# ASA/PIX 8.x: RADIUS-autorisatie (ACS 4.x) voor VPN-toegang met downloadbare ACL's met CLI- en ASDM-configuratievoorbeeld

## Inhoud



## Inleiding

Dit document beschrijft hoe u het security apparaat moet configureren om gebruikers te controleren op basis van een netwerktoegang. Aangezien u impliciet RADIUS-autorisaties kunt inschakelen, bevat deze sectie geen informatie over de configuratie van RADIUS-autorisatie op het beveiligingsapparaat. Het geeft wel informatie over hoe het beveiligingsapparaat omgaat met informatie over toegangslijsten die van RADIUS-servers wordt ontvangen.

U kunt een RADIUS-server configureren om een toegangslijst naar het beveiligingsapparaat te downloaden of een toegangslijst met naam op het moment van verificatie. De gebruiker is geautoriseerd om alleen te doen wat is toegestaan in de gebruikersspecifieke toegangslijst.

Downloadbare toegangslijsten zijn de meest schaalbare middelen wanneer u Cisco Secure ACS gebruikt om de juiste toegangslijsten voor elke gebruiker te geven. Raadpleeg voor meer informatie over de functies van de toegangslijst en de Cisco Secure ACS het configureren van een RADIUS-server om downloadbare toegangscontrolelijsten en downloadbare IP-ACL's te verzenden.

Raadpleeg ASA 8.3 en hoger: RADIUS-autorisatie (ACS 5.x) voor VPN-toegang met downloadbare ACL met CLI- en ASDM-configuratievoorbeeld voor de identieke configuratie op Cisco ASA met versies 8.3 en hoger.

# 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
- Cisco Adaptieve Security Office Manager versie 5.x en hoger
- Cisco VPN-clientversie 4.x en hoger
- Cisco Secure Access Control Server 4.x

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.

# Achtergrondinformatie

U kunt IP ACL's downloaden om sets ACL-definities te maken die u op veel gebruikers of gebruikersgroepen kunt toepassen. Deze reeksen ACL-definities worden ACL-inhoud genoemd. Ook, wanneer u NAFs integreert, controleert u de inhoud ACL die naar de AAA client wordt

verzonden waar een gebruiker toegang toe zoekt. Dat wil zeggen, een downloadbare IP ACL omvat één of meer ACL-contentdefinities, die allemaal gekoppeld zijn aan een NAF of (standaard) gekoppeld aan alle AAA-clients. NAF controleert de toepasbaarheid van gespecificeerde ACL-inhoud in overeenstemming met het IP-adres van de AAA-client. Voor meer informatie over NAFs en hoe zij downloadbare IP ACLs reglementeren, zie Info over Filters van de Toegang van het Netwerk.

Downloadbare IP-ACL's werken op deze manier:

1. Wanneer ACS een gebruiker toegang tot het netwerk verleent, bepaalt ACS of een downloadbare IP ACL aan die gebruiker of de groep van de gebruiker wordt toegewezen.
2. Als ACS op een downloadbare IP-ACL let die aan de gebruiker of de groep van de gebruiker wordt toegewezen, bepaalt het of een ACL-contentinvoer wordt geassocieerd met de AAA-client die de RADIUS-verificatieaanvraag heeft verzonden.
3. ACS stuurt, als deel van de gebruikerssessie, een RADIUS-toegangsaccepteer pakket, een eigenschap die de genoemde ACL specificeert, en de versie van de genoemde ACL.
4. Als de AAA-client reageert dat de huidige versie van ACL in zijn cache niet beschikbaar is, dat wil zeggen dat ACL nieuw is of is gewijzigd, stuurt ACS de ACL (nieuw of bijgewerkt) naar het apparaat.

Downloadbare IP-ACL's zijn een alternatief voor de configuratie van ACL's in de RADIUS Cisco cisco-av-paareigenschap [26/9/1] van elke gebruiker of gebruikersgroep. U kunt eenmaal een downloadbare IP-ACL maken, deze een naam geven en vervolgens de downloadbare IP-ACL toewijzen aan elke toepasbare gebruiker of gebruikersgroep als u zijn naam verwijst. Deze methode is efficiënter dan als u de RADIUS-Cisco cisco-av-paareigenschap van RADIUS voor elke gebruiker of gebruikersgroep vormt.

Verder, wanneer u NAFs gebruikt, kunt u verschillende inhoud van ACL op de zelfde gebruiker of groep gebruikers met betrekking tot de AAA client toepassen die zij gebruiken. Er is geen extra configuratie van de AAA-client nodig nadat u de AAA-client hebt geconfigureerd voor het gebruik van downloadbare IP ACL's vanuit ACS. Downloadbare ACL's worden beschermd door het back-up- of replicatieschema dat u hebt ingesteld.

Wanneer u de ACL-definities in de ACS-web interface invoert, gebruik dan geen sleutelwoord of naamvermeldingen; Gebruik in alle andere opzichten de standaard ACL-opdrachtsyntaxis en -semantiek voor de AAA-client waarop u de downloadbare IP ACL-ACL wilt toepassen. De ACL-definities die u in ACS invoert, omvatten een of meer ACL-opdrachten. Elke ACL-opdracht moet op een aparte lijn staan.

U kunt een of meer genoemde ACL-inhoud toevoegen aan een IP-ACL-adres dat kan worden gedownload. Standaard is elke ACL-inhoud van toepassing op alle AAA-clients, maar als u NAF's hebt gedefinieerd, kunt u de toepasbaarheid van elke ACL-inhoud beperken tot de AAA-clients die in de NAF zijn vermeld die u hieraan associeert. Dat wil zeggen, wanneer u NAFs gebruikt, kunt u elke ACL inhoud, binnen één enkele downloadbare IP ACL, van toepassing maken op meerdere verschillende netwerkapparaten of netwerkapparaatgroepen in overeenstemming met uw netwerkbeveiligingsstrategie.

U kunt ook de volgorde van de ACL-inhoud wijzigen in een downloadbare IP-ACL. ACS onderzoekt ACL-inhoud, vanaf de bovenkant van de tabel, en downloads de eerste ACL-inhoud die deze vindt met een NAF dat de AAA-client bevat die wordt gebruikt. Wanneer u de volgorde instelt, kunt u de systeemefficiëntie garanderen als u de meest toepasselijke ACL-inhoud hoger in de lijst plaatst. U moet zich realiseren dat, als uw NAFs bevolkingen van AAA cliënten omvatten die overlappen, u van het specifiekere naar het meer algemene moet overgaan. ACS downloads

bijvoorbeeld elke ACL-inhoud met de instelling All-AAA-Clients NAF en beschouwt geen ACL's die lager in de lijst staan.

Om IP ACL op een bepaalde AAA-client te kunnen downloaden, moet de AAA-client deze richting volgen:

- Gebruik RADIUS voor verificatie
- Ondersteuning van downloadbare IP ACL's

Dit zijn voorbeelden van Cisco-apparaten die IP ACL's ondersteunen die kunnen worden gedownload:

- ASA- en PIX-apparaten
- VPN 3000-Series concentrators
- Cisco-apparaten die IOS versie 12.3(8)T of hoger uitvoeren

Dit is een voorbeeld van het formaat dat u moet gebruiken om VPN 3000/ASA/PIX 7.x+ ACL's in het vak ACL-definities in te voeren:

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

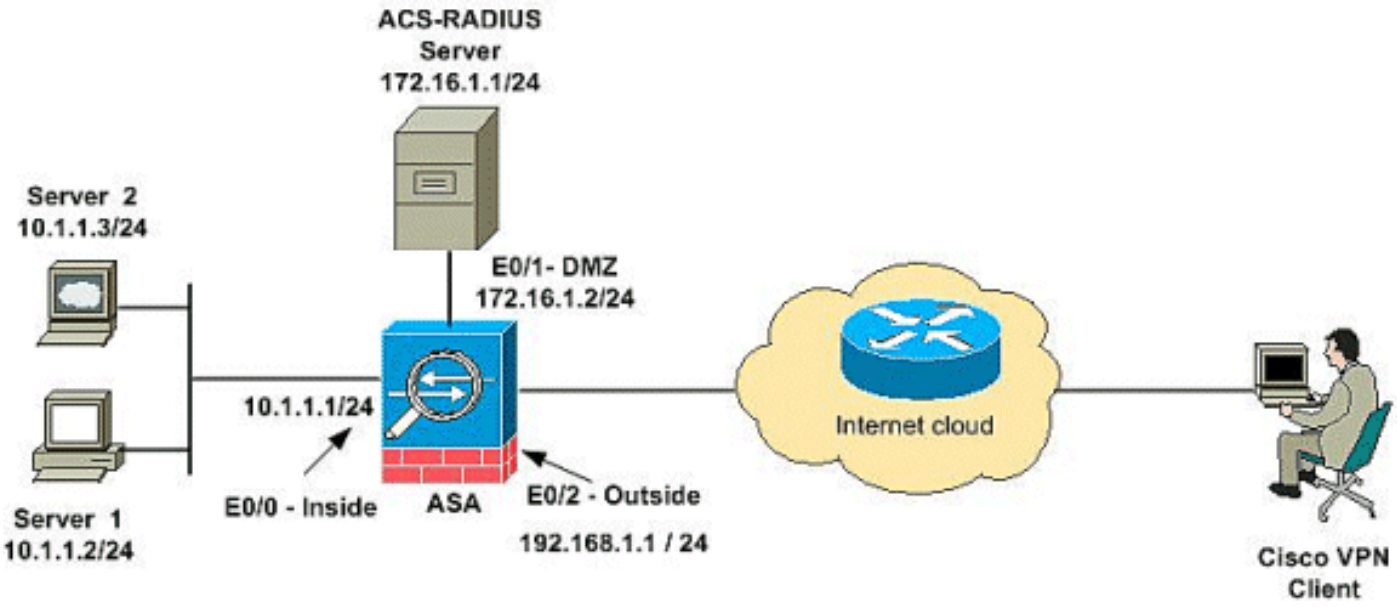
# Configureren

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:



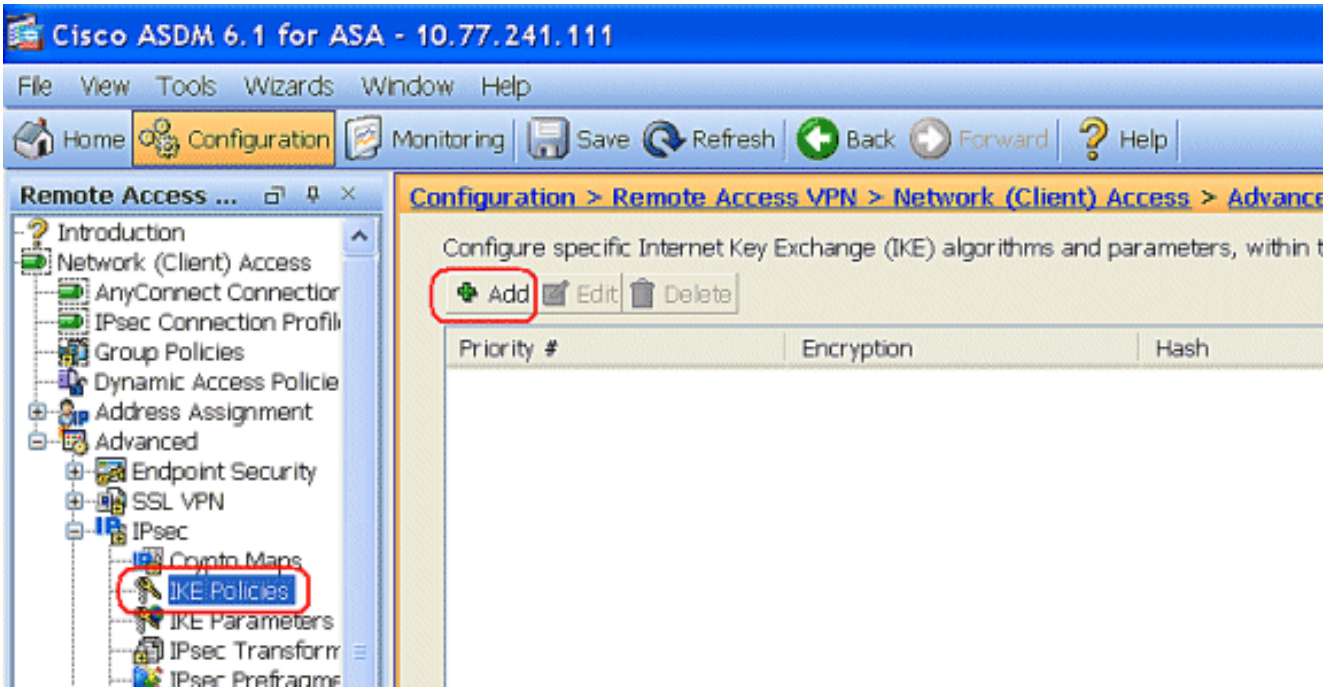

**Opmerking:** de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

## Externe toegang instellen (IPSec)

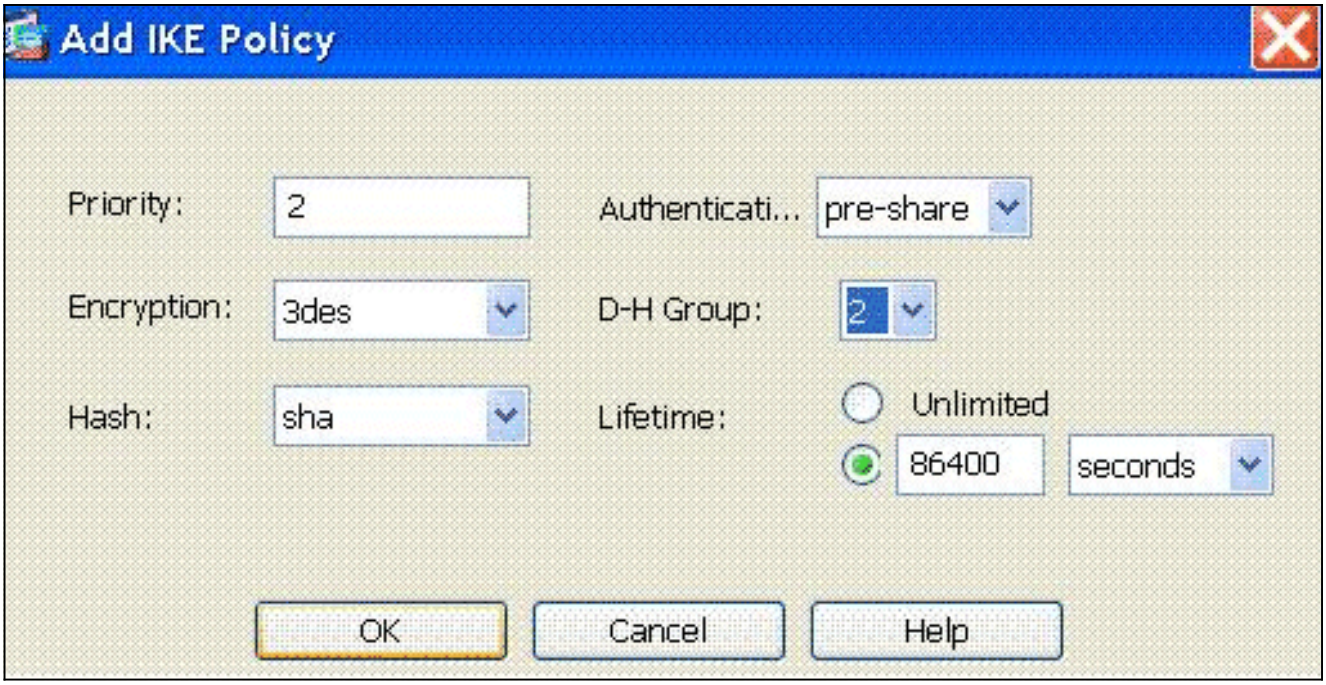
### ASDM-procedure

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.

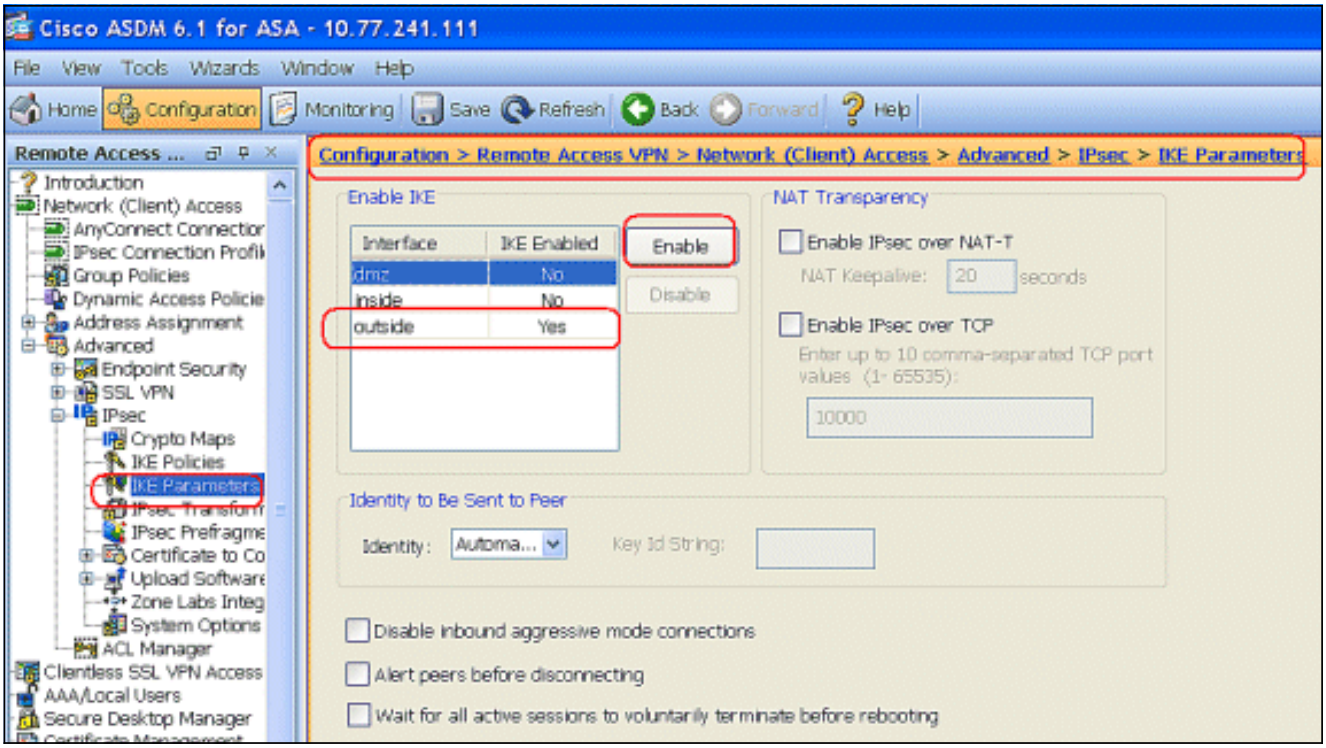



2. Geef de ISAKMP-beleidsdetails zoals aangegeven.

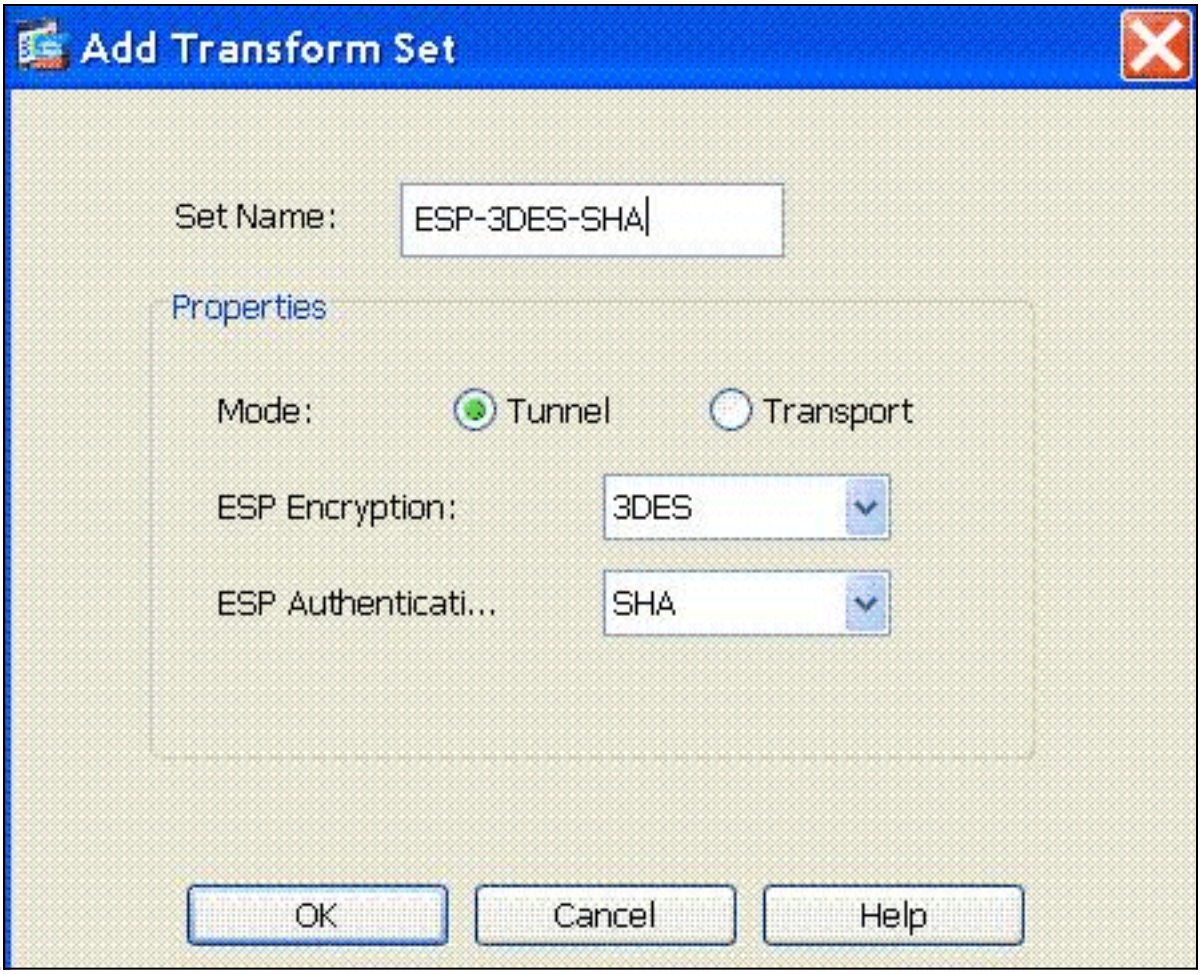



Klik op **OK** en **Toepassen**.

3. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-parameters** om IKE op externe interface in te schakelen.



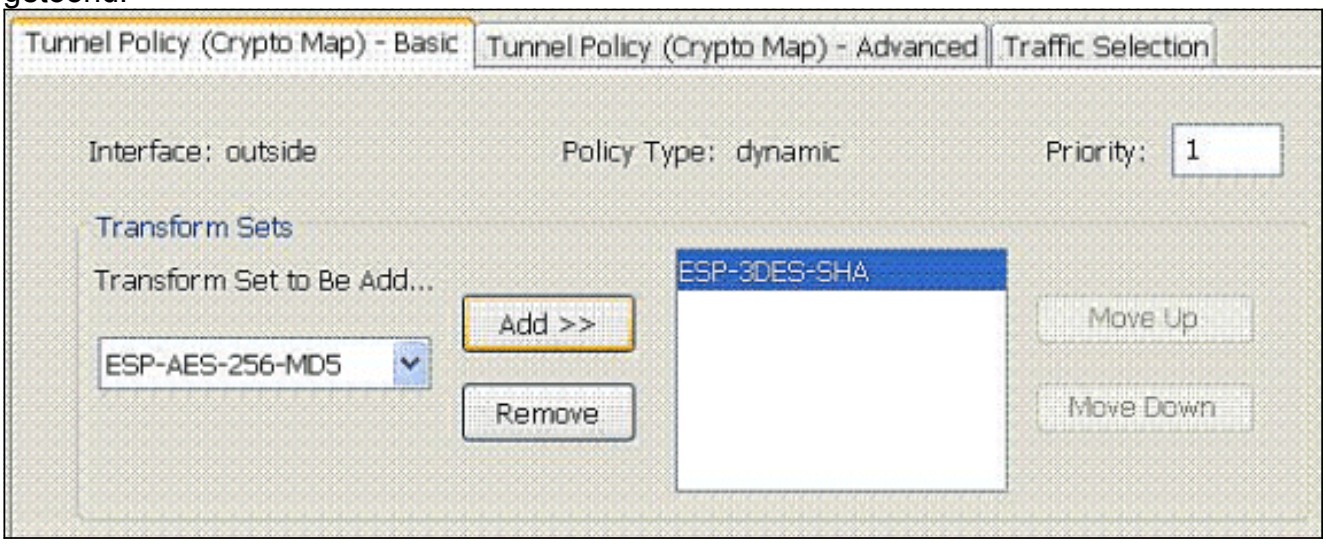

4. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transformatiesets > Add** om de **ESP-3DES-SHA** transformatieset te maken, zoals




getoond.

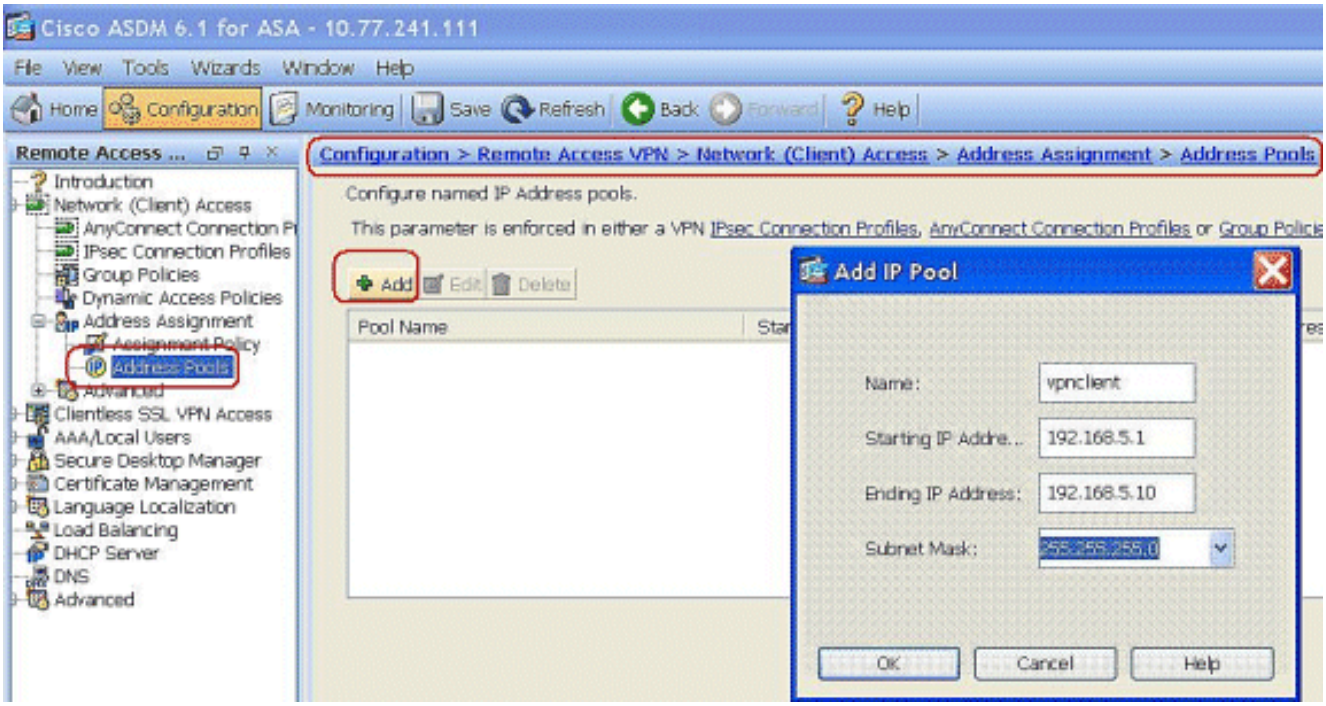
Klik op **OK** en **Toepassen**.

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.

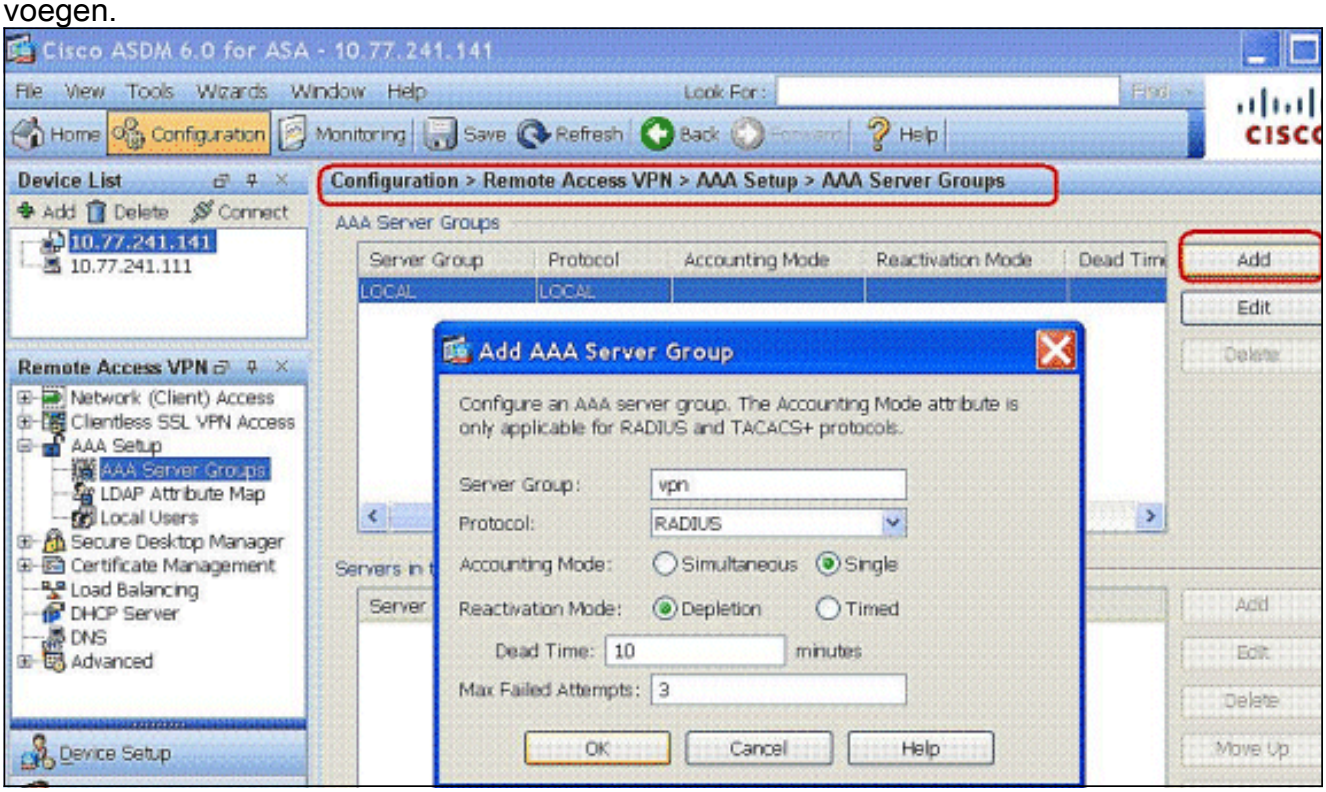



Klik op **OK** en **Toepassen**.

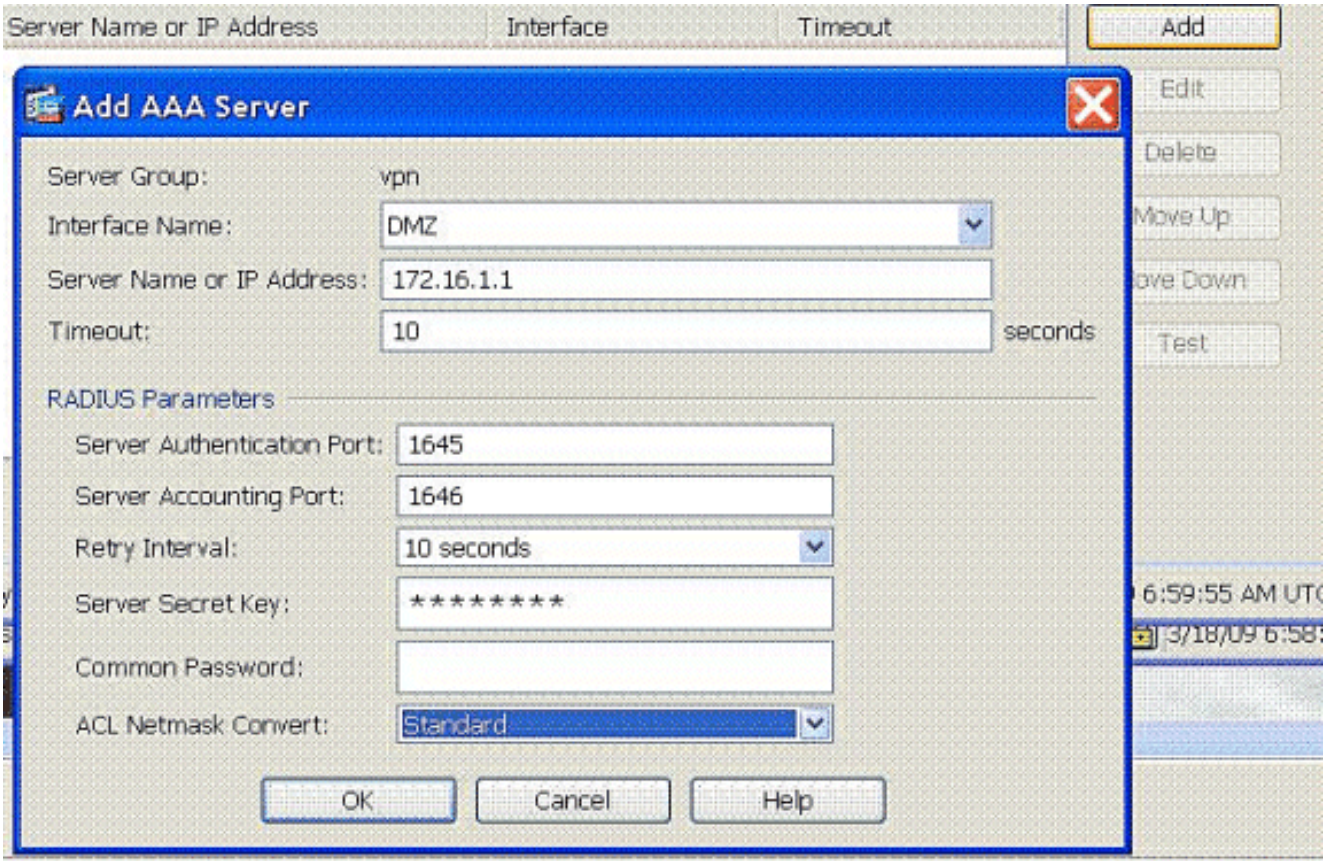
6. Kies **Configuration > Remote Access VPN > Network (Client) Access > Address Asmission > Address Pools** en klik op **Add** om de VPN-client toe te voegen aan de VPN-clientgebruikers.



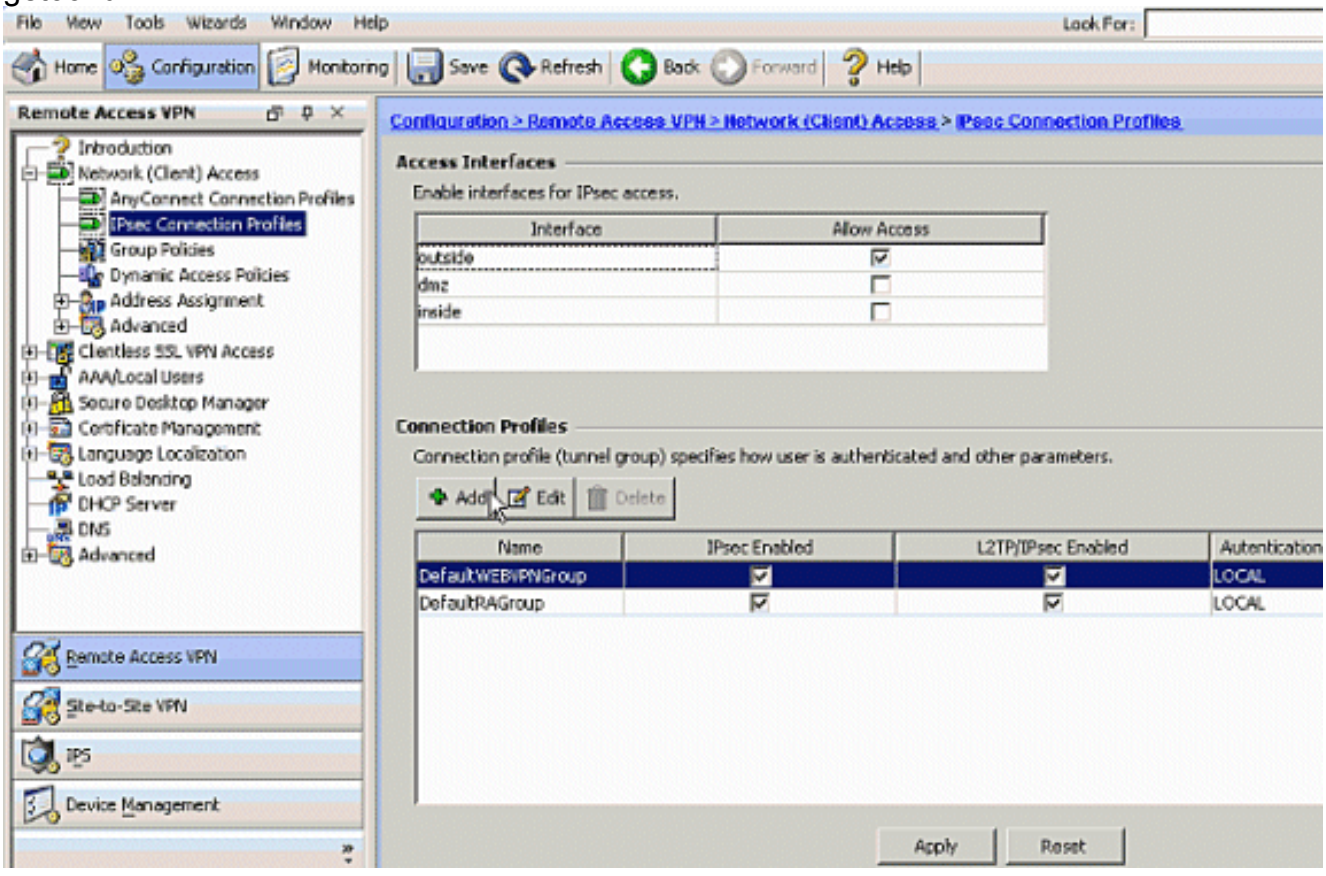

7. Kies **Configuration > Remote Access VPN > AAA-servergroepen** en klik op **Add** om de naam en het protocol van de AAA-servergroep toe te voegen.



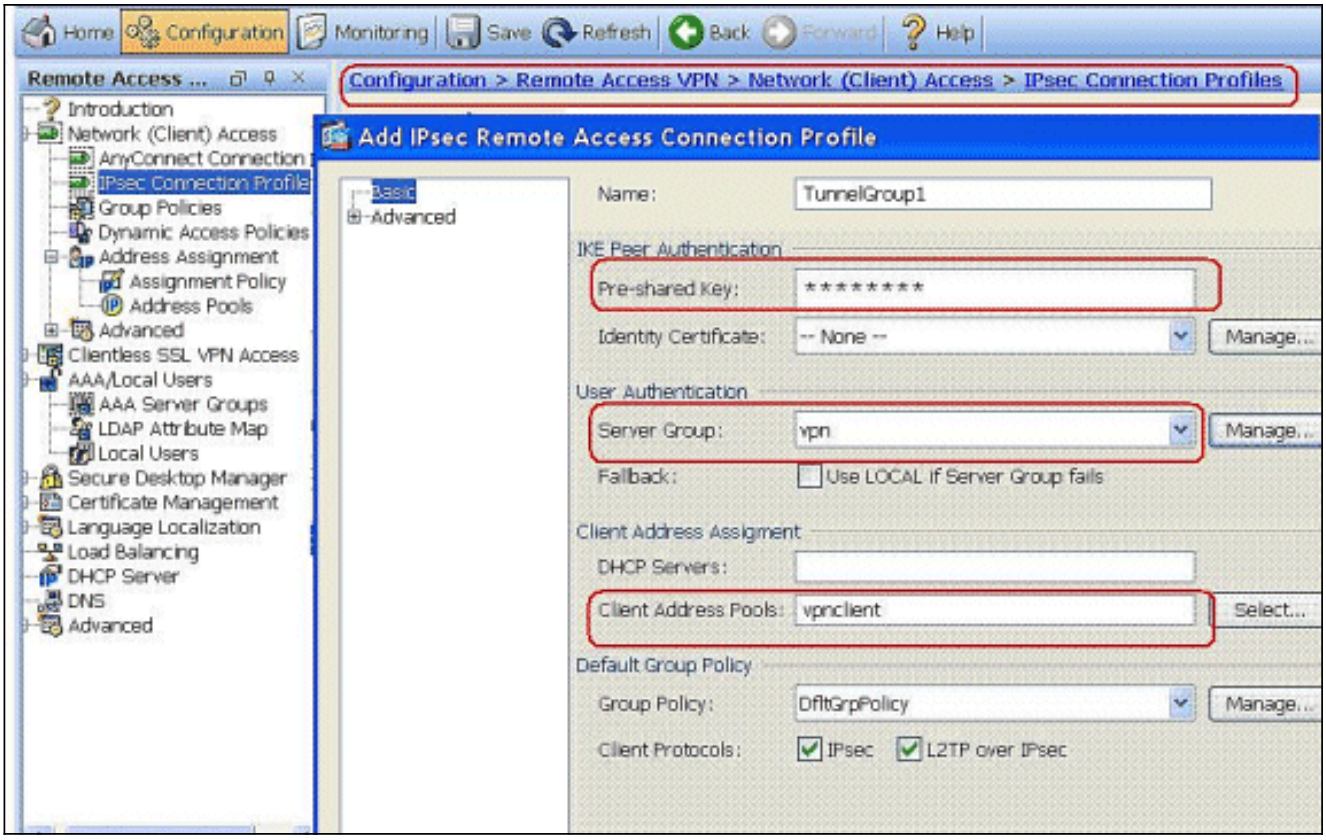

Voeg het AAA server IP adres (ACS) toe en de interface die het verbindt. Voeg ook de sleutel van de Server toe in het gebied van RADIUS-parameters. Klik op **OK**.




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

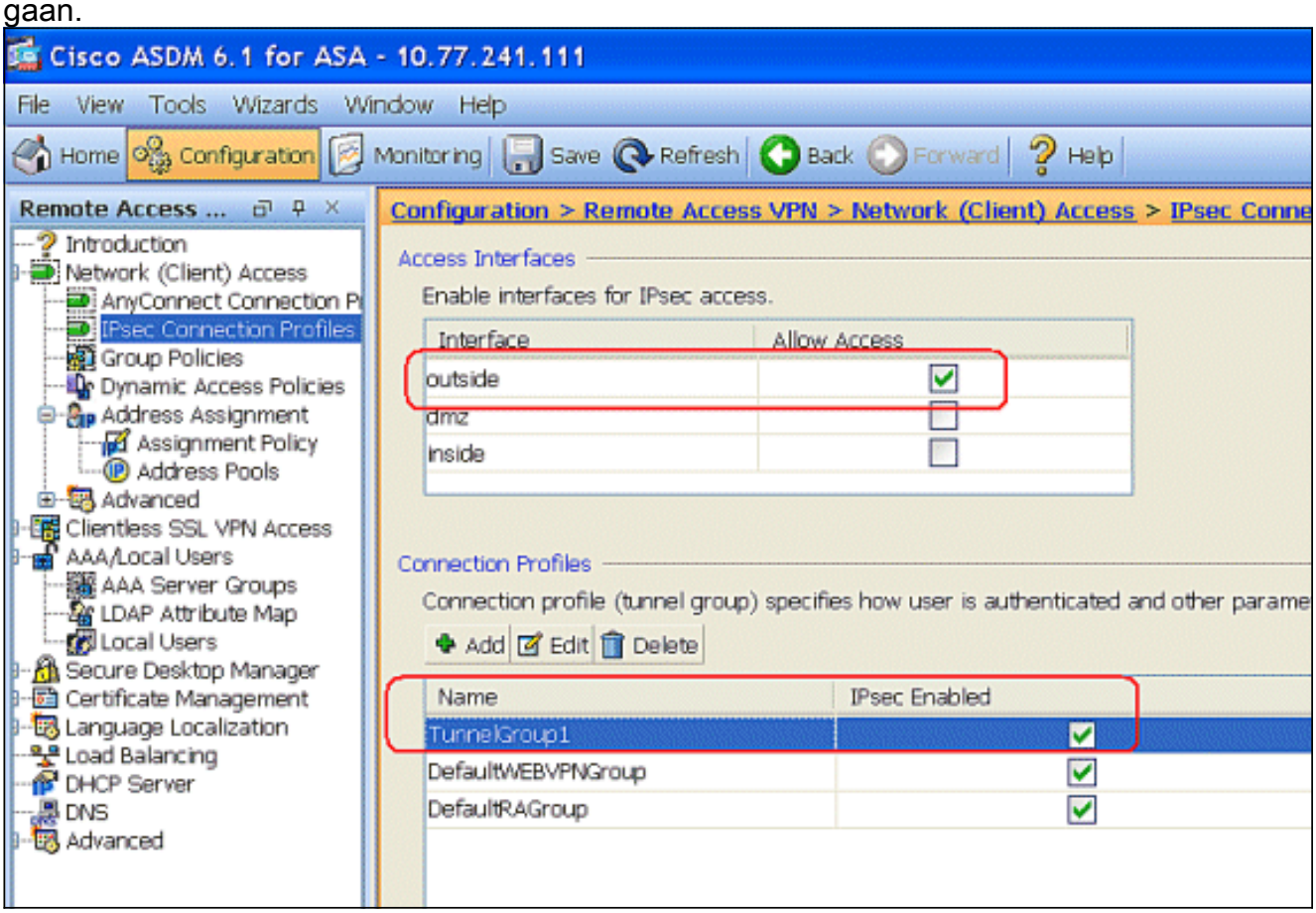



Kies onder het tabblad Basic de servergroep als **VPN** voor het veld Gebruikersverificatie.Kies **VPN-client** als de clientadrespools voor de VPN-clientgebruikers.




Klik op **OK**.

9. Schakel de externe interface 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 DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
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 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2
access-list new extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool vpnclient1 192.168.5.1-192.168.5.10 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 !--- Create the AAA server group
"vpn" and specify the protocol as RADIUS. !--- Specify
the CSACS server as a member of the "vpn" group and
provide the !--- location and key. aaa-server vpn
protocol radius
 max-failed-attempts 5
aaa-server vpn (DMZ) host 172.16.1.1
 retry-interval 1
 timeout 30
 key cisco123
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

!--- PHASE 2 CONFIGURATION ---! !--- The encryption
types for Phase 2 are defined here. !--- A Triple DES
encryption with !--- the sha hash algorithm is used.
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac

!--- Defines a dynamic crypto map with !--- the
specified encryption settings. crypto dynamic-map
outside_dyn_map 1 set transform-set ESP-3DES-SHA

!--- Binds the dynamic map to the IPsec/ISAKMP process.
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 3des
 hash sha
 group 2
 lifetime 86400

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
!
!
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
```

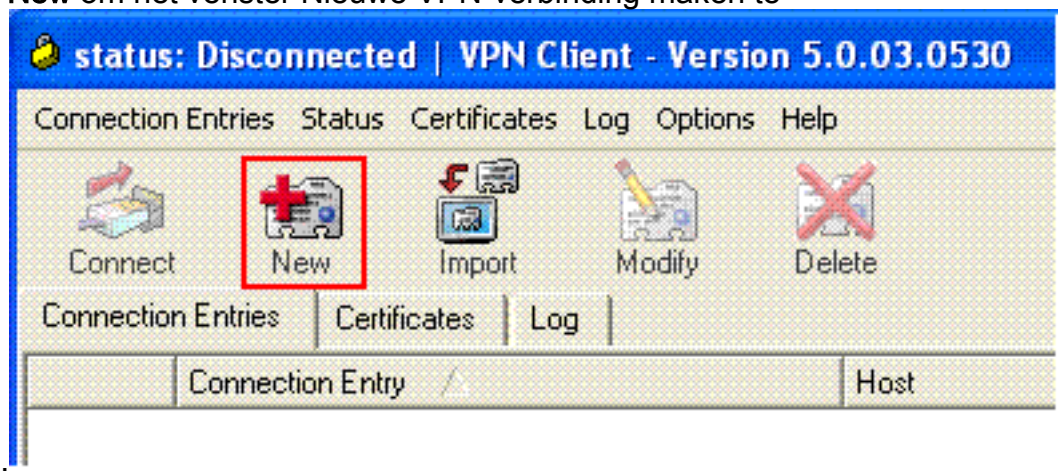
```
  inspect xdmcp
!
service-policy global_policy global
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes
 address-pool vpnclient
 authentication-server-group vpn

!--- 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#
```

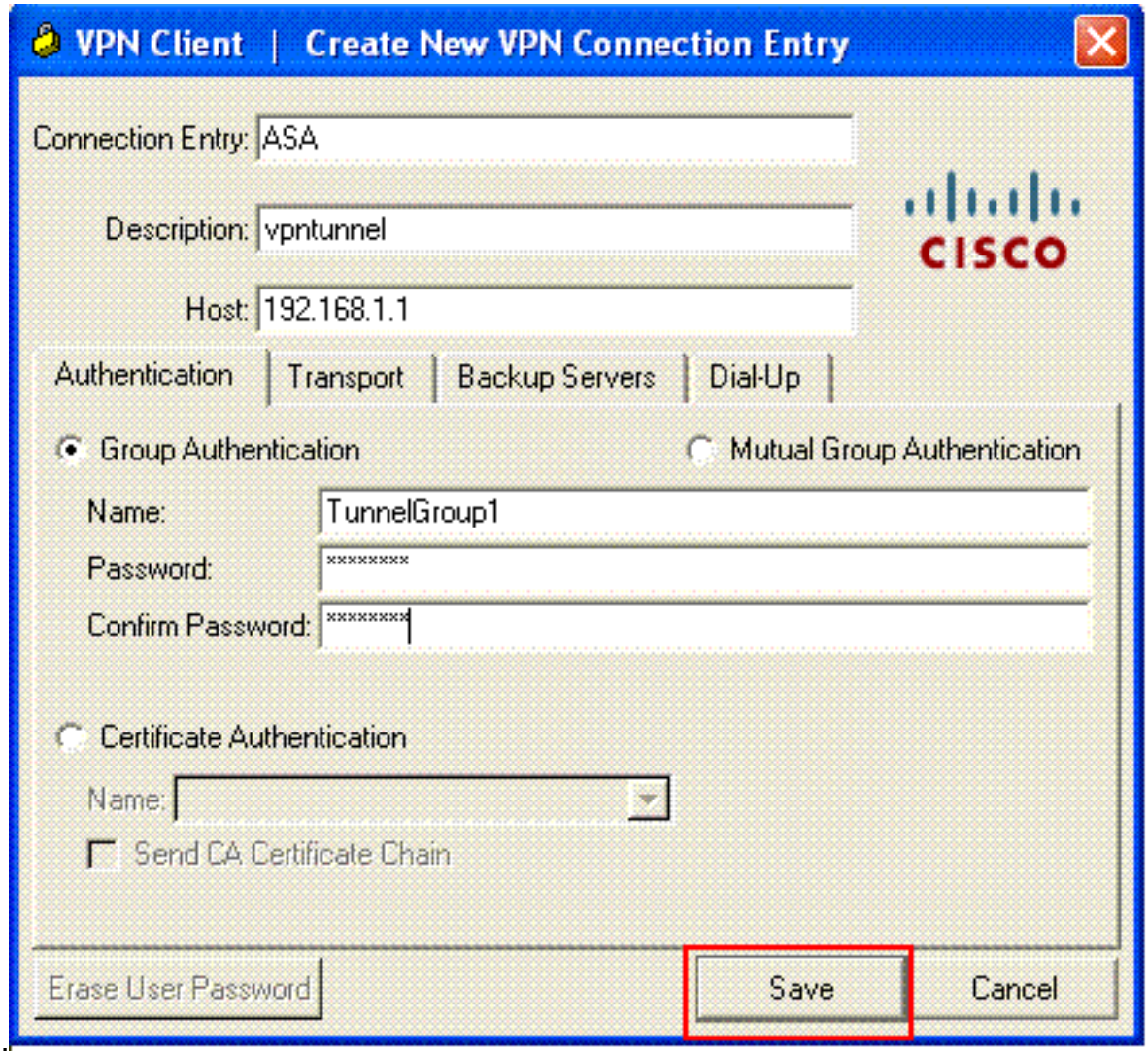
## Cisco VPN-clientconfiguratie

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.

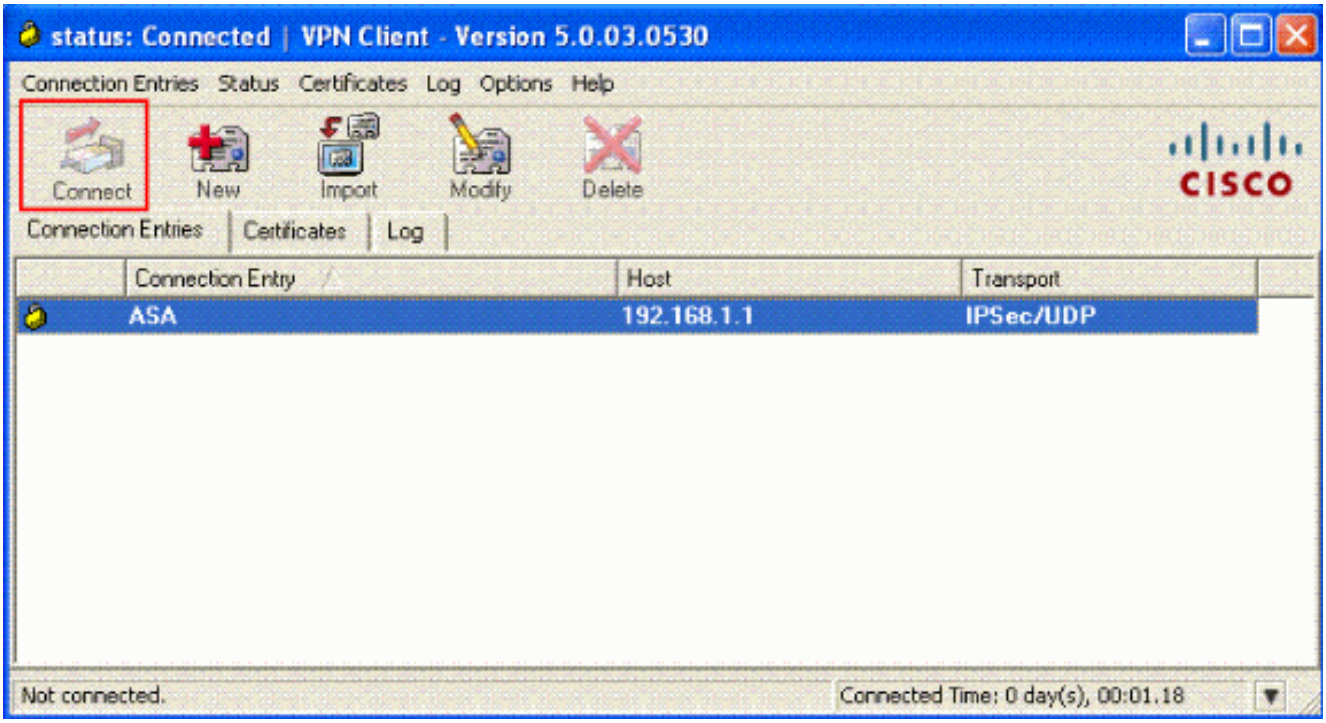



3. Vul de gegevens in van uw nieuwe aansluiting.Voer de naam van de verbindingsbocht in samen met een beschrijving. Voer het **externe IP-adres van de ASA** in het hostvak in. Voer vervolgens de naam van de VPN Tunnel Group (TunnelGroup1) en het wachtwoord in (Voorgedeelde sleutel - Cisco123) zoals ingesteld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

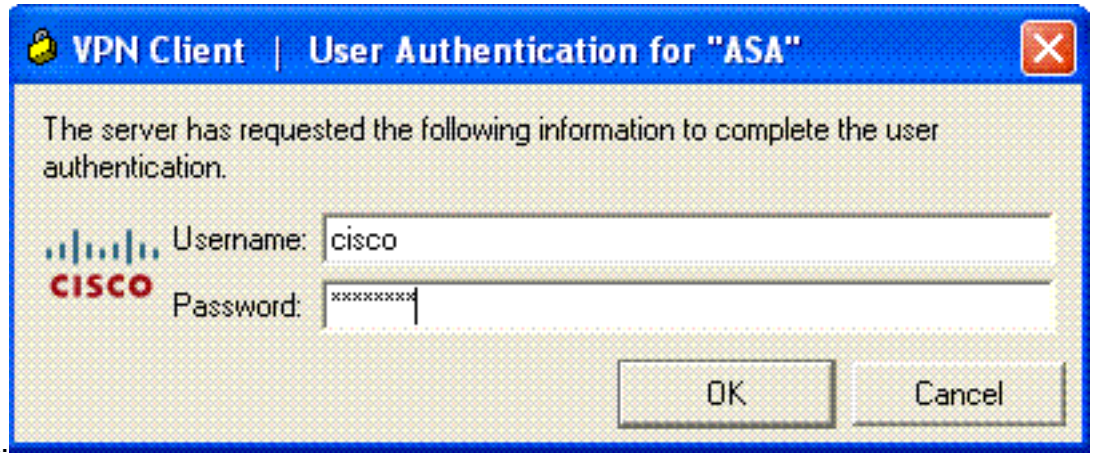



**Opslaan**.

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

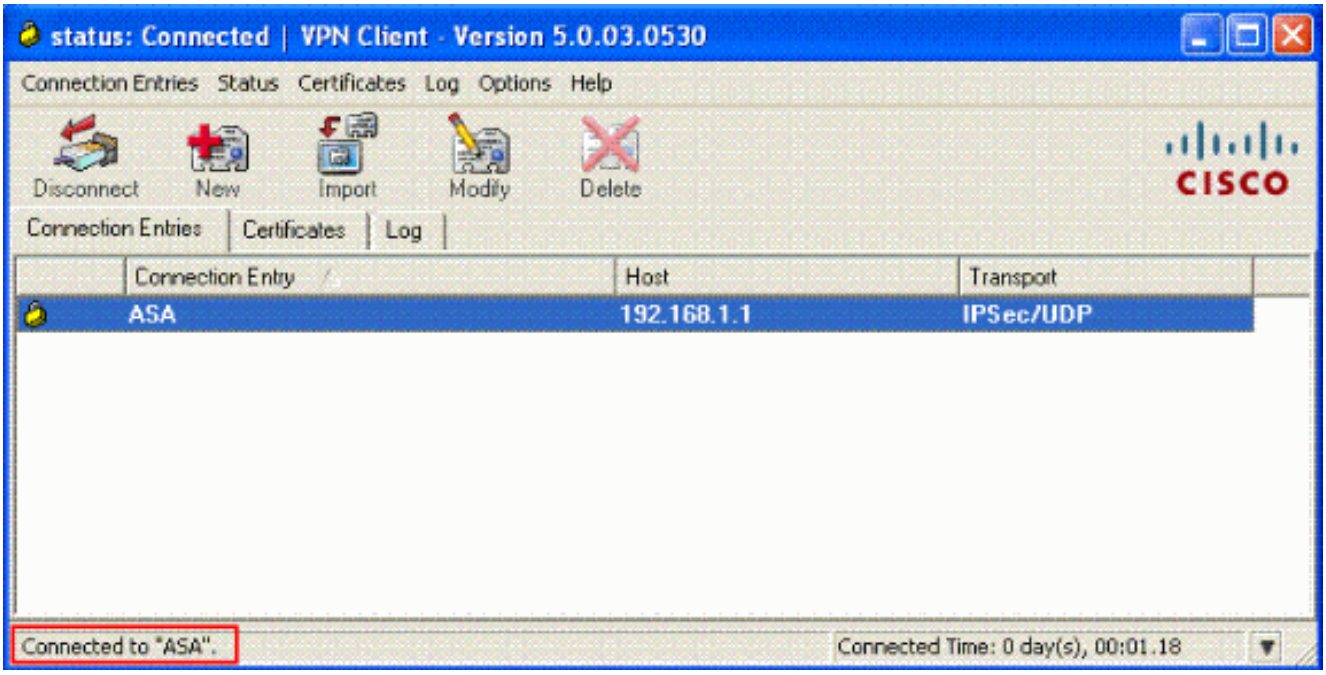



5. Voer desgevraagd de **gebruikersnaam** in **: Cisco** en **Wachtwoord: password1** zoals ingesteld in de ASA voor de toekomst, en klik op **OK** om verbinding te maken met het externe

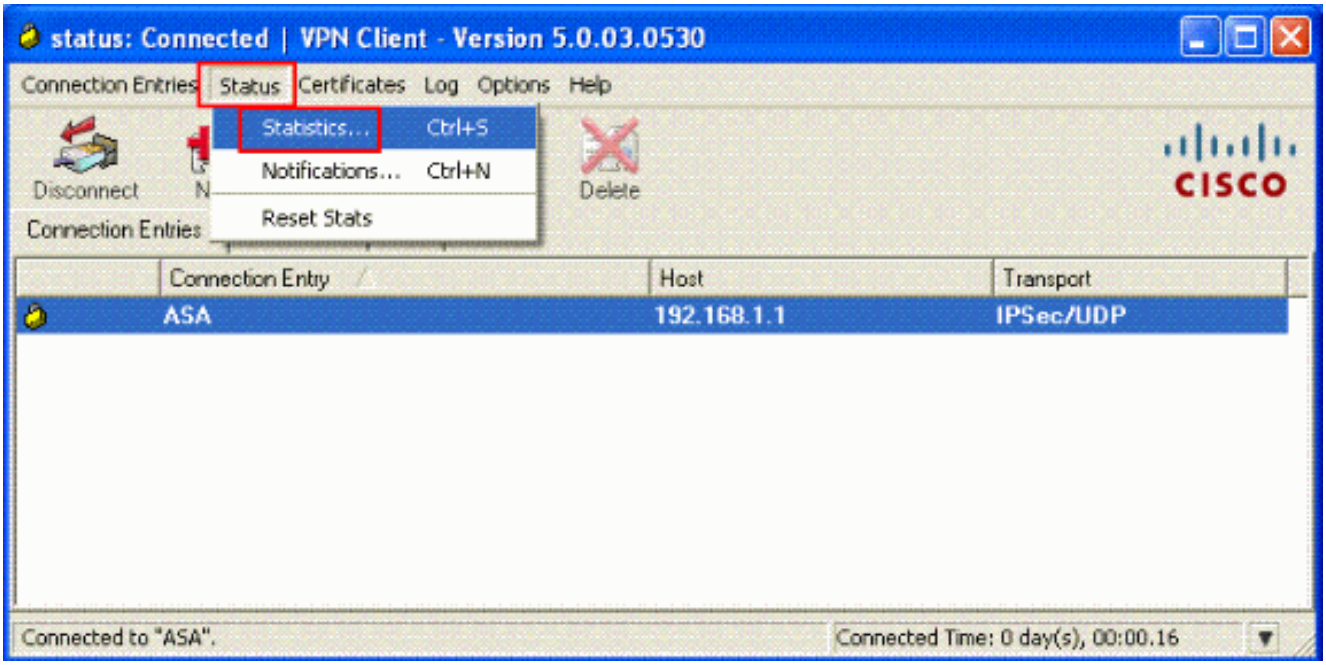



netwerk.

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.



## ACS voor downloadbare ACL voor individuele gebruiker configureren

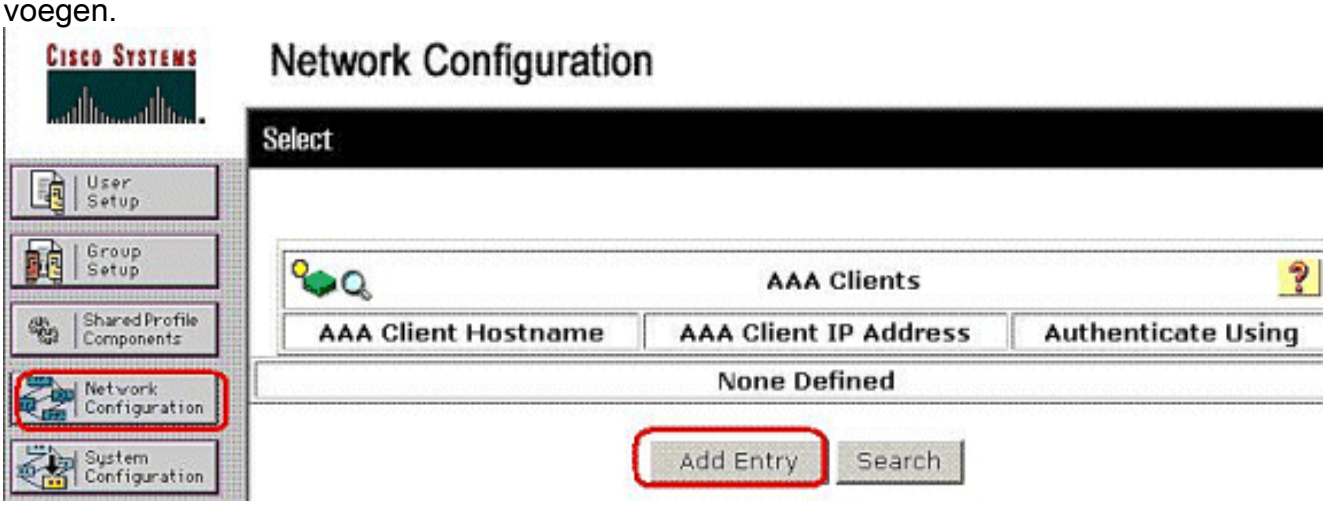
U kunt downloadbare toegangslijsten op Cisco Secure ACS als een gedeelde profielcomponent configureren en vervolgens de toegangslijst toewijzen aan een groep of een individuele gebruiker.

Om dynamische toegangslijsten uit te voeren, moet u de RADIUS-server configureren om deze te ondersteunen. Als de gebruiker zich echt verklaart, stuurt de RADIUS-server een downloadbare toegangslijst of toegangslijst naar het beveiligingsapparaat. Toegang tot een bepaalde dienst is toegestaan of geweigerd door de toegangslijst. Het security apparaat verwijdert de toegangslijst zodra de verificatiesessie verloopt.

In dit voorbeeld authenticeert de IPSec VPN-gebruiker **"cisco"** en de RADIUS-server stuurt een downloadbare toegangslijst naar het security apparaat. De gebruiker "cisco" heeft alleen toegang tot de 10.1.1.2 server en ontkent alle andere toegang. Om ACL te controleren, zie de Downloadbare ACL voor Gebruiker/Groep.

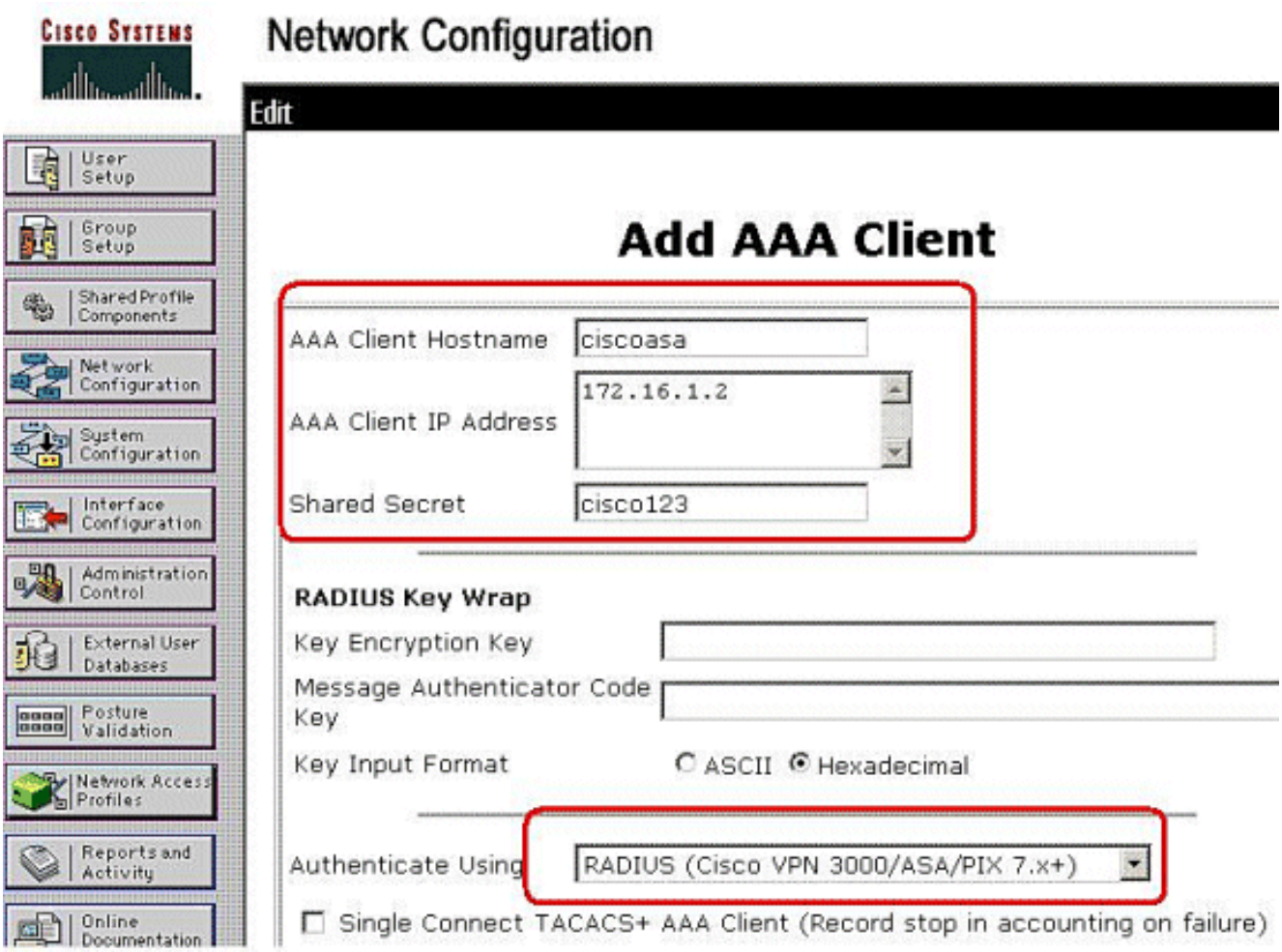
Voltooi deze stappen om RADIUS te configureren in een Cisco Secure ACS.

1. Kies links **netwerkconfiguratie** en klik op **Toegang toevoegen** om een bestandsindeling voor de ASA in de RADIUS-serverdatabase toe te voegen.

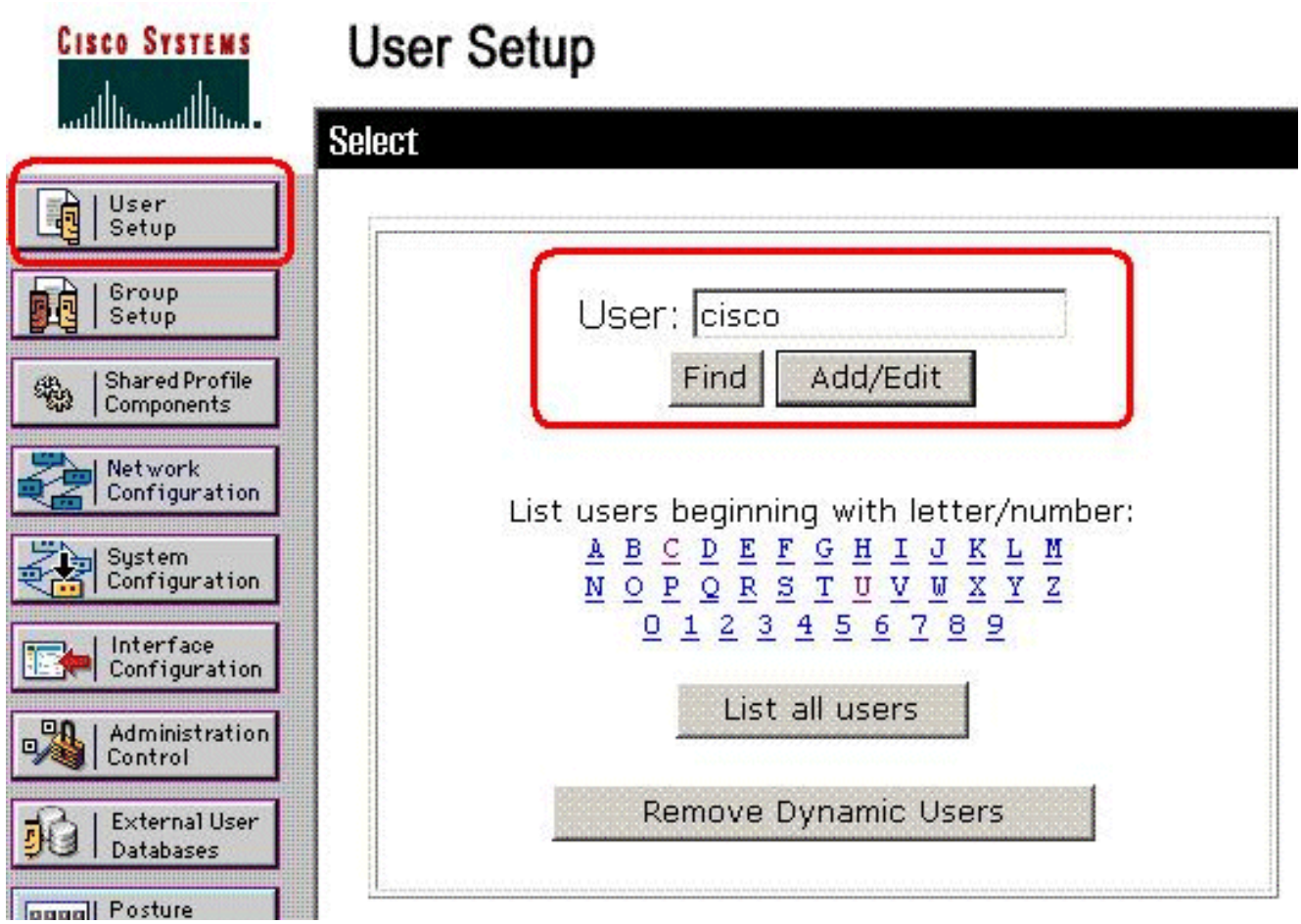



2. Voer **172.16.1.2** in in het veld IP-adres van de client en voer **"cisco123"** in voor het gedeelde geheime veld. Kies **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** in het *Verificeren met* vervolgkeuzelijst. Klik op **Inzenden**.

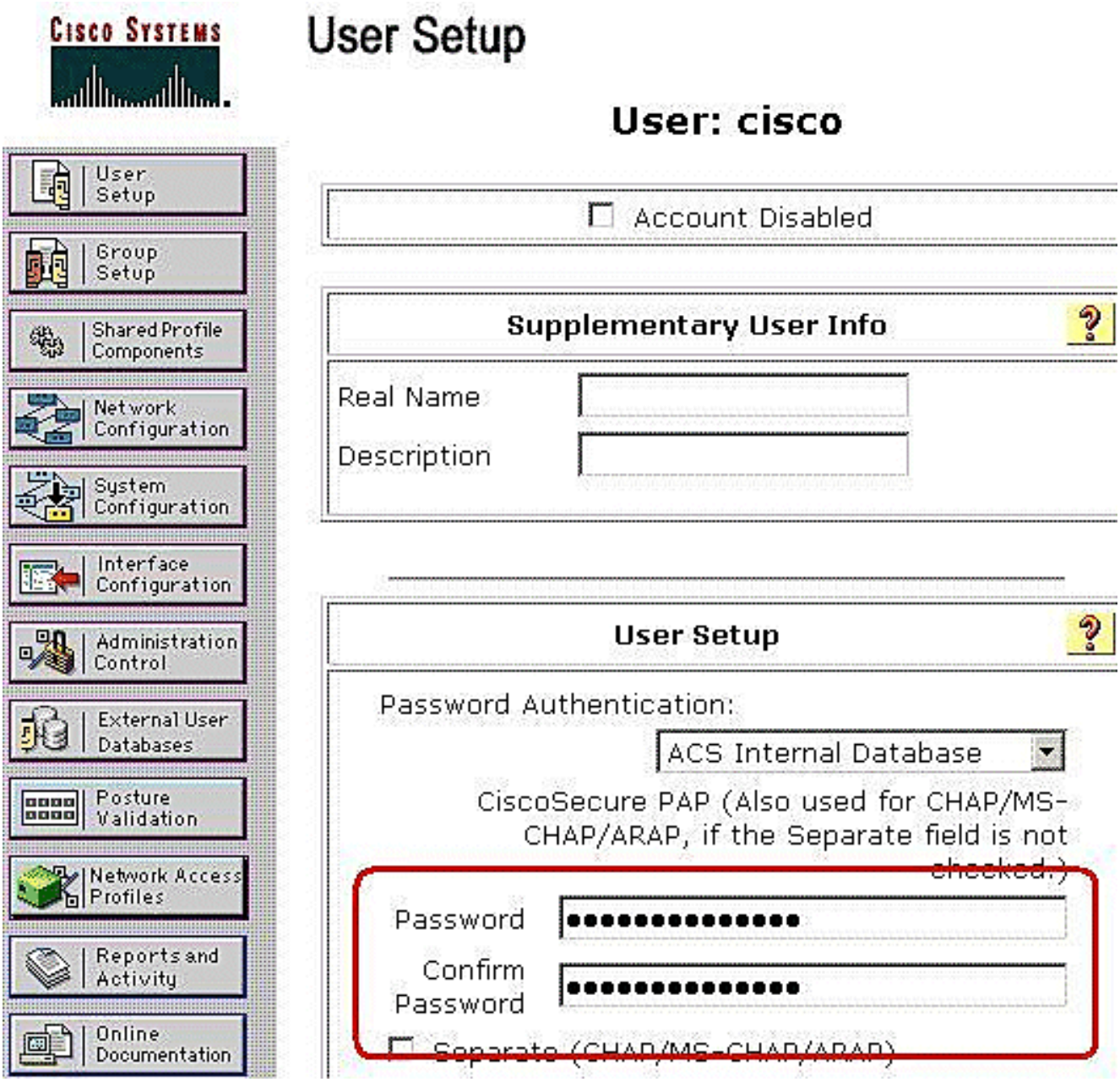
.



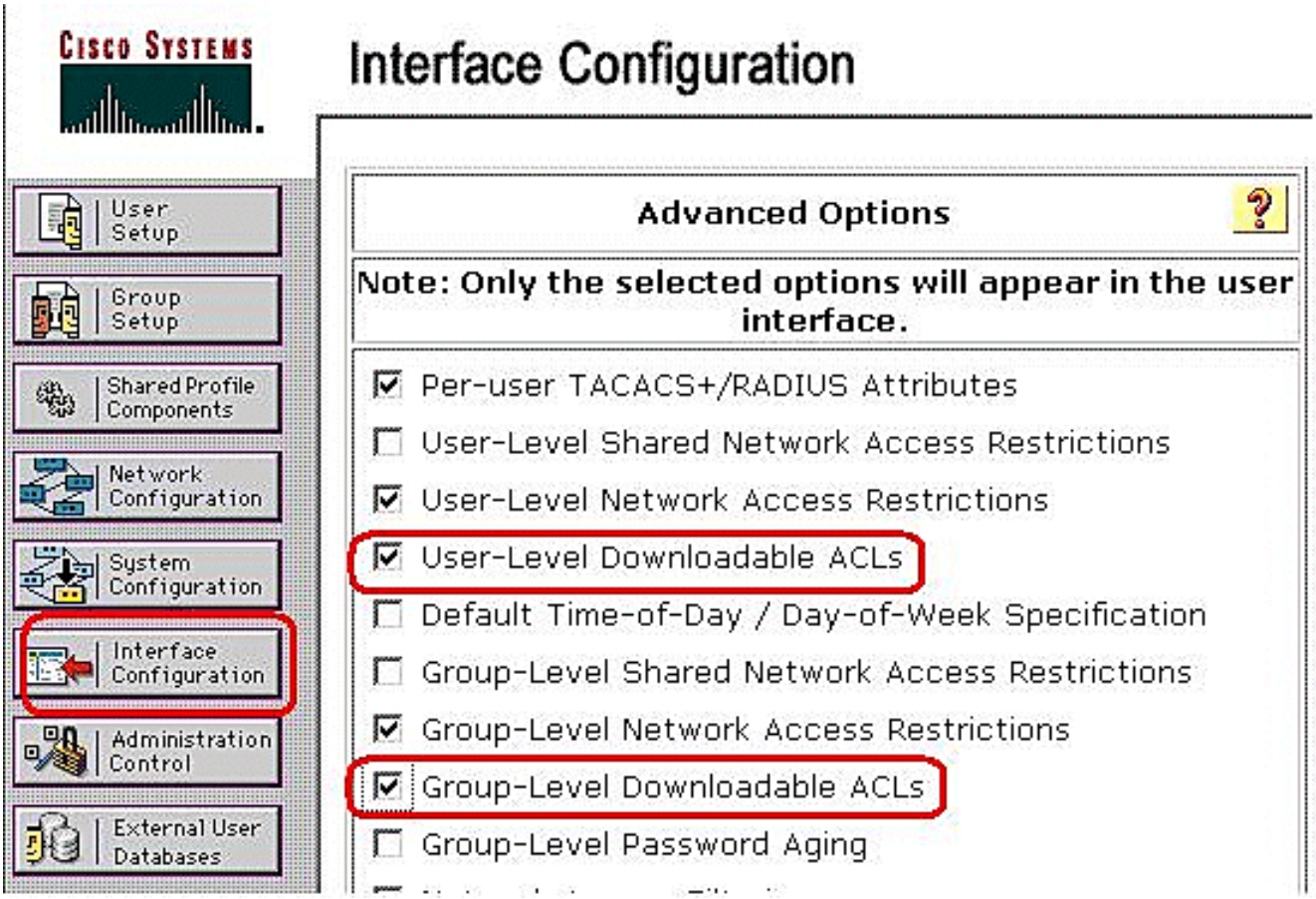

3. Voer de gebruikersnaam in het veld Gebruiker in de Cisco Secure-database in en klik op **Toevoegen/bewerken**.In dit voorbeeld is de gebruikersnaam **Cisco**.




4. Voer in het volgende venster het wachtwoord in voor **"cisco"**. In dit voorbeeld is het wachtwoord ook **wachtwoord 1**. Wanneer u klaar bent, klikt u op **Indienen**.

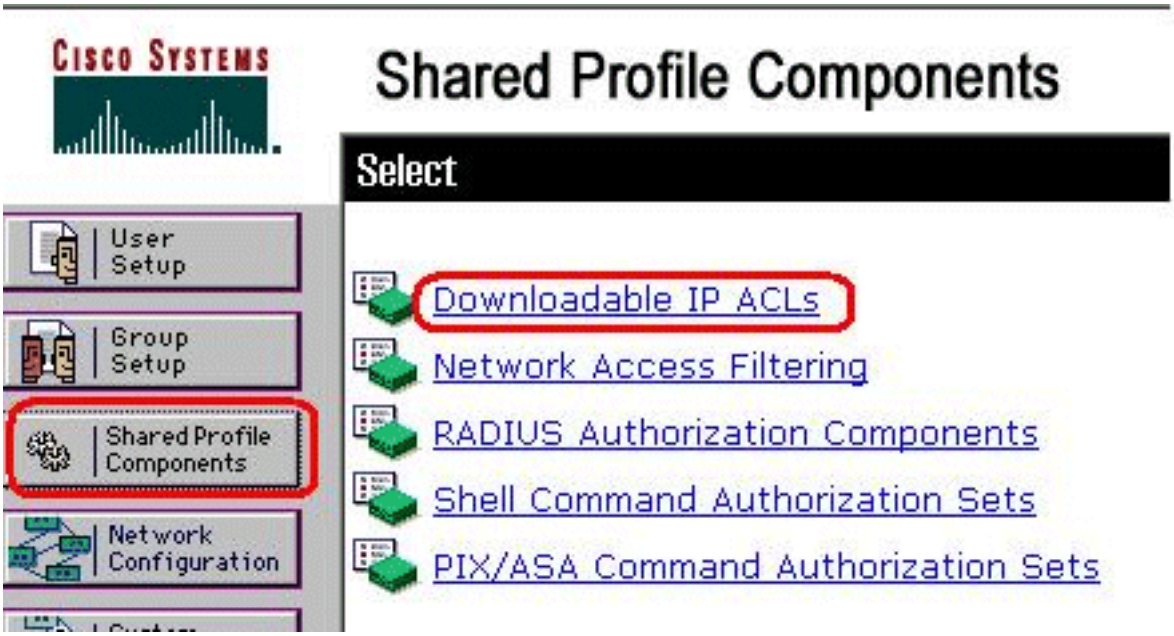



5. U gebruikt de pagina Geavanceerde opties om te bepalen welke geavanceerde opties de ACS-displays weergeven. U kunt de pagina's vereenvoudigen die in andere gebieden van de ACS web interface verschijnen als u de geavanceerde opties verbergen die u niet gebruikt. Klik op **Interface Configuration** en klik vervolgens op **Geavanceerde opties** om de pagina Geavanceerde opties te
openen.

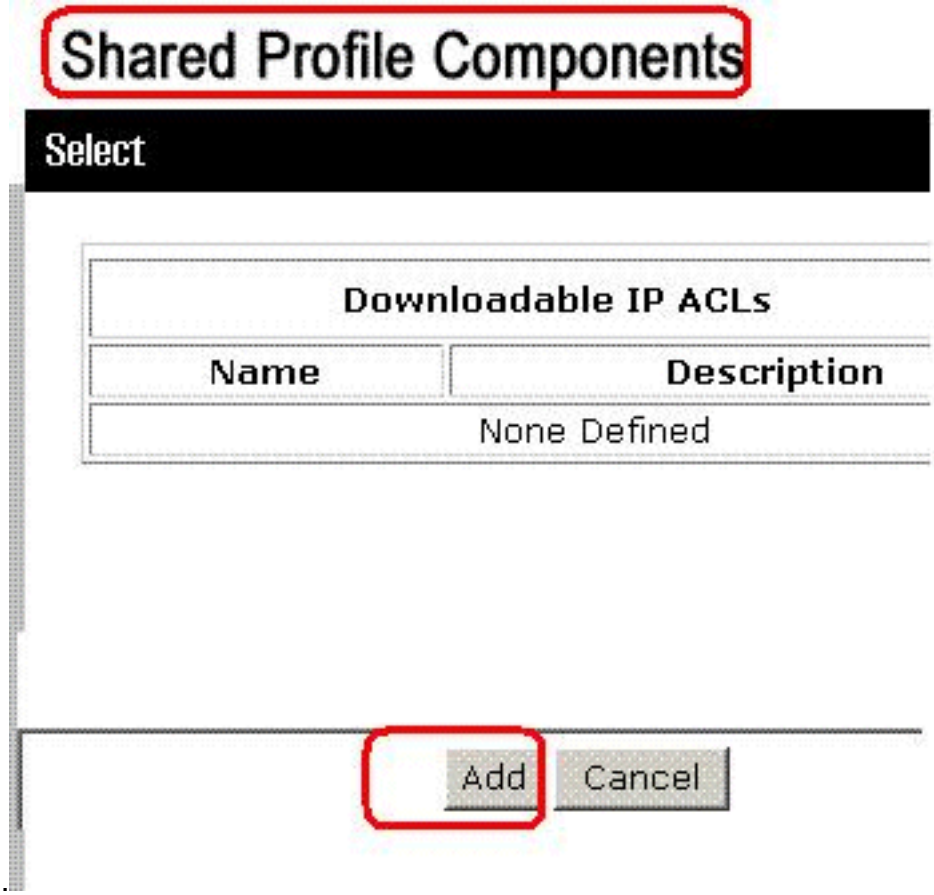



Controleer het vakje voor **door gebruiker** te **downloaden ACL's** en **downloadbare ACL's op groepsniveau**.**Downloadbare ACL's** op **gebruikersniveau** - Wanneer u deze optie kiest, stelt u de sectie Downloadbare ACL's (toegangscontrolelijsten) in op de pagina Gebruikersinstelling.**Downloadbare ACL's op groepsniveau** - Indien geselecteerd, maakt deze optie de sectie Downloadbare ACL's op de pagina Groepsinstallatie mogelijk.

6. Klik in de navigatiebalk op **Shared Profile Componenten** en klik op **Downloadbare IP-ACL's**.**N.B.:** Als *IP-ACL's* niet op de pagina Shared Profile Componenten worden weergegeven, moet u Downloadbare ACL's op gebruikersniveau, downloadbare ACL's op groepsniveau of beide op de pagina Advanced Opties van het gedeelte Interface Configuration inschakelen.

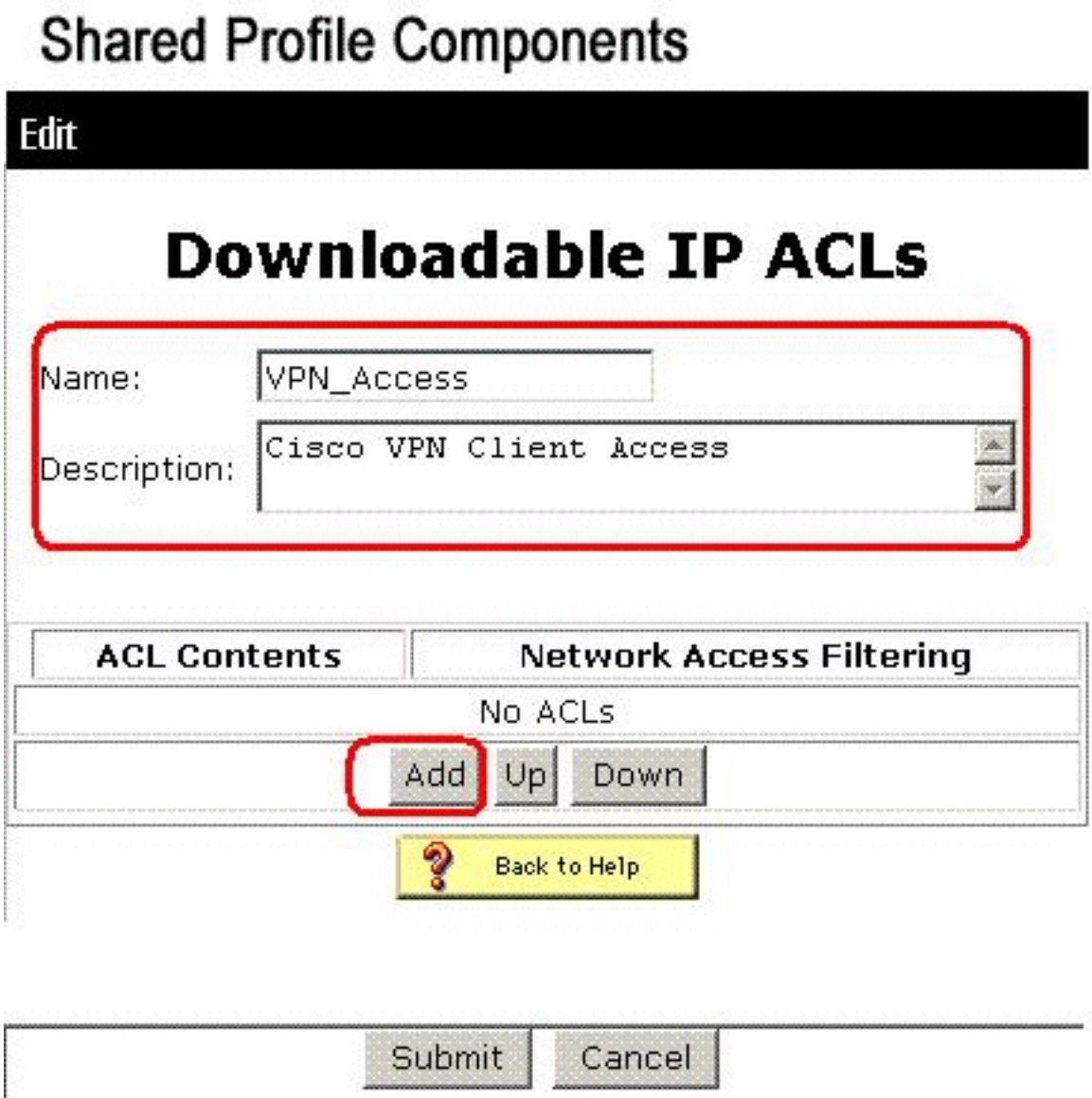



7. Klik op **Toevoegen**. De pagina Downloadbare IP ACL's wordt



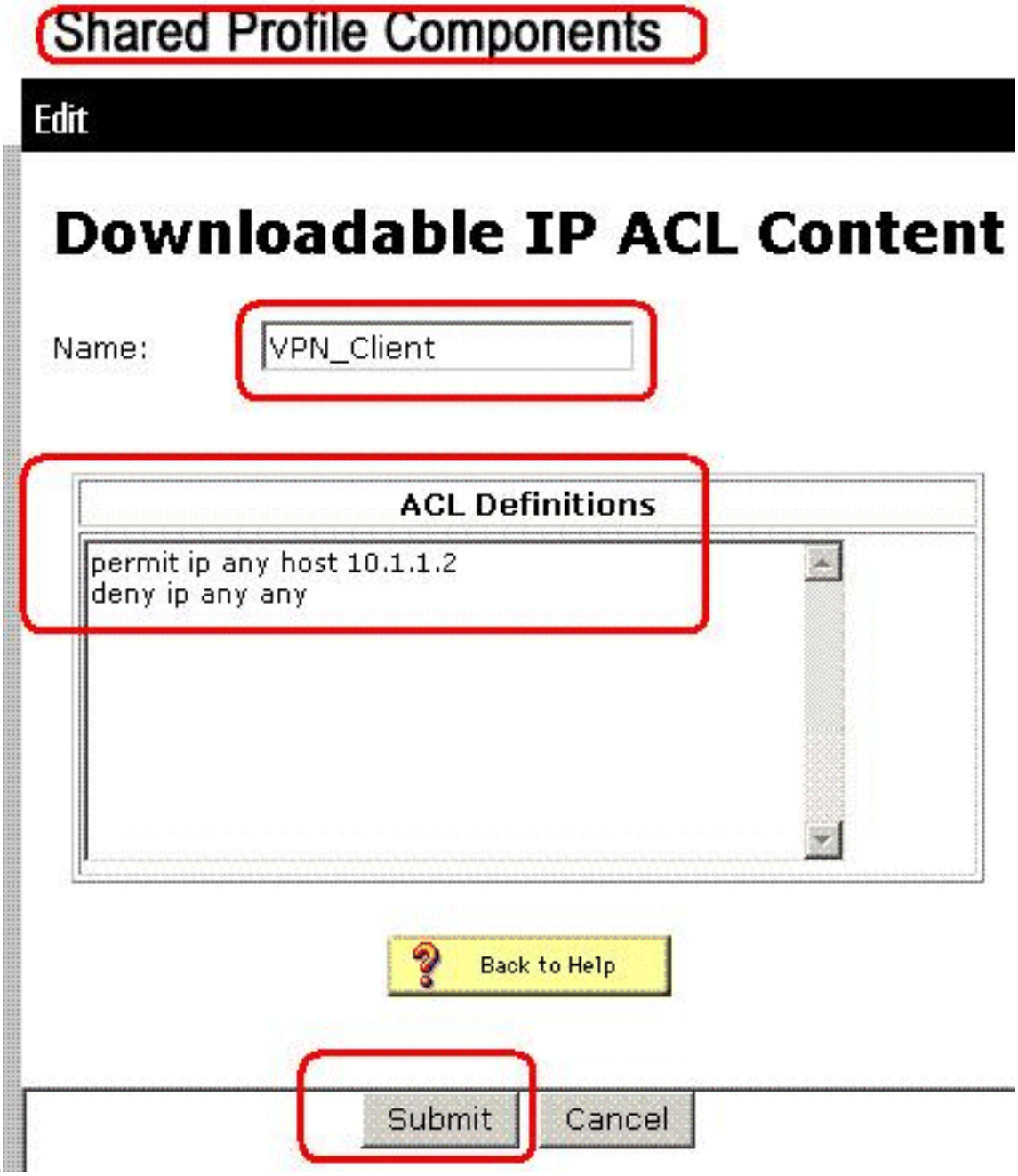

weergegeven.

8. Typ in het vak Naam de naam van de nieuwe IP-ACL.**Opmerking:** de naam van een IP ACL kan maximaal 27 tekens bevatten. De naam mag geen spaties of tekens van deze tekens bevatten: koppelteken (-), linkerbeugel ([), rechterbeugel (]), slash (/), backslash (\), offertes ("), linkerhoekbeugel (<), rechterhoekbeugel (>) of stippelrand (-).Typ in het vak Description een beschrijving van de nieuwe IP-ACL. De beschrijving kan maximaal 1000 tekens



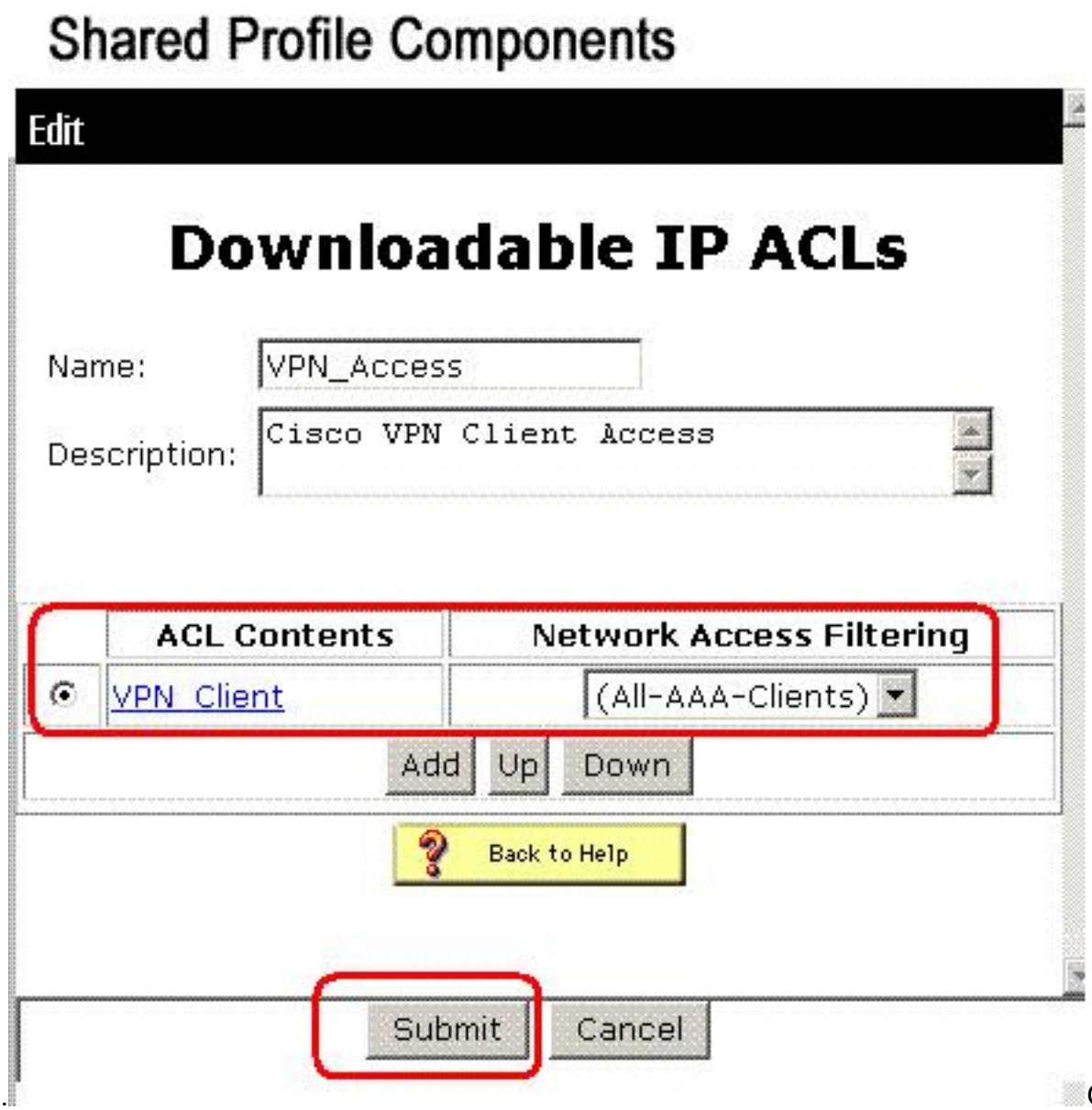

bevatten. Al
s u een ACL-inhoud aan de nieuwe IP ACL wilt toevoegen, klikt u op **Toevoegen**.

9. Typ in het vak Naam de naam van de nieuwe ACL-inhoud.**Opmerking:** de naam van een ACL-inhoud kan maximaal 27 tekens bevatten. De naam mag geen spaties of tekens van deze tekens bevatten: koppelteken (-), linkerbeugel ([), rechterbeugel (]), slash (/), backslash (\), offertes ("), linkerhoekbeugel (<), rechterhoekbeugel (>) of stippelrand (-).Typ in het vak ACL-definities de nieuwe ACL-definitie.**Opmerking:** Wanneer u de ACL-definities in de ACS-web interface invoert, gebruik dan geen sleutelwoord of naamvermeldingen; begin met een vergunning of ontken sleutelwoord.Om de ACL-inhoud op te slaan klikt u op




**Inzenden**.

10. De pagina Downloadbare IP ACL's wordt weergegeven met de nieuwe ACL-inhoud die in de kolom Inhoud van ACL bij naam is vermeld. Om een NAF aan de ACL inhoud te associëren, kies een NAF van het vakje van de Toegang van het Netwerk aan het recht van de nieuwe ACL inhoud. Standaard is NAF (All-AAA-Clients). Als u geen NAF toewijst, associeert ACS de ACL inhoud aan alle netwerkapparaten, wat de standaard




is. Om de volgorde van de ACL-inhoud in te stellen, klikt u op de radioknop voor een ACL-definitie en vervolgens klikt u op **Up** of **Down** om deze in de lijst te verplaatsen.Om IP ACL op te slaan klikt u op **Inzenden**.**Opmerking:** de volgorde van de ACL-inhoud is aanzienlijk. Van boven naar onder downloads worden alleen de eerste ACL-definitie gedownload die een toepasbare NAF-instelling heeft, die de standaardinstelling voor alle AAA-clients bevat, indien gebruikt. Meestal komt de lijst met ACL-inhoud van de NAF met de meest specifieke (engste) NAF naar de NAF met de meest algemene (All-AAA-Clients) NAF.**Opmerking:** ACS komt in de nieuwe IP ACL, die onmiddellijk van kracht wordt. Als IP ACL bijvoorbeeld bedoeld is voor gebruik met PIX-firewalls, is deze beschikbaar om naar een PIX-firewall te worden verzonden ter verificatie van een gebruiker die IP ACL-ACL kan downloaden, die aan zijn of haar gebruiker of groepsprofiel is toegewezen.

11. Ga naar de pagina Gebruikersinstelling en voer de gebruikerspagina uit. Klik onder het gedeelte Downloadbare ACL's op de **IP-ACL-code toewijzen:** aanvinkvakje. Kies een IP ACL uit de lijst. Als u de configuratie van de gebruikersaccountopties hebt voltooid, klikt u op **Indienen** om de opties op te


nemen.

## ACS voor downloadbare ACL voor groep configureren

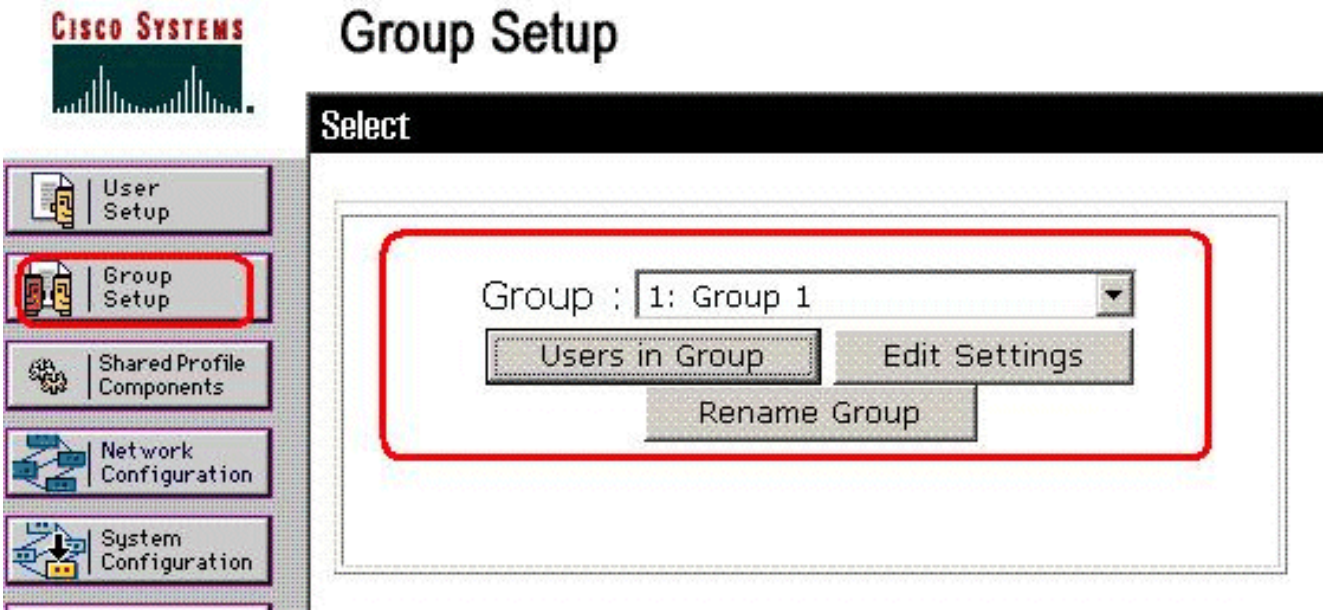
Complete stappen 1 tot en met 9 van het Configureren ACS voor downloadbare ACL voor individuele gebruiker en volg deze stappen om downloadbare ACL voor groep te configureren in een Cisco Secure ACS.

In dit voorbeeld, behoort de IPSec VPN gebruiker "cisco" tot de VPN groepen. Het VPN-groepsbeleid wordt toegepast op alle gebruikers in de groep.

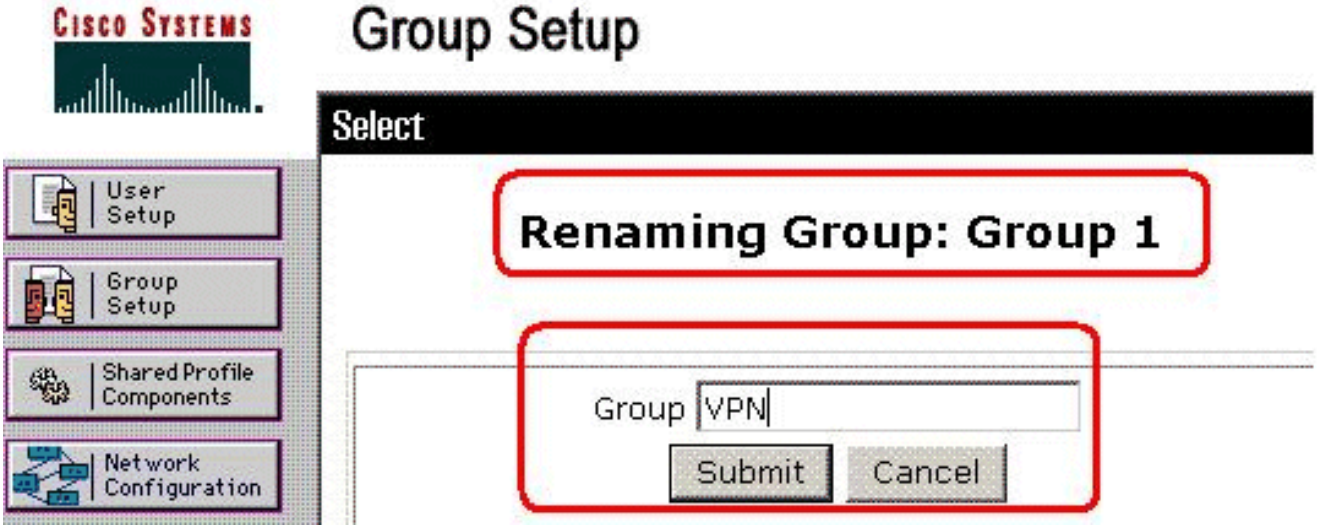
De VPN-groepsgebruiker **"cisco"** wordt geauthentiseerd en de RADIUS-server stuurt een downloadbare toegangslijst naar het security apparaat. De gebruiker "cisco" heeft alleen toegang tot de 10.1.1.2 server en ontkent alle andere toegang. Raadpleeg het gedeelte Downloadbare ACL's om de ACL's te controleren.

1. Klik in de navigatiebalk op **Groepsinstelling**. Selecteer pagina

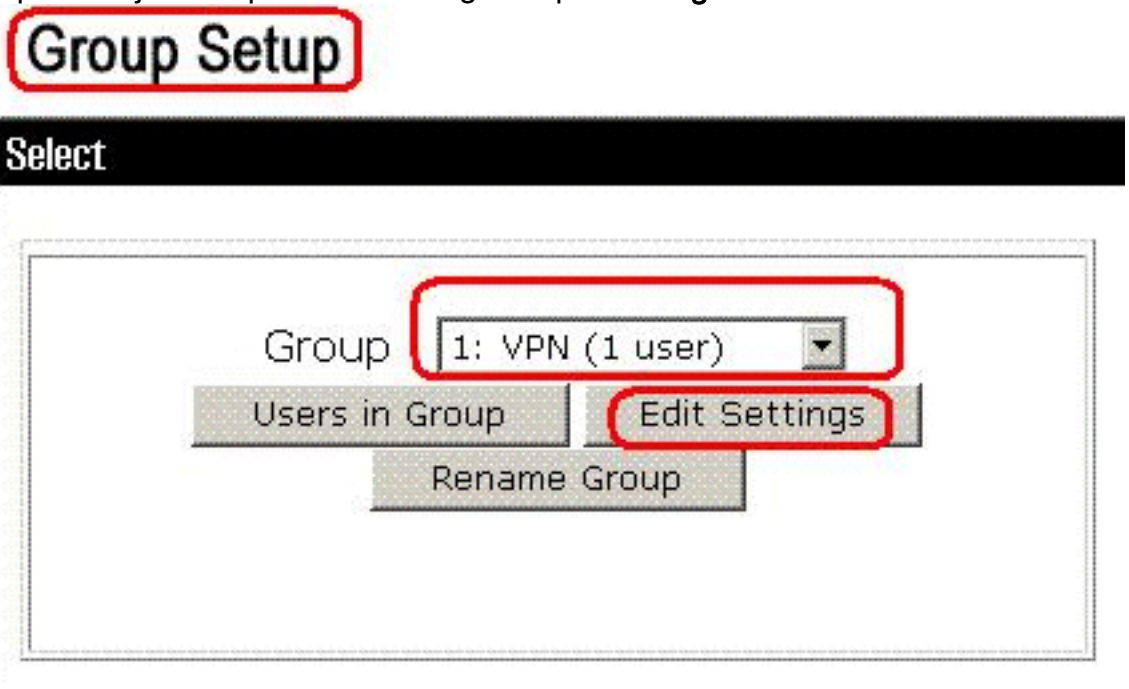
Groepsinstallatie.



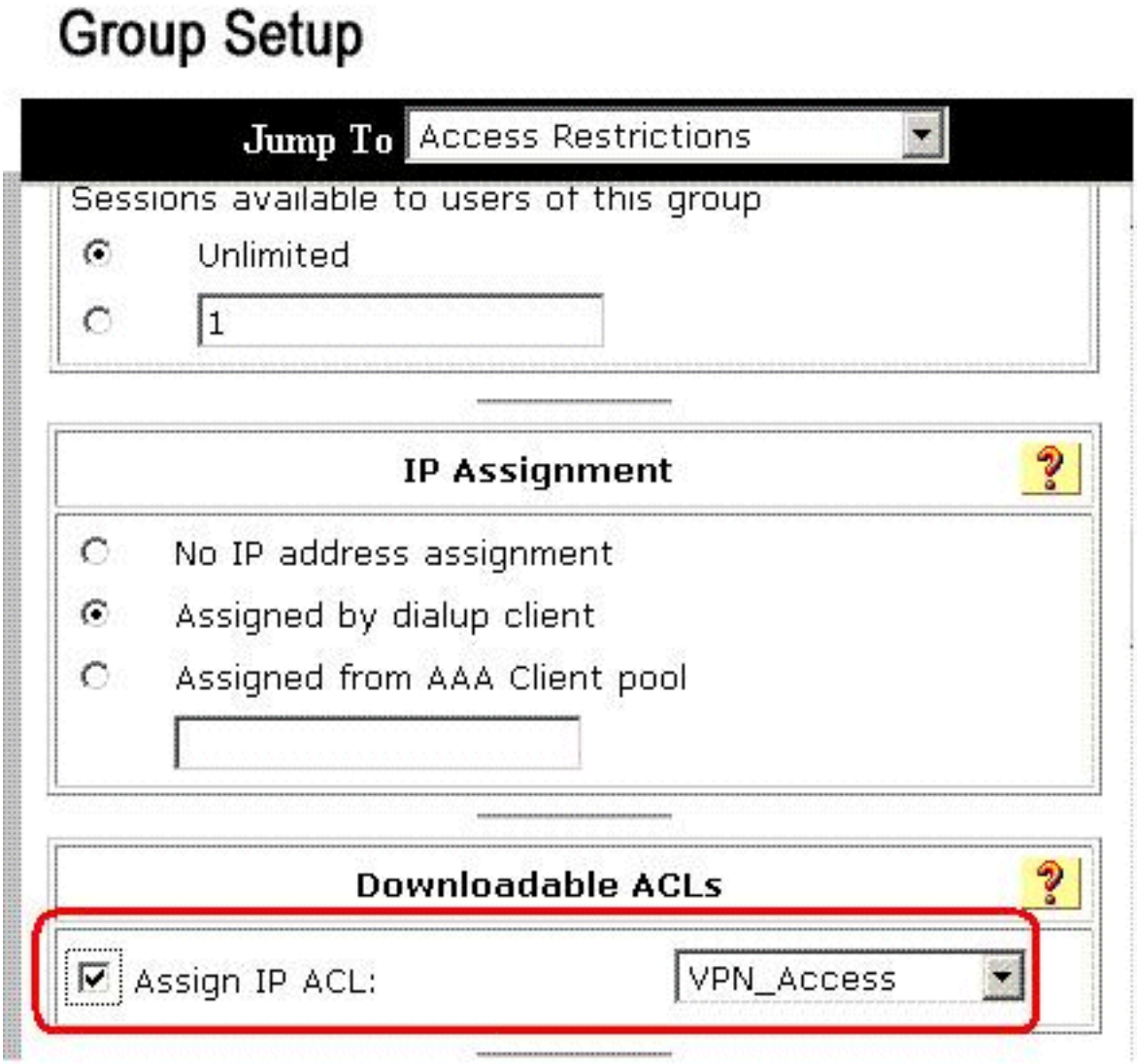

2. Hernoemen Groep 1 aan **VPN** en klik op **Inzenden**.




3. Kies een groep in de lijst Groep en klik vervolgens op **Instellingen bewerken**.

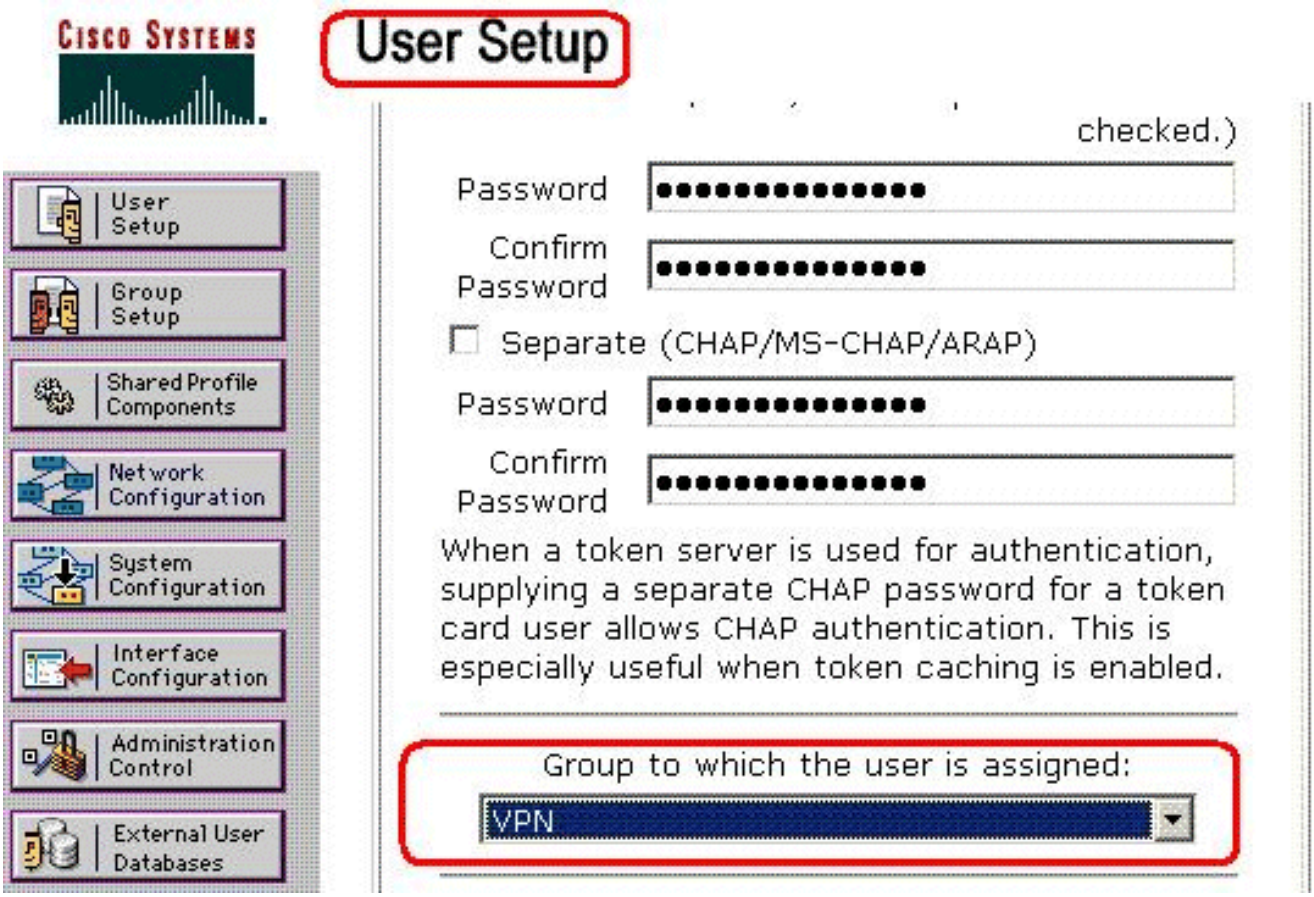


4. Klik onder het gedeelte Downloadbare ACL's op het vakje **IP-ACL-**toewijzing. Kies een IP ACL uit de




lijst.

5. Om de groepsinstellingen op te slaan die u zojuist hebt gemaakt, klikt u op **Inzenden**.
6. Ga naar de gebruikersinstelling en voer de gebruiker uit die u aan de groep wilt toevoegen: **VPN**. Klik op **Inzenden** als u klaar bent.




**Nu wordt de Downloadbare ACL die voor de VPN-groep is ingesteld voor deze gebruiker toegepast**.

7. Om andere groepsinstellingen te blijven specificeren, voert u andere procedures in dit hoofdstuk uit, zoals van toepassing

## RADIUS-instellingen voor IETF configureren voor een gebruikersgroep

Om een naam voor een toegangslijst te downloaden die u al op het security apparaat hebt gemaakt, vanaf de RADIUS-server wanneer een gebruiker de echtheid van het filter van de IETF RADIUS-id (attribuut nummer 11):

```
filter-id=acl_name
```

De VPN-groepsgebruiker **"cisco"** bevestigt deze verificatie en de RADIUS-server downloads een ACL-naam (nieuw) voor een toegangslijst die u al op het security apparaat hebt gemaakt. De gebruiker "cisco" kan toegang hebben tot alle apparaten die binnen het netwerk van de ASA **behalve** de 10.1.1.2 server zijn. Zie het gedeelte Filter-ID ACL om de ACL te controleren.

Zoals in het voorbeeld, wordt ACL genoemd **nieuw** gevormd voor het filteren in ASA.

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

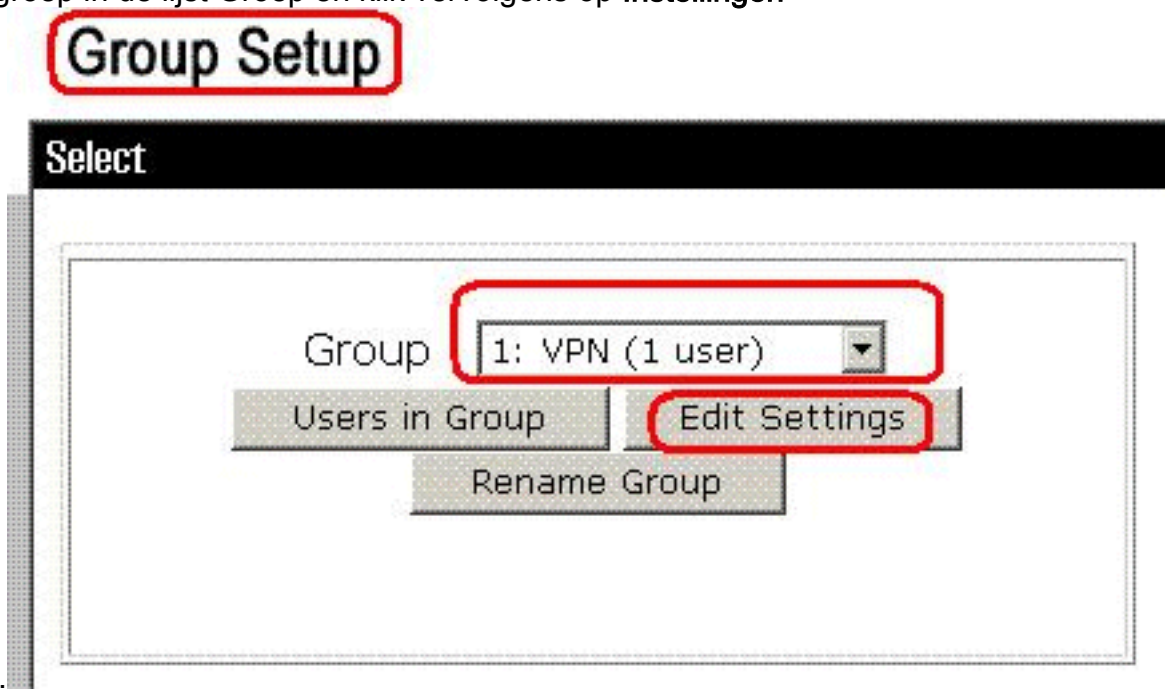
Deze parameters verschijnen alleen wanneer ze waar zijn. U hebt ingesteld

- AAA-client voor gebruik van een RADIUS-protocol in netwerkconfiguratie
- RADIUS-kenmerken op groepsniveau op de RADIUS-pagina (IETF) in het gedeelte Interface Configuration van de webinterface

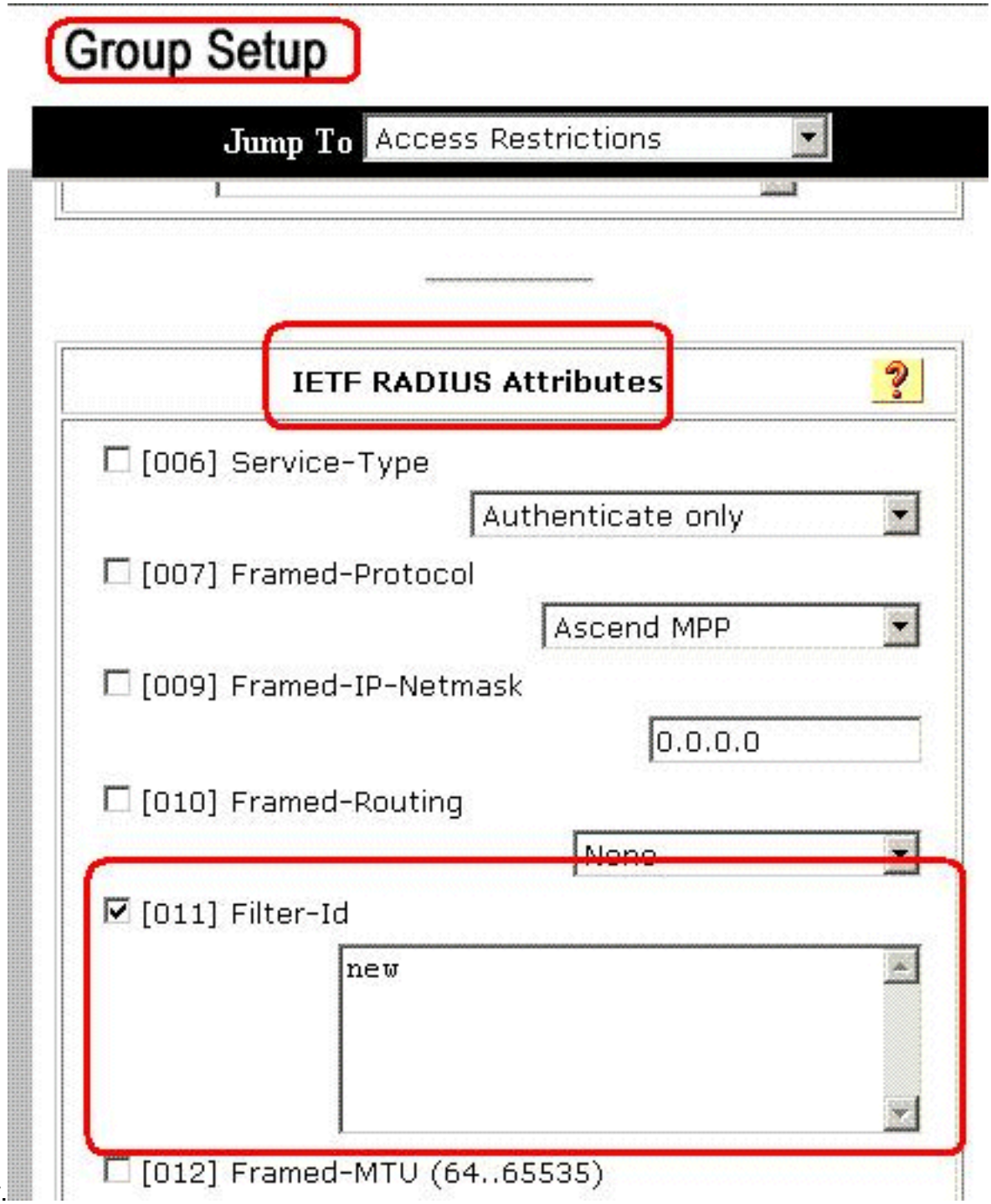
RADIUS-eigenschappen worden als profiel voor elke gebruiker van ACS naar de verzoekende AAA-client verzonden.

Om de instellingen van de eigenschap IETF aan te passen om als vergunning voor elke gebruiker in de huidige groep toe te passen, voert u deze acties uit:

1. Klik in de navigatiebalk op **Groepsinstelling**.Selecteer pagina Groepsinstallatie.
2. Kies een groep in de lijst Groep en klik vervolgens op **Instellingen**




**bewerken**.
De naam van de groep verschijnt boven op de pagina Instellingen groep.
3. Scrolt naar de IEFT RADIUS-kenmerken. Voor elke RADIUS-eigenschap van IETF moet u de huidige groep autoriseren. Controleer het aanvinkvakje van de eigenschap **[011] Filter-ID** en voeg vervolgens de ASA gedefinieerde ACL-naam (**nieuw**) toe aan de autorisatie voor de eigenschap in het veld. Raadpleeg de ASA *show-configuratie*




uitvoer.

4. Om de groepsinstellingen op te slaan die u zojuist hebt gemaakt en deze direct toe te passen, klikt u op **Inzenden** en **Toepassen**.**N.B.:** Als u de groepsinstellingen wilt opslaan en deze later wilt toepassen, klikt u op **Inzenden**. Wanneer u de wijzigingen wilt implementeren, kiest u **Systeemconfiguratie > Servicebeheer**. Kies vervolgens **Start opnieuw**.

## Verifiëren

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.

### Crypto opdrachten tonen

- **toon crypto isakmp sa**-toont alle huidige IKE Security Associations (SAs) bij een peer.

```
ciscoasa# sh crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active
   and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.10.2
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
ciscoasa#
```

- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige SA's.

```
ciscoasa# sh crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1,
   local addr: 192.168.1.1

      local ident (addr/mask/prot/port):
   (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
   (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.10.2, username: cisco
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 65, #pkts encrypt:
   65, #pkts digest: 65
      #pkts decaps: 65, #pkts decrypt:
   65, #pkts verify: 65
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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.: 192.168.1.1,
   remote crypto endpt.: 192.168.10.2

      path mtu 1500, ipsec overhead 58,
   media mtu 1500
      current outbound spi: EEF0EC32

    inbound esp sas:
      spi: 0xA6F92298 (2801345176)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec):
   28647
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xEEF0EC32 (4008766514)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec): 28647
         IV size: 8 bytes
```

```
            replay detection support: Y
```

## Downloadbare ACL voor gebruiker/groep

Controleer de downloadbare ACL voor de gebruiker Cisco. ACL's worden gedownload van het CSACS.

```
ciscoasa(config)# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
   192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411

access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic)
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
   ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
   ip any any (hitcnt=40) 0x7c718bd1
```

## Filter-ID ACL

De [101] Filter-ID is toegepast voor de groep - VPN, en gebruikers van de groep worden gefilterd volgens de ACL (nieuw) die in de ASA is gedefinieerd.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
   255.255.255.0 192.168.5.0 255.255.255.0
   (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip
   any host 10.1.1.2 (hitcnt=4) 0xb247fec8
access-list new line 2 extended permit ip any any
   (hitcnt=39) 0x40e5d57c
```

# Problemen oplossen

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

**Opmerking:** Raadpleeg voor meer informatie over het oplossen van problemen bij externe toegang IPSec VPN de meest gebruikelijke oplossingen voor probleemoplossing bij L2L en externe toegang 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 adaptieve security apparaatbeheer
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Cisco VPN-clientondersteuningspagina
- Cisco Secure Access Control Server voor Windows
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems