelgroep te creëren* ssigroup. *In het* Basic tabblad kunt u de lijst met configuraties uitvoeren zoals aangegeven: Geef de tunnelgroep een naam als ssigroup. Onder Client Address Assignment, kies de adrespool vpnpool van de Client Address Pools (Functie). Onder Default Group Policy, kies het groepsbeleid clientgroup van de Group Policy (Functie).

Basic	Name:	ssigroup	
Advanced	Aliases:		
	Authentication		- 199
	Method:	💿 AAA 💿 Certificate 💿 Both	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	
	Client Address Assignment		
	DHCP Servers:		
		None OHCP Link OHCP Subnet	
	Client Address Pools:	vpnpool	Select
	Client IPv6 Address Pool	s:	Select
		IPv6 address pool is only supported for SSL.	
	Default Group Policy		- 22
	Group Policy:	[clientgroup]	Manage

In het Advanced > Group Alias/Group URL tabblad specificeert u de naam van de groep als ssigroup\_users en klik op ok. Equivalente CLI-configuratie:

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

#### ASA release 9.1(2) configuratie in de CLI ciscoasa (config) #show running-config

```
: Saved
ASA Version 9.1(2)
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
interface Management0/0
shutdown
no nameif
no security-level
no ip address
```

```
!
passwd 2KFQnbNIdI.2KYOU encrypted
```

boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

*!--- Standard Split-Tunnel ACL that determines the networks that should travel the Anyconnect tunnel.* 

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN Clients

no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

*nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool* 

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool

object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate 3:00:00 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 uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat

threat-detection statistics access-list 1 class-map inspection\_default match default-inspection-traffic ! ! policy-map type inspect dns preset\_dns\_map parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns preset\_dns\_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global\_policy global webvpn enable outside

!--- Enable WebVPN on the outside interface

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

group-policy clientgroup internal

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1"

tunnel-group sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as remote access

tunnel-group sslgroup general-attributes
address-pool vpnpool

!--- Associate the address pool vpnpool created

default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup\_users enable

!--- Configure the group alias as sslgroup-users

```
prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

## VerifiërenGebruik deze sectie om te controleren of uw configuratie goed werkt.

• show vpn-sessiondb svc - Hiermee wordt de informatie over de huidige SSL-verbindingen weergegeven.

ciscoasa#**show vpn-sessiondb anyconnect** 

Session Type: SVC

Username : ssluser1 Index : 12 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : Clientless SSL-Tunnel DTLS-Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none

• show webvpn group-alias - Hier wordt het geconfigureerde alias voor verschillende groepen weergegeven.

ciscoasa#**show webvpn group-alias** Tunnel Group: **sslgroup** Group Alias: **sslgroup\_users enabled** 

• Kies in ASDM Monitoring > VPN > VPN Statistics > Sessions om de huidige zittingen in de ASA te



**Problemen oplossen**Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

• vpn-sessiondb logoff name - Opdracht om de SSL VPN sessie af te loggen voor de specifieke gebruikersnaam.

ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y

ciscoasa#Called vpn\_remove\_uauth: success!
webvpn\_svc\_np\_tear\_down: no ACL
webvpn\_svc\_np\_tear\_down: no IPv6 ACL
np\_svc\_destroy\_session(0xB000)

U kunt ook de vpn-sessiondb logoff anyconnect opdracht om alle AnyConnect-sessies te beëindigen.

 debug webvpn anyconnect <1-255> - Biedt de real-time webvpn-gebeurtenissen om de sessie vast te stellen.

Ciscoasa#debug webvpn anyconnect 7

```
CSTP state = HEADER PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6, IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6, IPv4'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
... input: 'X-DTLS-Accept-Encoding: lzs'
```

```
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Accept-Encoding: lzs, deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
NO SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260 (mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
```

- Unable to initiate NAC, NAC might not be enabled or invalid policy
- Kies in ASDM Monitoring > Logging > Real-time Log Viewer > View om de real time gebeurtenissen te zien. Dit voorbeeld toont de sessieinformatie tussen de AnyConnect 192.168.10.1 en Telnet Server 10.2.2.2 in het internet via ASA

172	.16.1	.1.				
Real-1	ime Log View	NCT-				
10e 10	ols <u>Window</u>	e Lielp				
þ. Ræge	· Rt Copy	See Or d	hur   🚰 Color S	interape i 🎒 Cons	te Rule 📓 Show Ru	de 😟 Show Detaile 🔅 Balo
Hilla by:	ALL ST		2 - CA 8 - CA 4	- Bprite	en subtritor 웹 :	Slaw All mod
Time	Syring ID	Source IP	Source Port	Destination IP	Destination Port	Decapition
22:03:02	302013	292.368.33.1	6/1050	30.2.2.2	60	Built result of CP connection 406 for outside 202.366.10.1/54060 (172.16.1.1/54060)). CCAL solver (1) to outside 10.2.2.2(80) (10.2.2.2(80) (pluse 1)
22:03:02	305011	192.163.10.1	64059	172.35.1.1	64059	Built dynamic TCP translation from outside: (52, 168, 10, 1,64039), OCAL (souser i) to outside: (72, 35, 1, 1)(4159

## Gerelateerde informatie

- <u>Cisco ASA 5500-X Series-firewalls</u>
- PIX/ASA- en VPN-client voor openbaar internet VPN op een Stick Configuration-voorbeeld
- SSL VPN-client (SVC) op ASA met ASDM Configuration Voorbeeld
- 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.