ASA/PIX: Statische IP-adressering voor IPSec VPN-client met CLI en ASDM-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) moet configureren om het statische IP-adres naar de VPN-client te geven met de Adaptieve Security Devices Manager (ASDM) of CLI. 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 met de Cisco VPN-client worden geverifieerd.

Raadpleeg PIX/ASA 7.x en Cisco VPN-client 4.x met Windows 2003 IAS RADIUS (Against Active Directory) verificatievoorbeeld voor het instellen van de VPN-verbinding op afstand tussen een Cisco VPN-client (4.x voor Windows) en de PIX 500 Series security applicatie 7.x. De externe VPN-clientgebruiker authenticeert de actieve map aan de hand van een Microsoft Windows 2003-server voor internetverificatie (IAS) RADIUS.

Raadpleeg PIX/ASA 7.x en Cisco VPN-client 4.x voor Cisco Secure ACS-verificatie Configuratievoorbeeld om een VPN-verbinding op afstand in te stellen tussen een Cisco VPN-client (4.x voor Windows) en PIX 500 Series security applicatie 7.x met een Cisco Secure Access Control Server (ACS versie 3.2) voor uitgebreide verificatie (Xauth).

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.

Opmerking: Raadpleeg HTTPS-toegang voor ASDM of PIX/ASA 7.x: SSH in het Voorbeeld van de configuratie van binnen en buiten 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:

- Software voor Cisco adaptieve security applicatie, versie 7.x en hoger
- Adaptieve Security Office 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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

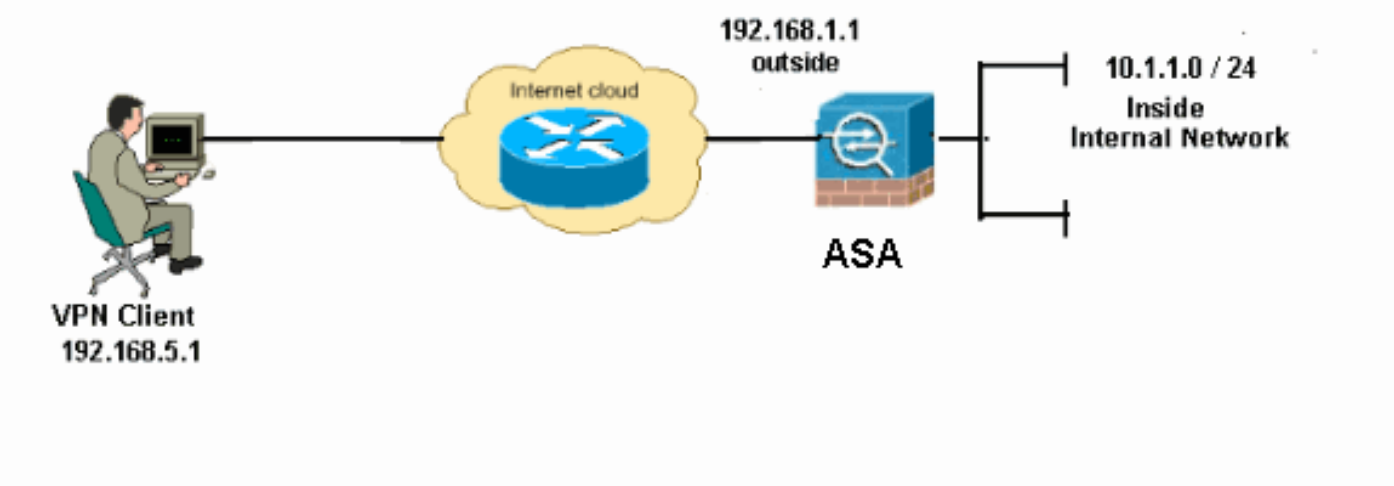
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



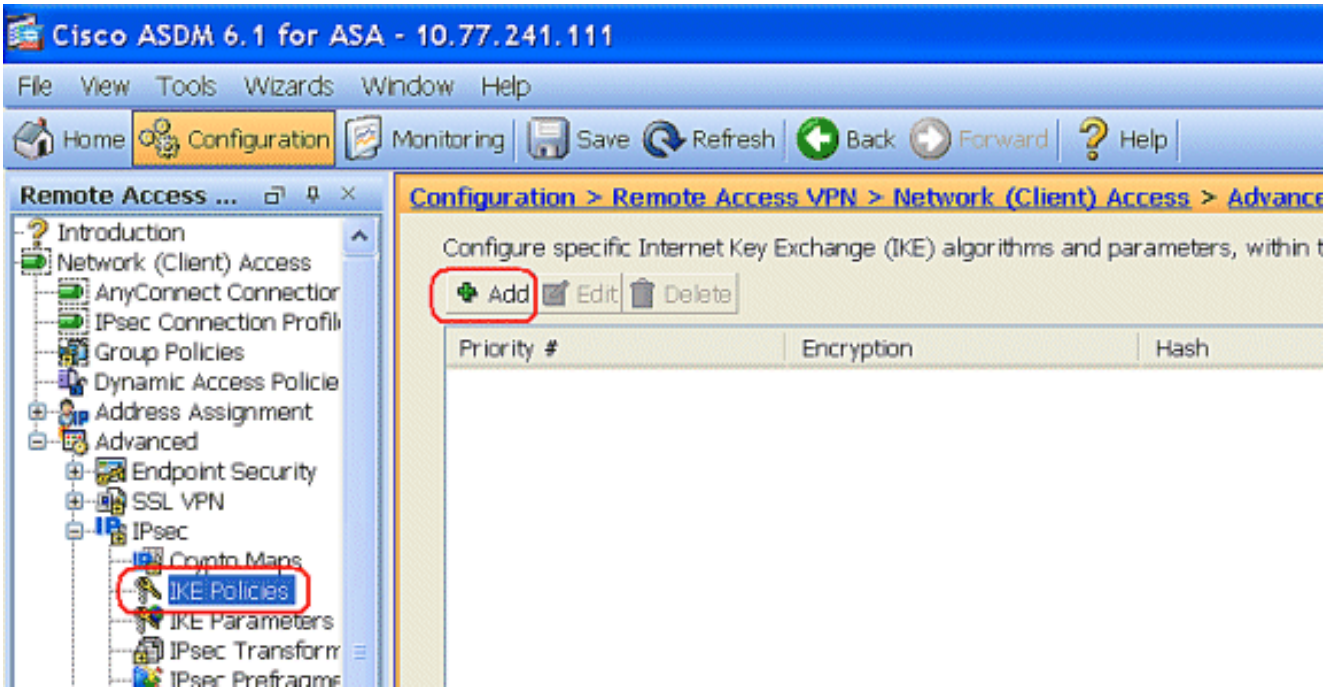
Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918-adressen, die werden gebruikt in een labomgeving.

Externe toegang instellen (IPSec)

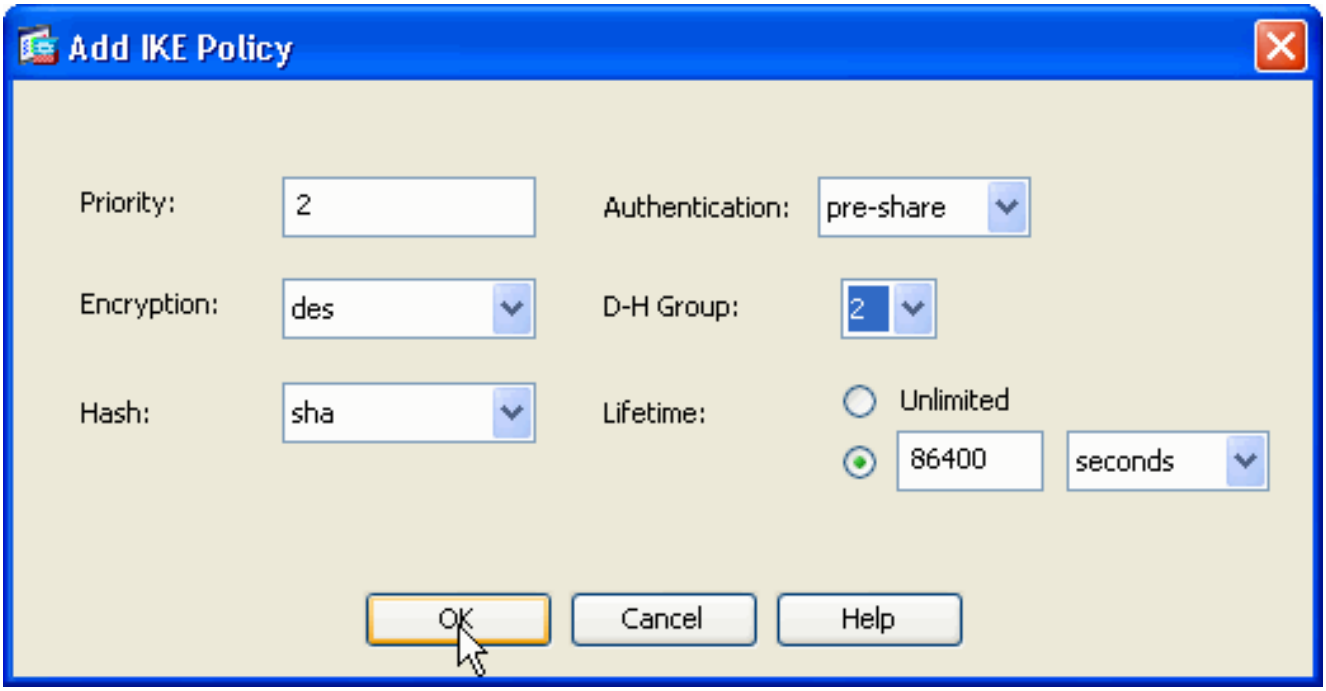
ASDM-procedure

Voltooi deze stappen om de externe VPN-toegang te configureren:

1. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-beleid > Add** om een ISAKMP-beleid te maken.

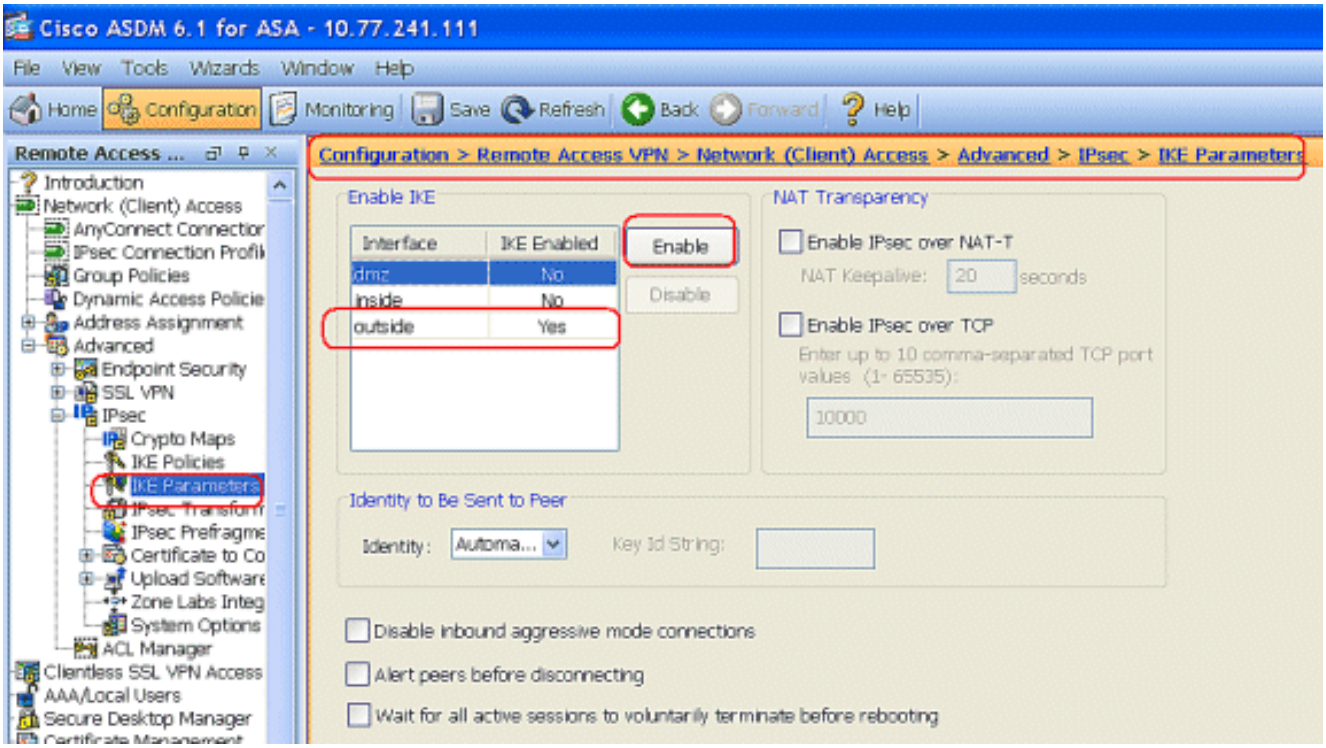


2. Geef de ISAKMP-beleidsdetails.

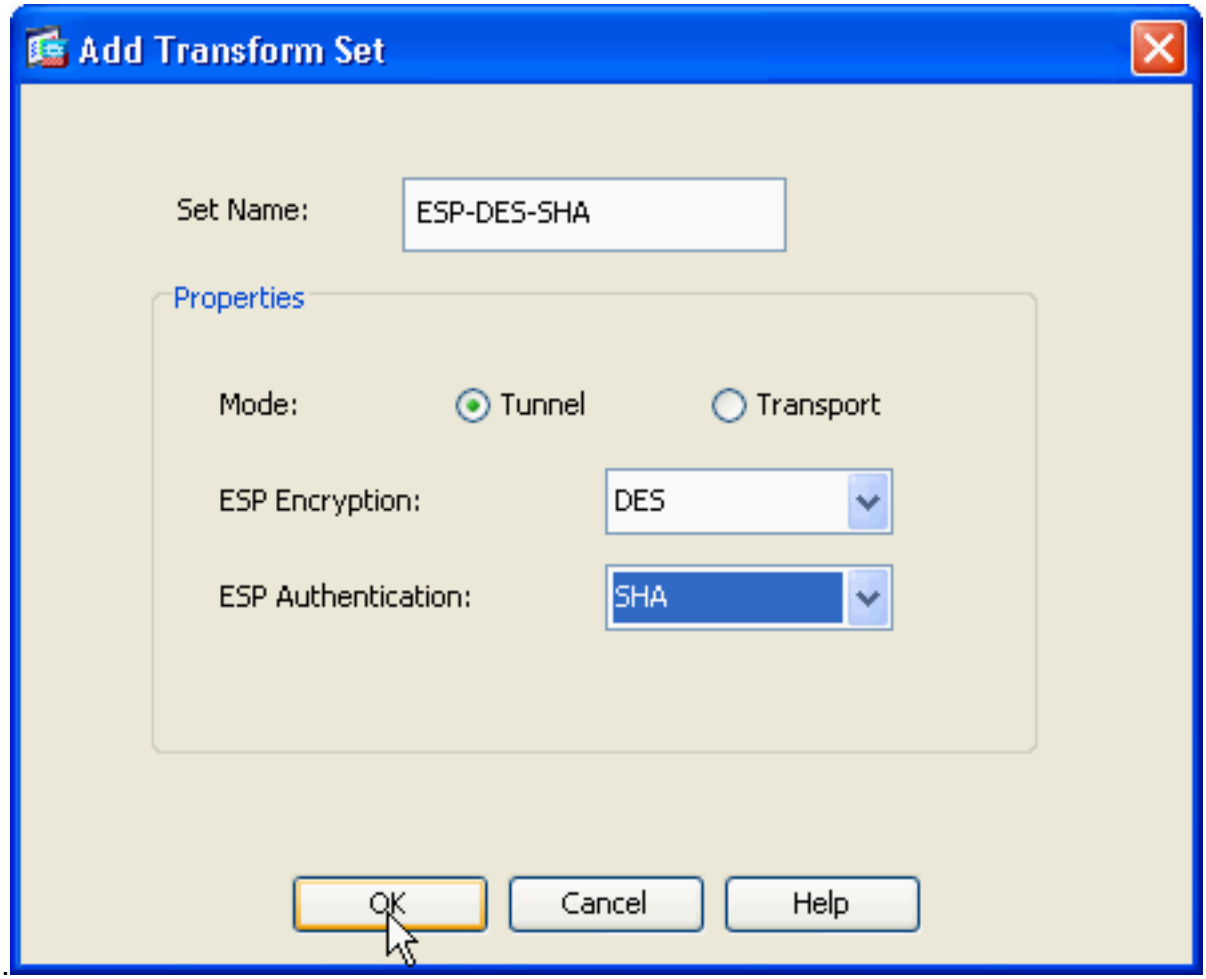


Klik op **OK** en **Toepassen**.

3. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-parameters** om IKE op de buiteninterface mogelijk te maken.

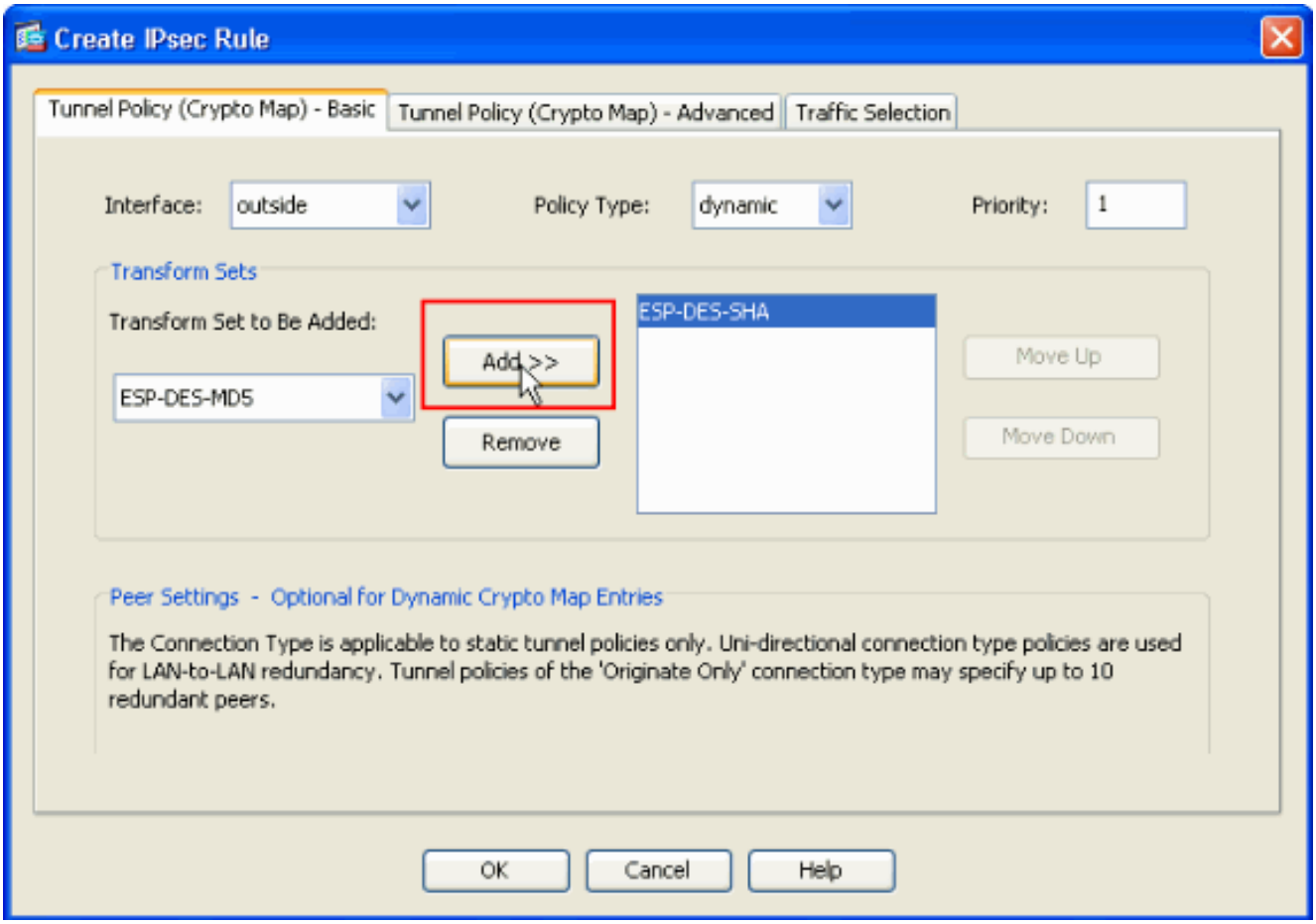


4. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transformatiesets > Add** om de **ESP-DES-SHA** transformatieset te maken, zoals



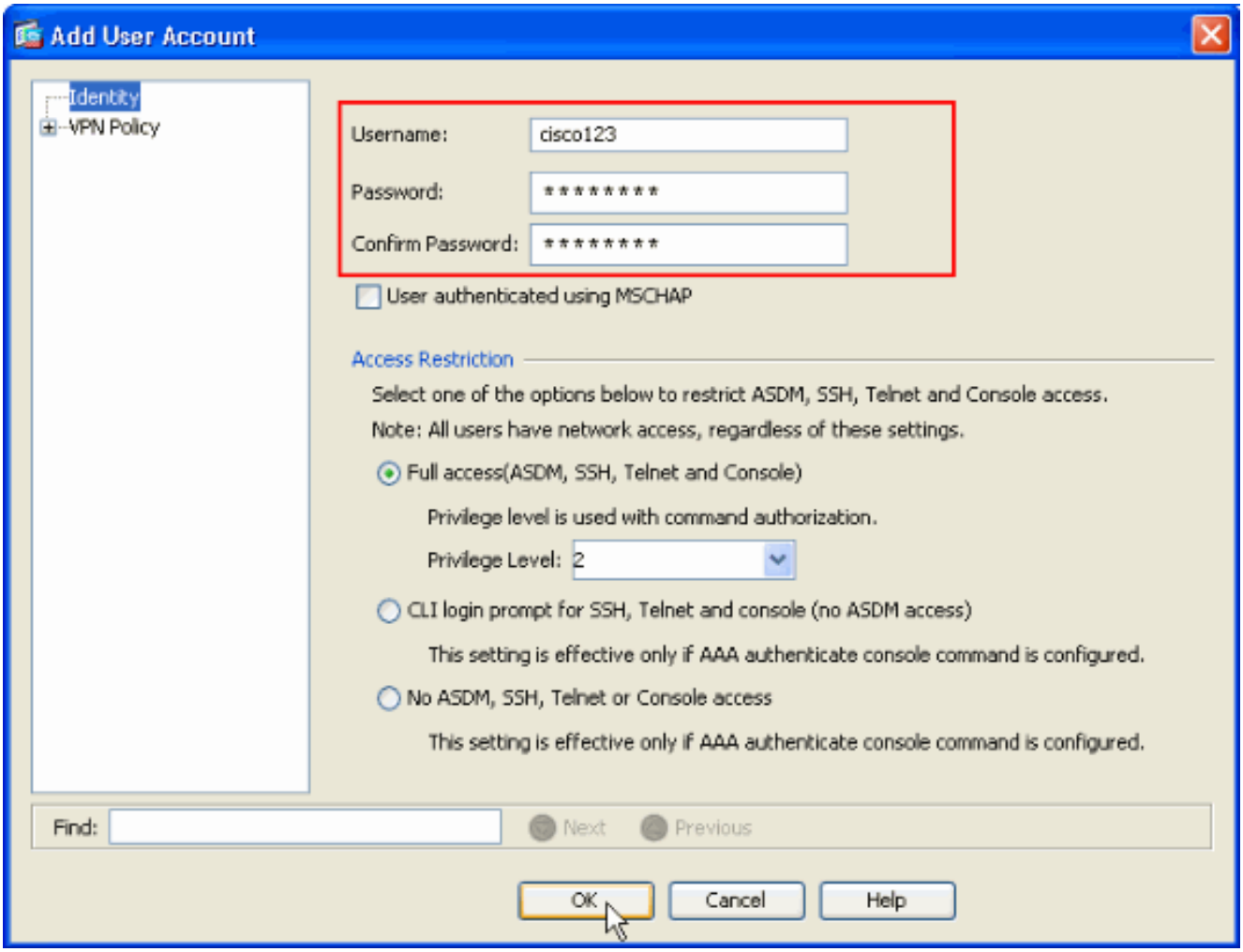
getoond.
Klik op **OK** en **Toepassen**.

5. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add** om een crypto-kaart te maken met dynamisch beleid van prioriteit 1, zoals
getoond.

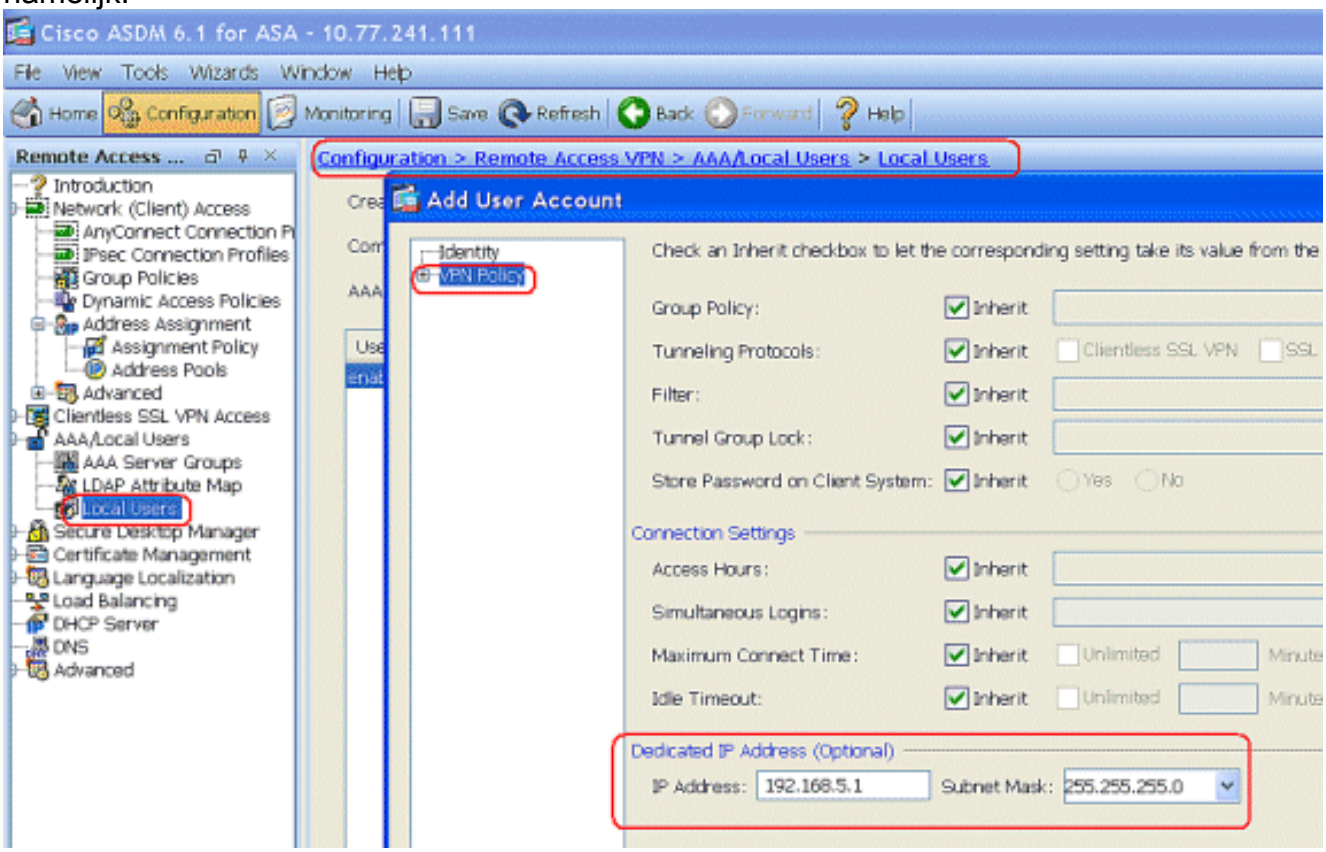


Klik op **OK** en **Toepassen**.

6. Kies **Configuration > Remote Access VPN > AAA-instelling > Local Gebruikers > Add** om de gebruikersaccount te maken (bijvoorbeeld gebruikersnaam - cisco123 en Wachtwoord - cisco123) voor VPN-clienttoegang.

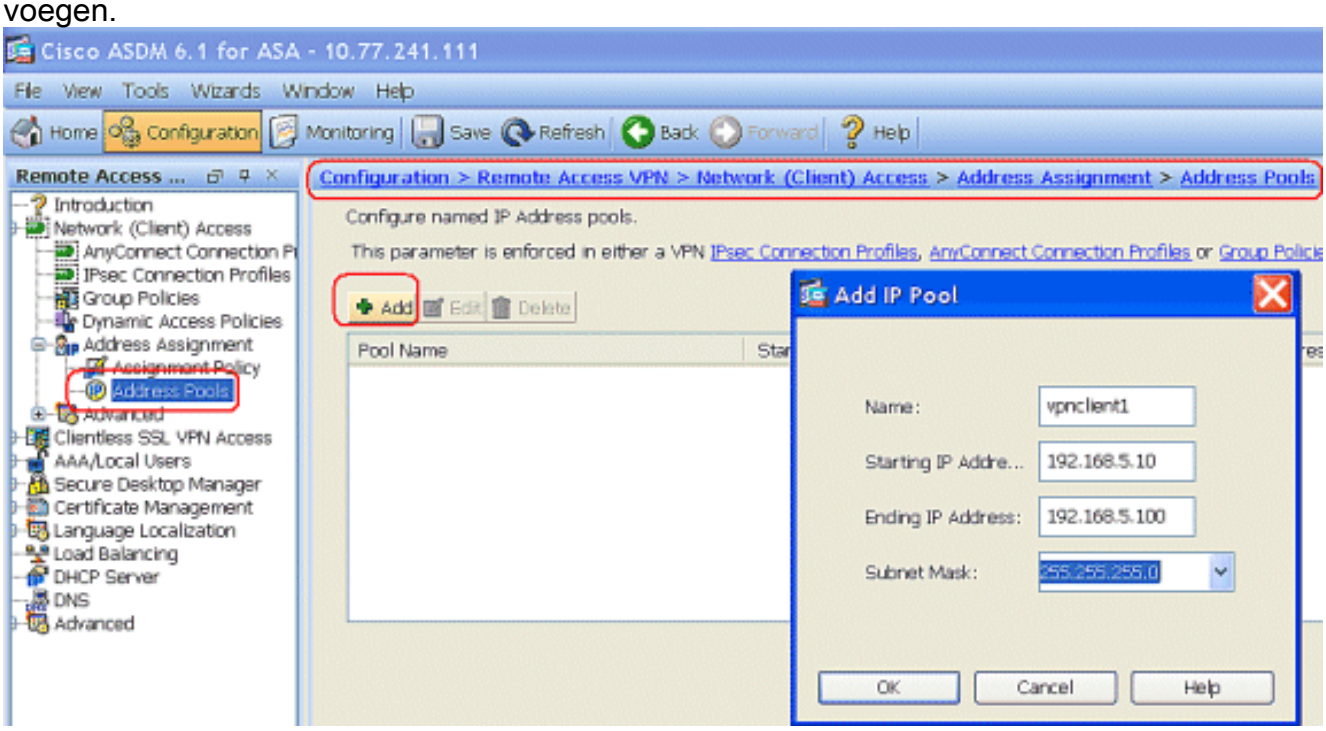


7. Ga naar **VPN-beleid** en voeg het **statische/speciale IP-adres** voor gebruiker "cisco123" toe, namelijk:

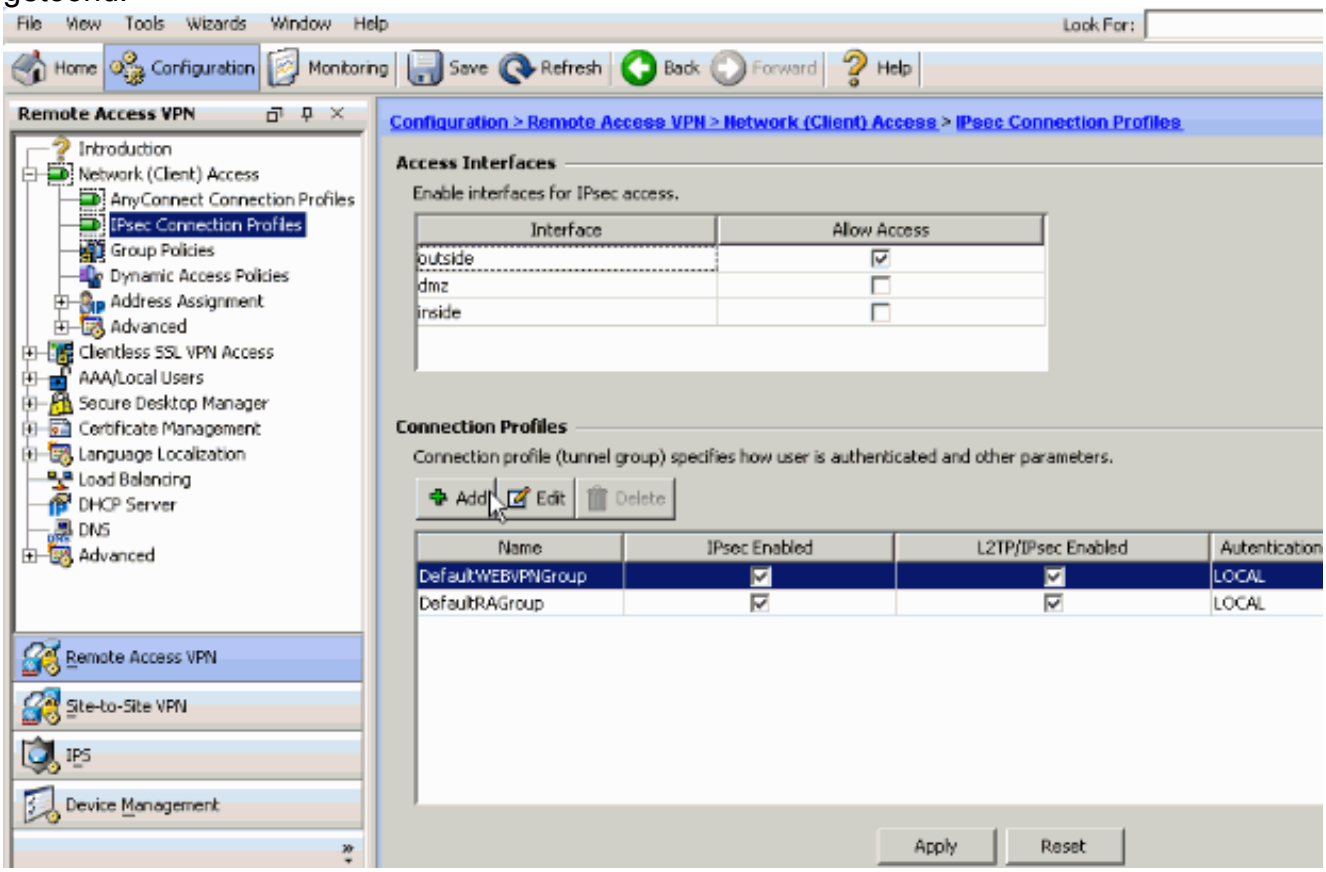


8. Kies **Configuration > Remote Access VPN > Network (Client) Access > Address Asmission > Adres Pools** en klik op **Add** om de VPN-client voor VPN-gebruikers toe te

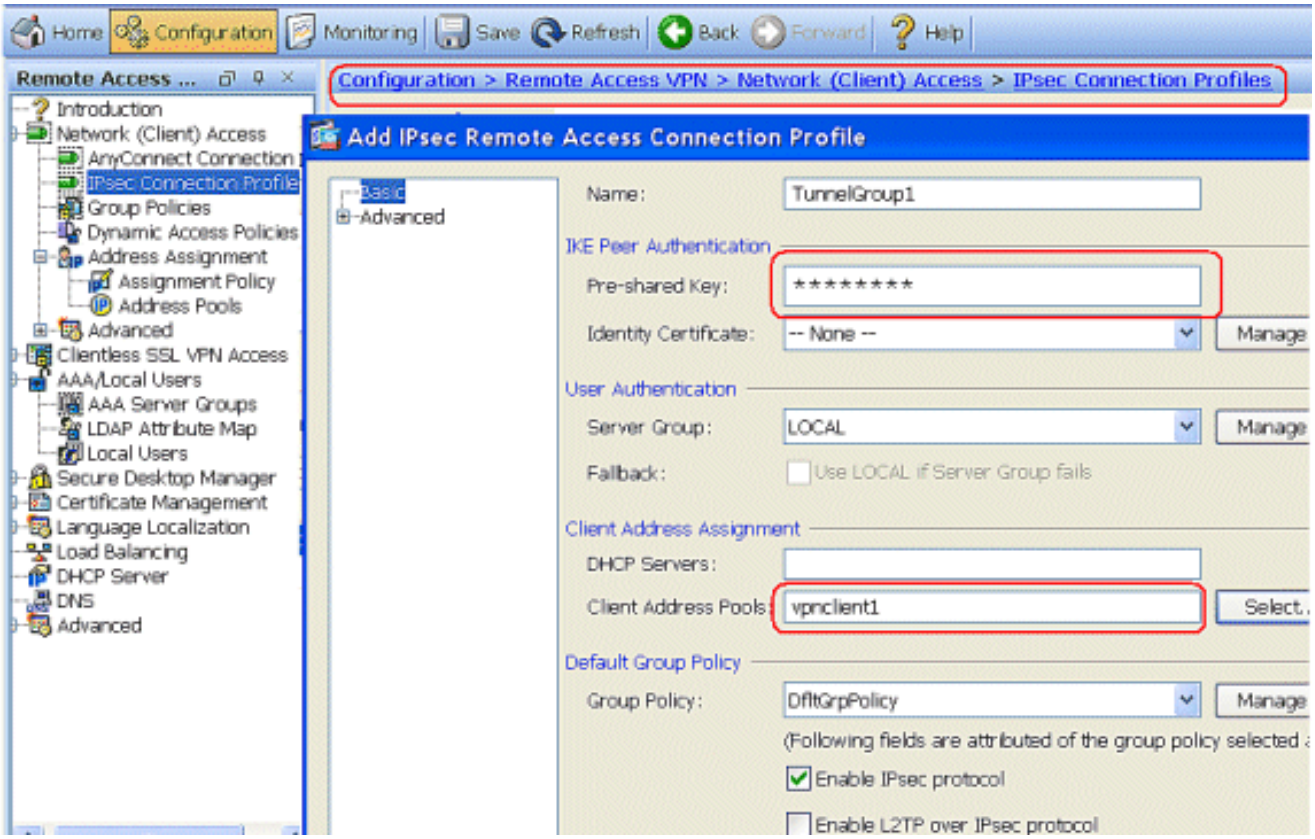
voegen.



9. Kies **Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profile > Add** om een tunnelgroep toe te voegen (bijvoorbeeld TunnelGroup1 en de PreShared key as cisco123), zoals wordt
getoond.

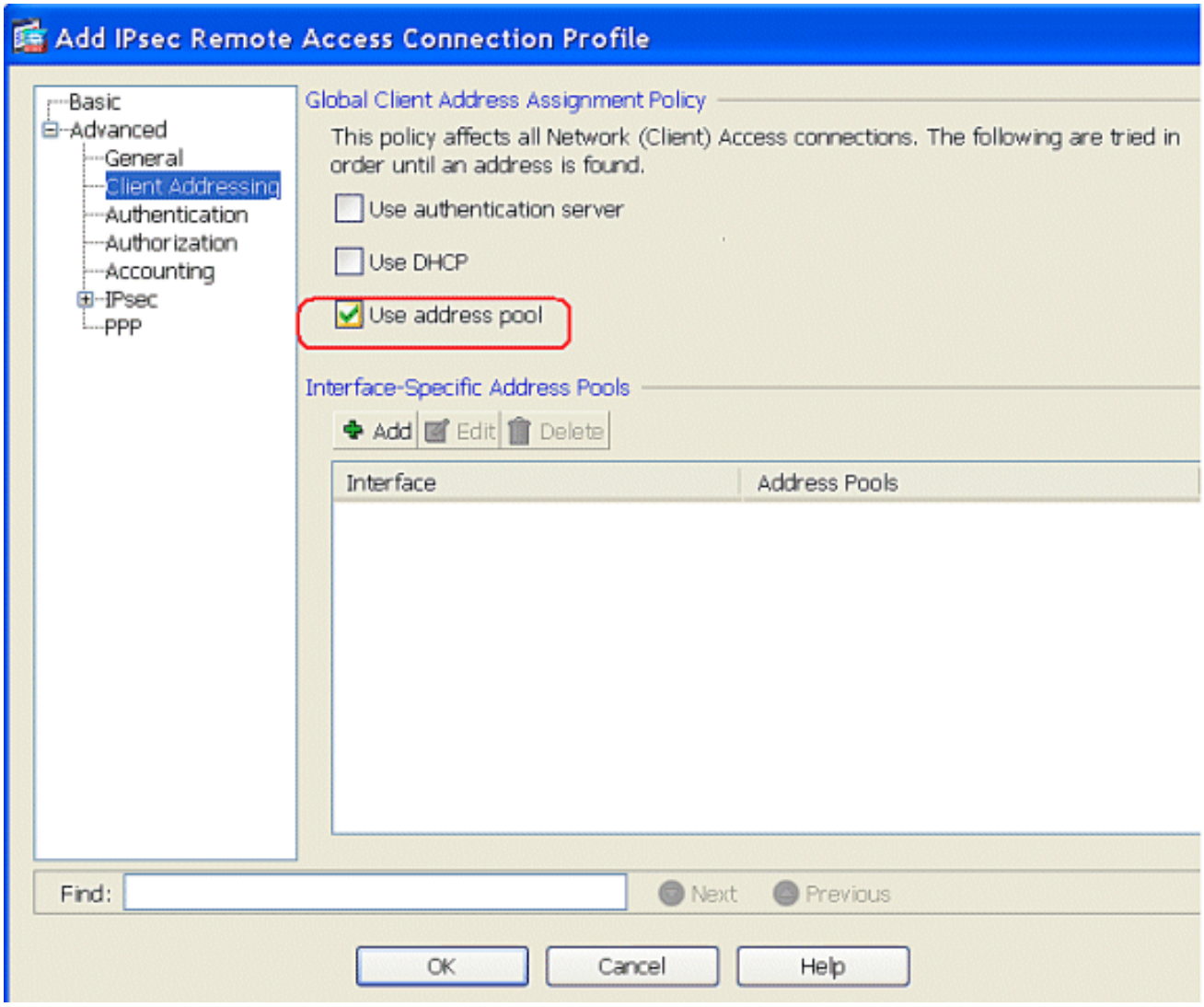


Kies onder het tabblad **Basic** de servergroep als **LOCAL** voor het veld Gebruikersverificatie.Kies **VPN-client1** als de clientadrespools voor de VPN-clientgebruikers.



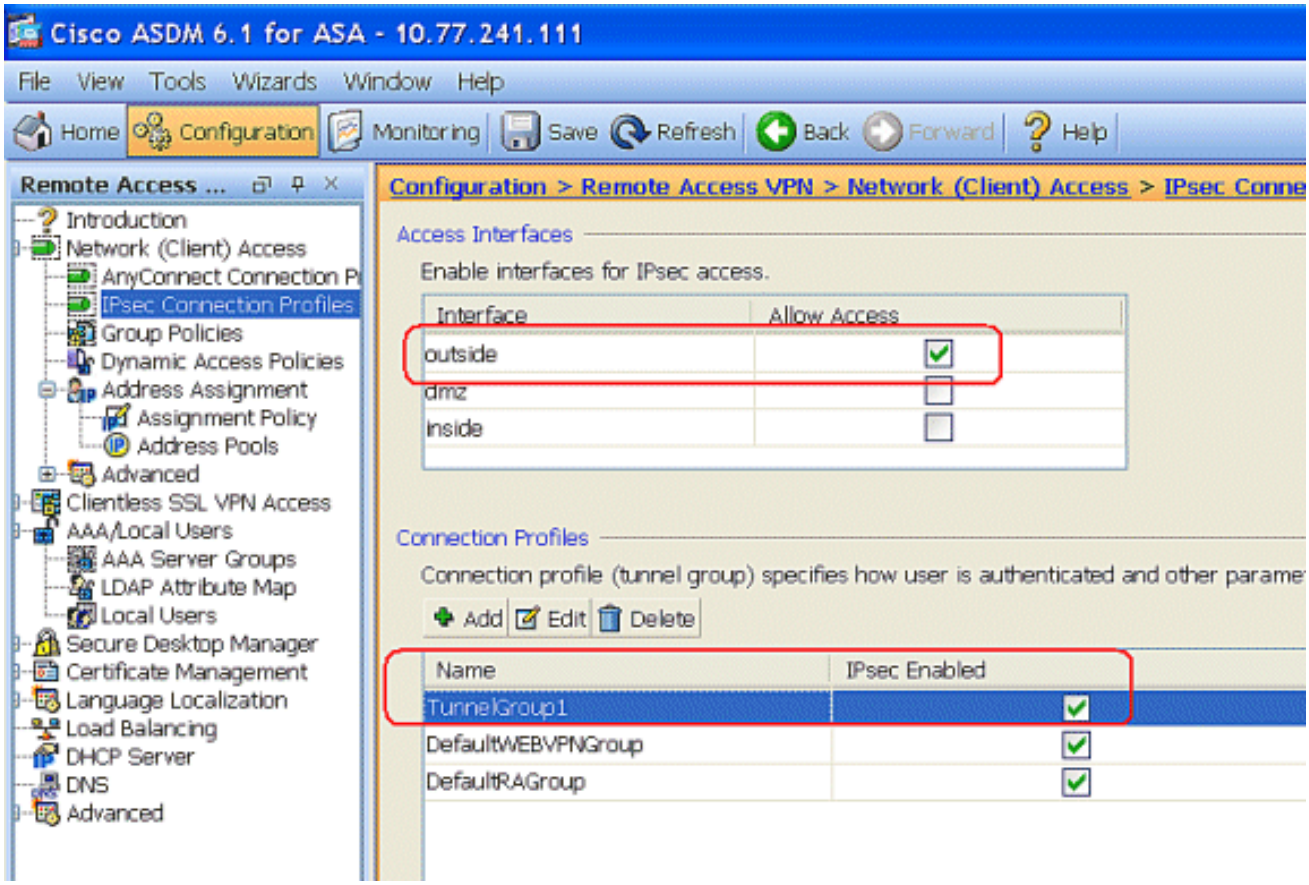
Klik op **OK**.

10. Kies **Geavanceerd > Clientadressering** en controleer het aankruisvakje **Adres gebruiken** om het IP-adres aan de VPN-clients toe te wijzen.**Opmerking:** Schakel de selectievakjes in om de **verificatieserver** te **gebruiken** en **DHCP** te **gebruiken**.



Klik op **OK**.

11. Schakel de interface **Outside** voor IPSec Access in. Klik op **Toepassen** om verder te gaan.



ASA/PIX met CLI configureren

Voltooi deze stappen om de DHCP-server te configureren om IP-adressen te geven aan de VPN-clients vanuit de opdrachtregel. Raadpleeg Beelden voor externe toegang VPN's of Cisco ASA 5500 Series adaptieve security applicaties-commando-referenties voor meer informatie over elke opdracht die wordt gebruikt.

Configuratie op het ASA-apparaat uitvoeren

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0

no failover
icmp unreachable rate-limit 1 burst-size 1
```

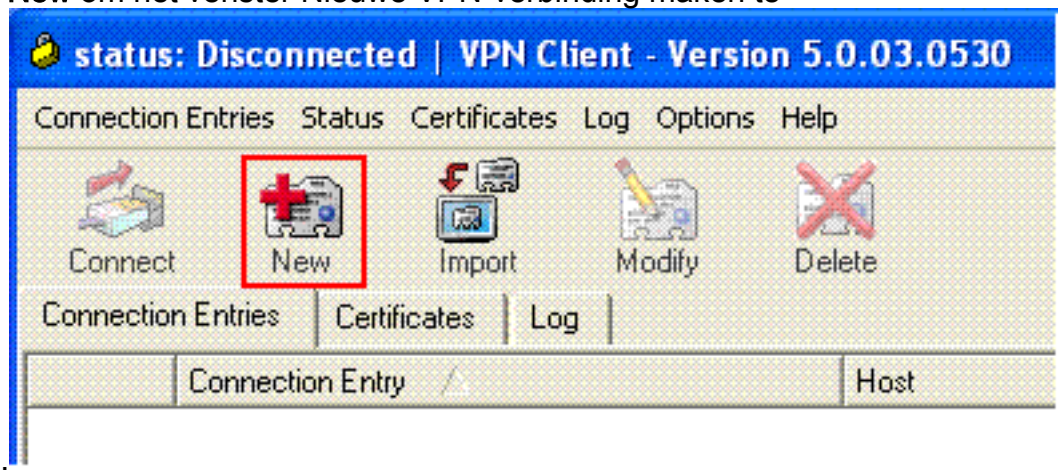
```
!--- Specify the location of the ASDM image for ASA to
fetch the image for ASDM access. asdm image disk0:/asdm-
613.bin no asdm history enable arp timeout 14400 global
(outside) 1 192.168.1.5 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 192.168.1.2 1 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 crypto ipsec transform-set
ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-DES-SHA crypto
map outside_map 1 ipsec-isakmp dynamic outside_dyn_map
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside !--- PHASE 1 CONFIGURATION
---! !--- This configuration uses ISAKMP policy 2. !---
The configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 2 authentication pre-share
encryption des hash sha group 2 lifetime 86400 no crypto
isakmp nat-traversal !--- Specifies that the IP address
to the vpn clients are assigned by the local and not by
AAA or dhcp. The CLI vpn-addr-assign local for VPN
address assignment through ASA is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign dhcp

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
!
!
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
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal

!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode

username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
  vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

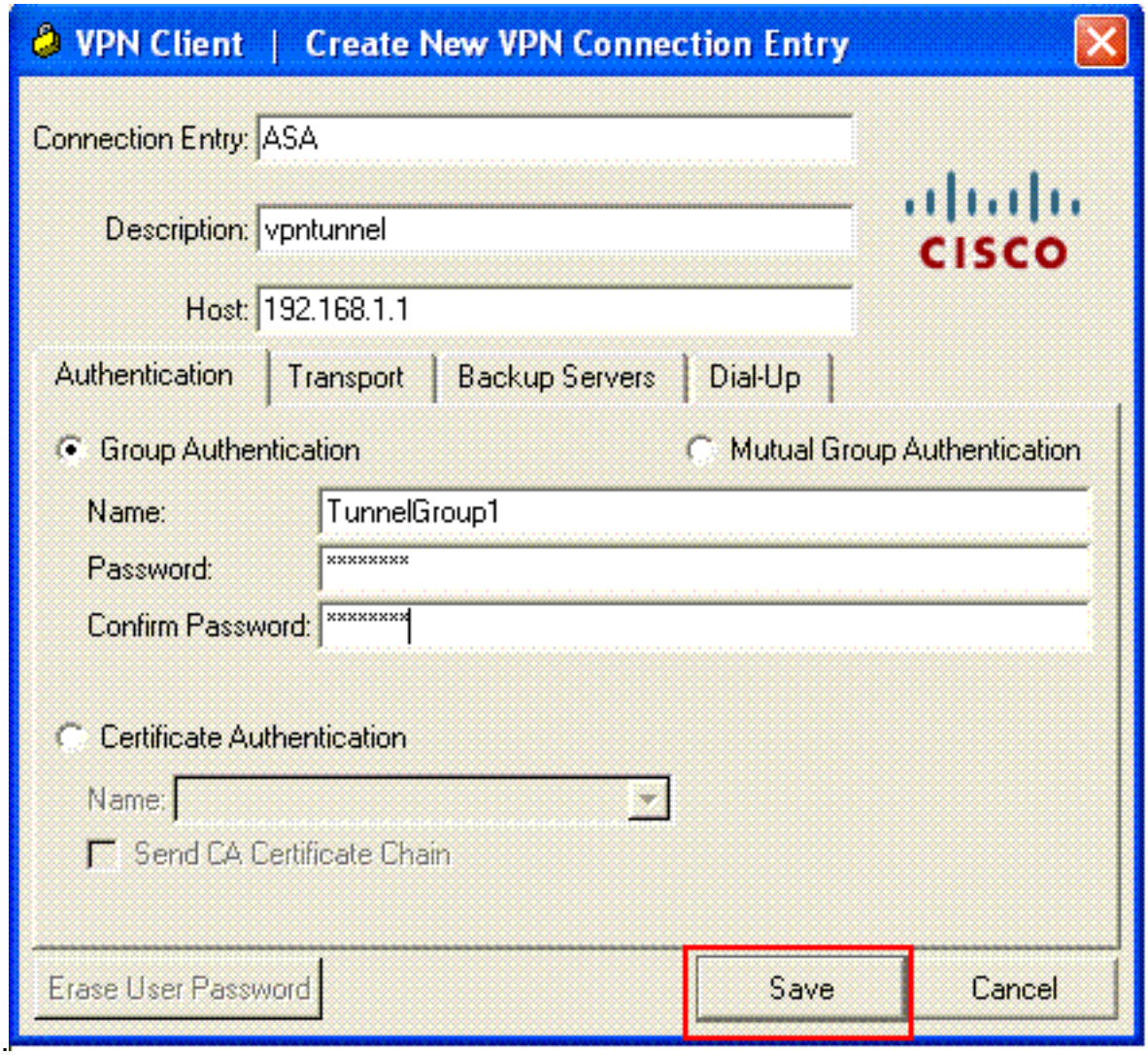
Cisco VPN-clientconfiguratie

Probeer met de Cisco ASA te verbinden met de Cisco VPN-client om te verifiëren dat de ASA met succes is geconfigureerd.

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client**.
2. Klik op **New** om het venster Nieuwe VPN-verbinding maken te starten.

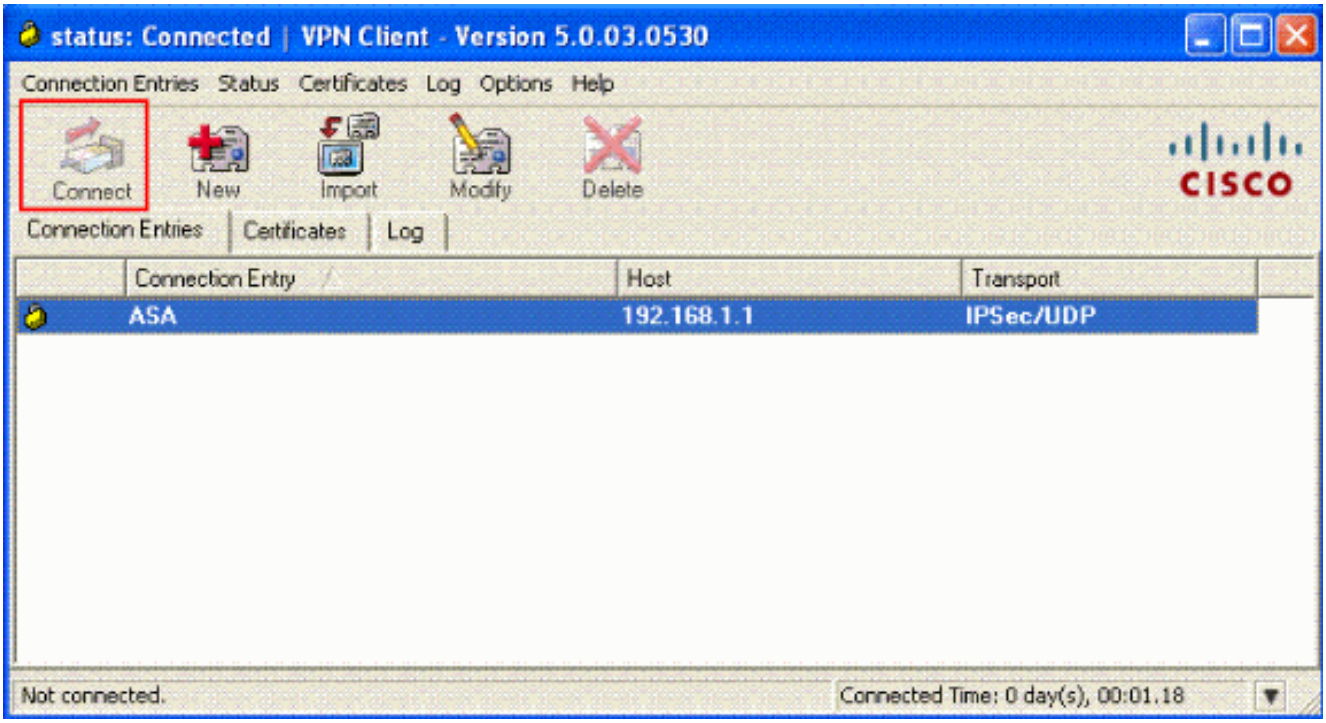


3. Vul de gegevens in van uw nieuwe aansluiting.Voer de naam van de verbindingsbocht in samen met een beschrijving. Voer het **externe IP-adres van de ASA** in het hostvak in. Voer vervolgens de naam van de VPN Tunnel Group (TunnelGroup1) en het wachtwoord in (Voorgedeelde sleutel - Cisco123) zoals ingesteld in ASA. Klik op

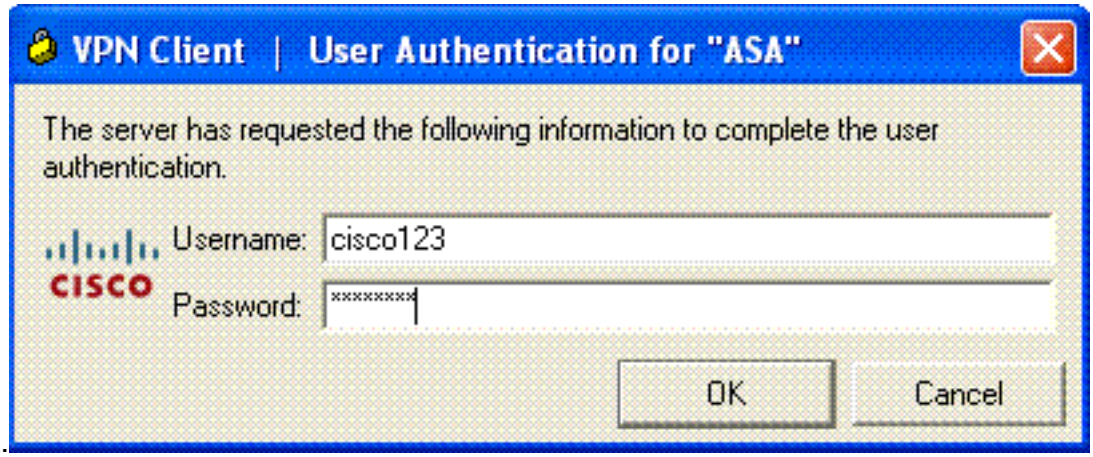


Opslaan.

4. Klik op de verbinding die u wilt gebruiken en klik op **Connect** vanuit het hoofdvenster van VPN-
client.

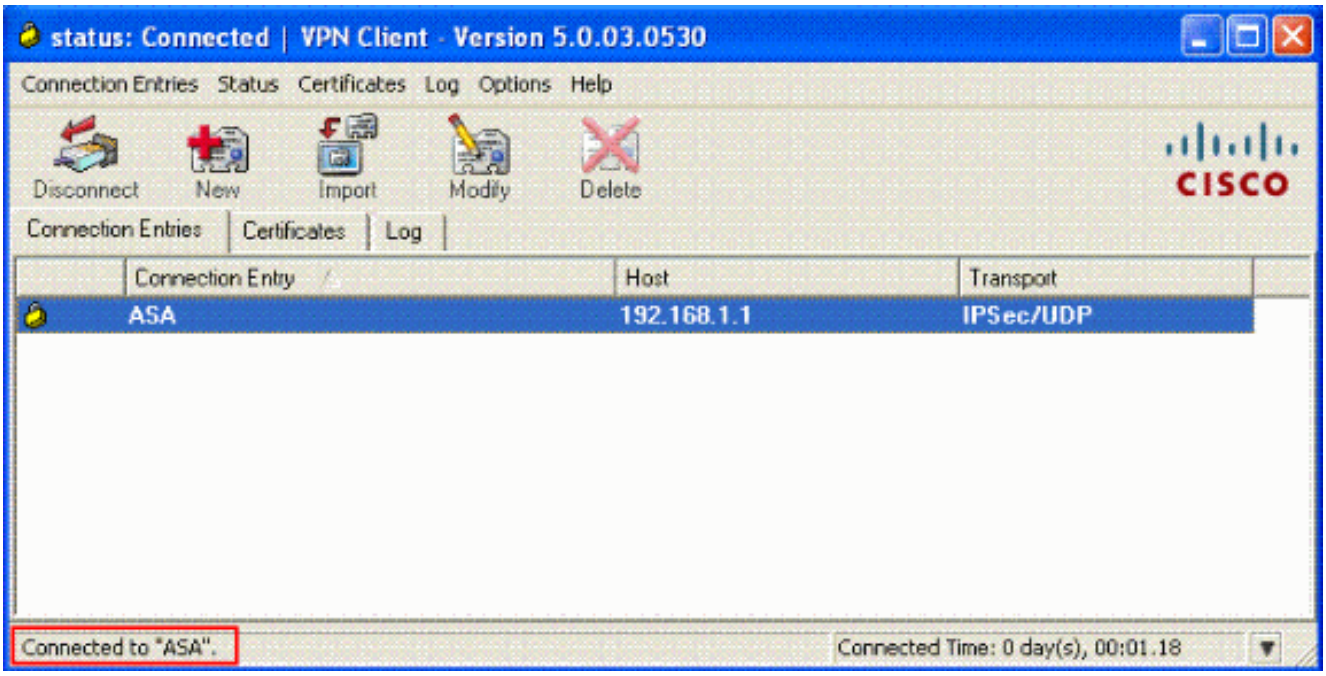


5. Voer desgevraagd de **gebruikersnaam** in **: Cisco123** en **Wachtwoord: cisco123** zoals ingesteld in de ASA for Xauth en klik op **OK** om verbinding te maken met het externe

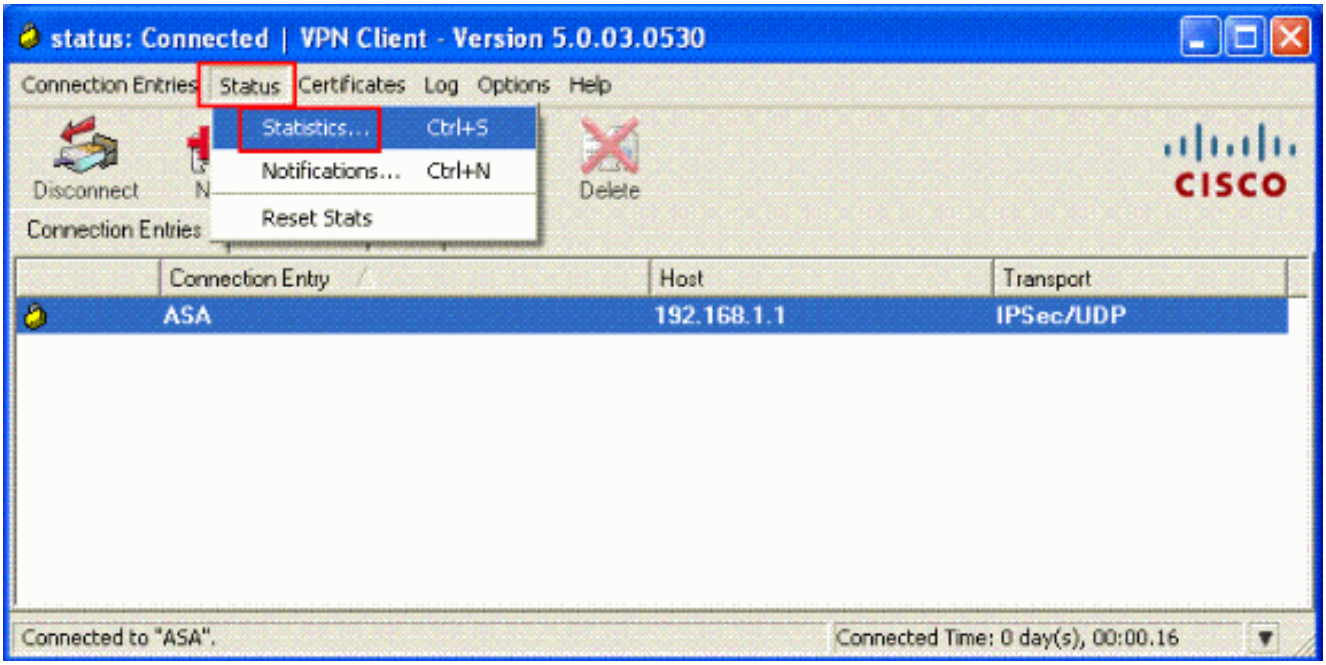


netwerk.

6. De VPN-client is verbonden met de ASA op de centrale site.



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



Verifiëren

Opdrachten tonen

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

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

- **toon crypto isakmp sa**-toont alle huidige IKE Security Associations (SAs) bij een peer.
- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige SA's.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Ook wordt een voorbeelduitvoer van debug-uitvoer weergegeven.

Opmerking: Voor meer informatie over de oplossing van problemen met betrekking tot IPSec VPN verwijst u naar de meest gebruikelijke oplossingen voor probleemoplossing in L2L en externe access IPSec VPN.

Beveiligingsassociaties wissen

Wanneer u problemen oplossen, zorg er dan voor dat de bestaande veiligheidsassociaties worden gewist nadat u een wijziging hebt aangebracht. In de bevoorrechte modus van de PIX, gebruik deze opdrachten:

- **duidelijk [crypto] ipsec sa**-Delete de actieve IPSec SA's. Het sleutelwoord crypto is optioneel.
- **Schakel [crypto] isakmp sa**—Verwijdert de actieve IKE SA's. Het sleutelwoord crypto is optioneel.

Opdrachten voor probleemoplossing

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

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-** opdrachten gebruikt.

- **debug crypto ipsec 7**-displays de IPSec-onderhandelingen van fase 2.
- **debug crypto isakmp 7** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Gerelateerde informatie

- Cisco ASA 5500 Series ondersteuningspagina voor adaptieve security applicaties
- Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties
- Ondersteuning van Cisco PIX 500 Series security applicaties
- Cisco PIX 500 Series security applicaties, opdracht

- Cisco adaptieve security apparaatbeheer
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Cisco VPN-clientondersteuningspagina
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems