# ASA/PIX: Remote VPN-server met Ininkomend NAT voor VPN-clientverkeer met CLI en ASDMconfiguratievoorbeeld

### Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Achtergrondinformatie Configuraties ASA/PIX configureren als een externe VPN-server met ASDM Configureer de ASA/PIX met NAT inkomend VPN-clientverkeer met ASDM Configureer als een externe VPN-server en voor inkomende NAT met CLI Verifiëren ASA/PIX security applicatie - show Opdrachten Problemen oplossen Gerelateerde informatie

## **Inleiding**

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) kunt configureren om op te treden als een externe VPN-server met behulp van Adaptieve Security Devices Manager (ASDM) of CLI en NAT in het inkomende VPN-clientverkeer. De ASDM levert veiligheidsbeheer en controle van wereldklasse door middel van een intuïtieve, makkelijk te gebruiken web-gebaseerde beheerinterface. Nadat de Cisco ASA-configuratie is voltooid, kan deze via de Cisco VPN-client worden geverifieerd.

## Voorwaarden

### Vereisten

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco ASDM of CLI in staat te stellen configuratiewijzigingen door te voeren. De ASA wordt ook verondersteld te zijn geconfigureerd voor uitgaande NAT. Raadpleeg <u>Inside Hosts Toegang tot</u> <u>Outside Networks met het gebruik van PAT</u> voor meer informatie over het configureren van uitgaande NAT. **Opmerking:** Raadpleeg <u>HTTPS-toegang voor ASDM</u> of <u>PIX/ASA 7.x: SSH in het Voorbeeld van de</u> <u>configuratie van binnen en buiten</u> om het apparaat extern te kunnen configureren door de ASDM of Secure Shell (SSH).

#### Gebruikte componenten

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

- Cisco adaptieve security applicatie, versie 7.x en hoger
- Adaptieve Security Adapter Manager versie 5.x en hoger
- Cisco VPN-clientversie 4.x en hoger

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.

#### Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX security applicatie versie 7.x en hoger.

#### **Conventies**

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

### **Achtergrondinformatie**

Remote-toegangsconfiguraties bieden beveiligde externe toegang voor Cisco VPN-clients, zoals mobiele gebruikers. Een VPN-toegang op afstand stelt externe gebruikers in staat om veilig toegang te krijgen tot gecentraliseerde netwerkbronnen. De Cisco VPN-client voldoet aan het IPSec-protocol en is specifiek ontworpen om met het security apparaat te werken. Het security apparaat kan echter wel IPSec-verbindingen maken met veel klanten die aan het protocol voldoen. Raadpleeg de <u>ASA Configuration Guides</u> voor meer informatie over IPSec.

Groepen en gebruikers zijn kernconcepten in het beheer van de beveiliging van VPN's en in de configuratie van het security apparaat. Ze specificeren eigenschappen die de toegang van gebruikers tot en het gebruik van VPN bepalen. Een groep is een verzameling gebruikers die als één entiteit worden behandeld. Gebruikers krijgen hun eigenschappen van groepsbeleid. Tunnelgroepen identificeren het groepsbeleid voor specifieke verbindingen. Als u geen bepaald groepsbeleid aan gebruikers toewijst, is het standaard groepsbeleid voor de verbinding van toepassing.

Een tunnelgroep bestaat uit een reeks records die tunnelverbindingsbeleid bepalen. In deze registers worden de servers geïdentificeerd waarop de tunnelgebruikers zijn geauthentiseerd, evenals de eventuele boekhoudkundige servers waarop de verbindingsinformatie wordt verzonden. Ze identificeren ook een standaardgroepsbeleid voor de verbindingen, en ze bevatten protocol-specifieke verbindingsparameters. Tunnelgroepen omvatten een klein aantal eigenschappen die verband houden met de totstandbrenging van de tunnel zelf. Tunnelgroepen bevatten een muiswijzer op een groepsbeleid dat gebruikersgeoriënteerde eigenschappen definieert.

## **Configuraties**

#### ASA/PIX configureren als een externe VPN-server met ASDM

Voltooi deze stappen om Cisco ASA als een externe VPN-server met ASDM te configureren:

1. Open uw browser en voer https://<IP\_Address van de interface van ASA in die is geconfigureerd voor ASDM Access>om toegang te krijgen tot de ASDM in de ASA.Controleer of alle waarschuwingen die uw browser u geeft, behoren tot de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De ASA presenteert dit venster om het downloaden van de ASDM-toepassing mogelijk te maken. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-applet.



- 2. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDMtoepassing te downloaden.
- 3. Voltooi na het downloaden van de ASDM Launcher de stappen die door de aanwijzingen zijn geleid om de software te installeren en de Cisco ASDM Launcher uit te voeren.
- 4. Voer het IP-adres in voor de interface die u met de http opdracht en een gebruikersnaam en wachtwoord hebt ingesteld als u er een hebt opgegeven.Dit voorbeeld gebruikt cisco123 als de gebruikersnaam en cisco123 als het

	🕵 Cisco ASDM Launch	er v1.5(30)	
		SDM Launcher	cisco
	Device IP Address / Name:	10.77.241.111	<b>*</b>
	Username:	cisco123	
	Password:	* * * * * * *	
	📃 Run in Demo Mode		
wachtwoord.		μζ	1

5. Selecteer Wizard > IPsec VPN-wizard in het Home

	G Cisco ASDM 6.1 for ASA - 10.77.241.111								
	File	View	Tools	Wiz	ards	Window	Help		
	Home & Cor Device List Add Delete 10.77.241.10 10.77.241.1		_	Star	tup Wizaro	ł		-	
				IPse	ec VPN Wiza	ard	N		
			t i	-	551	VPN Wizarı	d	1.5	
				Hiat	Availabiliti	u and 9	calability Wizard		
				nigi	I AVAIIADIIIC	y anu s			
venster.				Pac	ket Capture	e Wizar	d		

6. Selecteer het tunneltype **Remote Access** VPN en zorg ervoor dat de VPN-tunnelinterface naar wens wordt ingesteld en klik op **Volgende** zoals hier wordt weergegeven.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Br	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type: Site-to-Site VPN
THE HAR	Site-to-Site
	Remote Access
	VPN Tunnel Interface:       Outside         Image: Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

 Het VPN-clienttype is geselecteerd, zoals wordt weergegeven. Cisco VPN-client is hier geselecteerd. Klik op Volgende.

🖆 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
Brandt	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
	VPN Client Type:
Home	Cisco VIII Clent, Delease 2 y or higher :
Corporate Network	or other Easy VPN Remote product
cuto .	or other basy why remote product
THE THE	Microsoft Windows client using L2TP over IPsec
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
- THUM	PAP V CHAP V MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the client will send tunnel group name as - username@tunnelgroup.
- A-	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

 Voer een naam in voor de naam van de tunnelgroep. Voer de te gebruiken authenticatieinformatie in, de vooraf gedeelde sleutel in dit voorbeeld. De pre-gedeelde sleutel die in dit voorbeeld wordt gebruikt is cisco123. De naam van de Tunnelgroep die in dit voorbeeld wordt gebruikt is cisco. Klik op Volgende.

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Br	The ASA allows you to group remote access tunnel users based on common connection parameters and clent attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote clent.   Authentication Method <ul> <li>Pre-shared key</li> <li>Pre-Shared Key:</li> <li>clscol23</li> </ul> <ul> <li>Certificate</li> <li>Certificate Signing Algorithm: rsa-sig</li> <li>Certificate Name:</li> <li>Challenge/response authentication (CRACK)</li> </ul>
	< Back Next > Finish Cancel Help

9. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep. Opmerking: U voegt gebruikers in stap 10 toe aan de lokale gebruikersdatabase. Opmerking: Raadpleeg <u>PIX/ASA 7.x-groepen voor verificatie en</u> <u>autorisatie van VPN-gebruikers via het ASDM Configuration Voorbeeld</u> voor informatie over de configuratie van een externe AAA-servergroep met ASDM.

💼 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Bandh Bra	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
	< Back Next > Finish Cancel He	P

10. Geef een gebruikersnaam en optioneel wachtwoord op en klik op Toevoegen om nieuwe gebruikers toe te voegen aan de gebruikersverificatiedatabase. Klik op Volgende.N.B.: Verwijder bestaande gebruikers niet uit dit venster. Selecteer Configuratie > Apparaatbeheer > Gebruikers/AAA > Gebruikersrekeningen in het hoofdvenster van ASDM om bestaande items in de database te bewerken of deze uit de database te verwijderen.

🖆 VPN Wizard		E
VPN Wizard	User Accounts (Step 5 of 11)	
	Add new users into the user authentic or to remove them from the database Users/AAA > User Accounts in the ma	cation database. To edit existing entries in the database , go to Configuration > Device Management > in ASDM window.
Home	User to Be Added	
Corporate Network	Username:	disco123
	cisco	Add >>
	•••••	Delete
THINK	Confirm Password (optional):	
-6	•••••	
	L]	
		< Back Next > Finish Cancel Help

11. Om een pool van lokale adressen te definiëren die dynamisch aan externe VPN-clients moet worden toegewezen, klikt u op **Nieuw** om een nieuwe **IP-pool** te maken.

🖆 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP Horne Corporate Nativark	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients. Tunnel Group Name : cisco	
THE REAL PROPERTY OF	Pool Name: New	
	Range End Address: Subnet: Mask:	
	< Back Next > Finish Cancel Help	2

12. Typ deze informatie in het nieuwe venster Add IP Pool en klik op OK.Naam van de IPpoolIP-adres startenIP-adres

Name:	vpnpool
Starting IP Address:	192.168.1.1
Ending IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0

#### beëindigenSubnetmasker

13. Nadat u de pool van lokale adressen definieert die dynamisch aan externe VPN-clients moeten worden toegewezen wanneer ze worden aangesloten, klikt u op **Volgende.** 

🖆 VPN Wizard		$\mathbf{X}$
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP Home	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporate Network	Tunnel Group Name : cisco	
THE THE	Pool Name: vpnpool 🖌 New	
	Pool Settings	
THURING	Range Start Address: 192.168.1.1	
- It - I'll	Range End Address: 192.168.1.254	
	Subnet Mask: 255.255.255.0	
		J
	< Back Next > Finish Cancel Help	

14. *Optioneel:* Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional)	(Step 7 of 11)
Brandi Brandi	Attributes you configure below are push ASA. If you do not want an attribute pu	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	cisco
Franke he	Primary DNS Server:	
	Secondary DNS Server:	
AT ALL	Primary WINS Server:	
T	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. Specificeer de parameters voor IKE, ook bekend als IKE Fase 1.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de client-

pc.

🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch Designed State Home	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Network	Encryption: DE5	
	Authentication: MD5	
	Diffie-Helman Group: 2	
	< Back Next Finish Cancel Help	2

 Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op Voltooien als u tevreden bent met de configuratie.



### Configureer de ASA/PIX met NAT inkomend VPN-clientverkeer met ASDM

Voltooi deze stappen om Cisco ASA aan NAT inkomend VPN-clientverkeer met ASDM te configureren:

1. Kies **Configuratie > Firewall > NAT-regels** en klik op **Toevoegen**. Selecteer in de vervolgkeuzelijst de optie **Dynamische NAT-regel** 



#### toevoegen.

 In het venster Dynamische NAT-regel toevoegen, kiest u Buitenkant als de interface en klikt u op de knop Bladeren naast het vak Bron.

🖾 Add	Dyna	mic NAT Rule		$\mathbf{X}$
Original Interf Sourc Translat Select	face: [ :e: [ ted — t a gloi	Outside bal pool for dynamic tr	anslation.	
Poo 0	l ID	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Conn	ectior	Settings	OK Cancel Help	*

3. Selecteer in het venster Bladeren Bron de juiste netwerkobjecten en kies ook de **bron** onder de sectie Geselecteerde Bron en klik op **OK**. Hier wordt de netwerkobject 192.168.1.0 geselecteerd.

📬 Browse Source				
🗣 Add 🗹 Edit 👔 De	elete Q			
Filter:				Filter Clear
Name	<sup>1</sup> IP Address	Netmask	Description	
Network Objects				
🗠 🏈 any	0.0.0.0	0.0.0.0		
📲 inside-network	172.16.1.0	255.255.255.	0	
🙀 Outside-netwo	rk 10.10.10.0	255.255.255.	0	
192.168.1.0	192.168.1.0	255.255.255.	0	
Selected Source				
Source -> 192.	168.1.0/24			
				Cancel

4. Klik op beheren.

r.	Add Dyna	amic NAT Rule		X
Or Tr	iginal Interface: Source: anslated —	Outside 192.168.0.0		
	Select a glo	bal pool for dynamic t	ranslation.	-
	Pool ID	Interface	Addresses Pool	
	0	(outbound)	Same as original address (identity)	
	0	(inbound)	Same as original address (identity)	Manage
1	onnectio	n Settings		8
			OK Cancel Help	

5. Klik in het venster Global Pool beheren op **Toevoegen**.

🕵 Manage Global Pool 🛛 🛛 🔀					
🖶 Add 🗹 Edit 💼 Delete					
Pool ID	Interface	Addresses Pool			
	ОК	Cancel Help			

6. Kies in het venster Global Address Pool binnendringen als de interface en 2 als de Pool ID. Zorg er ook voor dat de radioknop naast PAT met IP-adres van de interface is geselecteerd. Klik op Add>> en vervolgens op OK.

🞼 Add Global Address Pool		X
Interface: inside  Pool ID: 2		
IP Addresses to Add         Range         Starting IP Address:         Ending IP Address:         Netmask (optional):         IP Address:         IP Address:         Netmask (optional):         IP Address:         Netmask (optional):	Add >> << Delete	Addresses Pool  inside
Port Address Translation (PAT) using IP     Address of the interface	Cancel	Help

7. Klik op **OK** nadat u de globale pool met de **Pool ID 2** in de vorige stap hebt geselecteerd.

🕵 Add Dyn	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated -			
Select a glo	bal pool for dynamic	translation.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
2	inside	🚥, inside	Manage
			4
Connectio	n Settings		۲

8. Klik nu op **Toepassen** zodat de configuratie wordt toegepast op de ASA. Dit voltooit de configuratie.

Configura	Configuration > Firewall > NAT Rules					
💠 Add	🝷 📝 Edit 🎁 Dele	te 🛉 🗲 🖌 👗	🐚 🏨 - 🛛 🔍 Find 🗄	🔁 Diagram 🗐	Packet Trace	
	Turne	Original			Translated	
#	Туре	Source	Destination	Service	Interface	Addre:
🖬 Outsid	de (1 Dynamic rules)					
1	Dynamic	192.168.1.0/2	4		inside	🔤 insia
inside ⊡	(1 Exempt rules, 1 D	namic rules)				
1	🔁 Exempt	🌍 апу	192.168.1.0/24		(outbound)	
2	<b>Dynamic</b>	🌍 any			Outside	🎫 Out
						2
C See h	la braffic bhuarada bh a	لتحمينها ستكمينا	voss tuppelation			
			Appiy Reset	J		

### ASA/PIX configureren als een externe VPN-server en voor inkomende NAT met CLI

Config op het ASA-apparaat uitvoeren		
ciscoasa# <b>show running-config</b>		
: Saved		
ASA Version 8.0(3)		
!		
hostname ciscoasa		
enable password 8Ry2YjIyt7RRXU24 encrypted		
names		
!		
interface Ethernet0/0		
nameif Outside		
security-level 0		
ip address 10.10.10.2 255.255.255.0		
!		
interface Ethernet0/1		

nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 1 1 passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside\_nat0\_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-list inside\_nat0\_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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 no snmp-server location no snmp-server contact !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside\_map 65535 ipsec-isakmp dynamic SYSTEM\_DEFAULT\_CRYPTO\_MAP crypto map Outside\_map interface Outside crypto isakmp enable Outside !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and !---

Policy details are hidden as the default values are

```
chosen. crypto isakmp policy 10
authentication pre-share
 encryption des
hash sha
group 2
lifetime 86400
crypto isakmp policy 30
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
telnet timeout 5
ssh timeout 60
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
group-policy cisco internal
group-policy cisco attributes
vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 0
username cisco attributes
vpn-group-policy cisco
tunnel-group cisco type remote-access
tunnel-group cisco general-attributes
address-pool vpnpool
default-group-policy cisco
!--- Specifies the pre-shared key "cisco123" which must
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
policy-map type inspect dns migrated_dns_map_1
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns migrated_dns_map_1
 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
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#
```

## Verifiëren

Probeer via de Cisco ASA-client verbinding te maken met de Cisco ASA om te controleren of de ASA is geconfigureerd.

1. Klik op

NIEUW.						
VPN Client - Version 5.0.03.0530	👌 VPN Client - Version 5.0.03.0530 📃 🗖 🔀					
Connection Entries Status Certificates Log Options	; Help					
Connect News Import Modify	Delete		cisco			
Connection Entries Certificates Log						
Connection Entry	Host	Transport				
Not connected.						

 Vul de gegevens in van uw nieuwe aansluiting.Het veld Host moet het IP-adres of de hostnaam van de eerder geconfigureerd Cisco ASA bevatten. De informatie over de groepsverificatie moet overeenkomen met de informatie die in stap 4 wordt gebruikt. Klik op Opslaan als u klaar

VPN Client   Create New VPN Connection Entry	×
onnection Entry: MyVPNClient	
Description:	
Host: 10.10.10.2	
Authentication Transport Backup Servers Dial-Up	
Group Authentication	Authentication
Name: cisco	
Password: ******	
Confirm Password:	
<ul> <li>Certificate Authentication</li> <li>Name: </li> <li>Send CA Certificate Chain</li> </ul>	
rase User Password	Cancel
	VPN Client       Create New VPN Connection Entry         onnection Entry:       MyVPNClient         Description:       Host:         Host:       10.10.10.2         Authentication       Transport         Backup Servers       Dial-Up         Image:       cisco         Password:       Image:         Confirm Password:       Image:         Image:       Image: </td

3. Selecteer de nieuwe verbinding en klik op **Connect**.

Status: Disconnected   VPN Client - Version 5.	0.03.0530		
Connection Entries Status Certificates Log Options Help	)		
Confuct New Import Modify De Connection Entries Certificates Log	<b>K</b> lete		cisco
Connection Entry	Host	Transport	
MyvPhulient	10.10.10.2	IFSec/UUP	
Not connected.			

4. Voer een gebruikersnaam en wachtwoord in voor uitgebreide verificatie. Deze informatie moet overeenkomen met de informatie die in **stappen 5 en 6** is

VPN Client   User Authentication for "MyVPN	Client" 🛛 🔀				
The server has requested the following information to complete the user authentication.					
Username: cisco123 CISCO Password: *******					
	Cancel				

gespecificeerd.

5. Zodra de verbinding met succes is tot stand gebracht, kiest u **Statistieken** uit het menu Status om de details van de tunnel te controleren.

🤌 status: Connected   VI				
Connection Entries Status Ce	ertificates Log Options Help	0		
Disconnect N	tics Ctrl+S cations Ctrl+N		(1) CI	iniji. Isco
Connection Entries Reset	Stats			
Connection Entry	Δ	Host	Transport	
MyVPNClient		10.10.10.2	IPSec/UDP	
Connected to "MyVPNClient".		Connect	ed Time: 0 day(s), 00:00.36	▼ //

Dit venster toont informatie over verkeer en

Tunnel Details	Firewall	
Address Information Client: 192.168.1.1 Server: 10.10.10.2	<b>Connection Informatio</b> Entry: Time:	<b>n</b> MyVPNClient 0 day(s), 00:01.13
<b>Bytes</b> Received: 5412 Sent: 5416	<b>Crypto</b> Encryption: Authentication:	56-bit DES HMAC-MD5
Packets Encrypted: 39 Decrypted: 31 Discarded: 8 Bypassed: 22	<b>Transport</b> Transparent Tunneling Local LAN: Compression:	g:Inactive Disabled None
		Reset
		Close

venster wordt informatie over gesplitste tunneling weergegeven:

8	VPN Client	Statistics			X		
Tunnel Details Route Details Firewall							
Local LAN Routes		Secured Routes					
	Network	Subnet Mask	Network	Subnet Mask			
			0.0.0.0	0.0.0.0			
				Close			

#### ASA/PIX security applicatie - show Opdrachten

• toon crypto isakmp sa-toont alle huidige IKE SAs bij een peer.

```
Active SA: 1
     Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1
     IKE Peer: 10.10.10.1
 1
     Type : user
                               Role
                                        : responder
     Rekey
             : no
                               State
                                        : AM_ACTIVE

    toon crypto ipsec sa-Toont alle huidige IPsec SAs bij een peer.

 ASA#show crypto ipsec sa
 interface: Outside
     Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
 .10.2
       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
       current_peer: 10.10.10.1, username: cisco123
       dynamic allocated peer ip: 192.168.1.1
       #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
       #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C
    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
        slot: 0, conn id: 24576, crypto-map: SYSTEM DEFAULT CRYPTO MAP
         sa timing: remaining key lifetime (sec): 27255
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
        sa timing: remaining key lifetime (sec): 27255
        IV size: 8 bytes
        replay detection support: Y
ciscoasa(config)#debug icmp trace
!--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
2
!--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
len=32
ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
2
ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
```

### Problemen oplossen

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

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Raadpleeg de <u>meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing</u> voor meer informatie over de oplossing van problemen met de site-site VPN.

### Gerelateerde informatie

- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- <u>Cisco adaptieve security apparaatbeheer</u>
- <u>Cisco ASA 5500 Series adaptieve security applicaties, probleemoplossing en meldingen</u>
- Technische ondersteuning en documentatie Cisco Systems