Lock-and-Key: Dynamische toegangslijsten

Inhoud

Inleiding

De toegang op het slot en de sleutel staat u toe om dynamische toegangslijsten in te stellen die per gebruiker toegang tot een specifieke bron/bestemming gastheer door een proces van gebruikersauthenticatie verlenen. Gebruikerstoegang is dynamisch toegestaan door een Cisco IOS® Firewall zonder enig compromis in de beveiligingsbeperkingen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. In dit geval bestond de labomgeving uit een 2620 router die Cisco IOS®-softwarerelease 12.3(1) runde. 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.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Overdenkingen

De toegang op het slot en de sleutel staat een externe gebeurtenis toe om een opening in de Cisco IOS Firewall te plaatsen. Nadat deze opening bestaat, is de router vatbaar voor bron adres spoofing. Om dit te voorkomen, moet u coderingsondersteuning bieden door IP-encryptie te gebruiken met verificatie of encryptie.

Spoofing is een probleem met alle bestaande toegangslijsten. De toegang op slot en toets lost dit probleem niet op.

Omdat de toegang op slot en sleutel een mogelijk pad door uw netwerkfirewall introduceert, moet u dynamische toegang overwegen. Een andere host, die uw geauthentiseerd adres overslaat, krijgt toegang achter de firewall. Dankzij dynamische toegang is er de mogelijkheid dat een niet-geautoriseerde host, die uw geauthentiseerd adres spaart, toegang krijgt achter de firewall. De toegang op slot en sleutel veroorzaakt niet het probleem van adresspoofing. Het probleem wordt hier alleen geïdentificeerd als een probleem voor de gebruiker.

Prestaties

De prestaties worden in deze twee situaties beïnvloed.

- Elke dynamische toegangslijst dwingt een toegangslijst opnieuw op te bouwen op de siliciumschakelmachine (SSE). Dit veroorzaakt dat de SSE switchingpad tijdelijk vertraagt.
- Dynamische toegangslijsten vereisen de faciliteit van de ongebruikte tijd (zelfs als de tijd wordt verlaten om in gebreke te blijven). Daarom kunnen dynamische toegangslijsten niet worden gewijzigd. Deze items worden verwerkt in het protocol fast-switching pad.

Kijk naar de configuratie van de grensrouter. Afstandsgebruikers maken access list items op de grensrouter aan. De toegangslijst wordt dynamisch versterkt en verkleind. Vermeldingen worden dynamisch van de lijst verwijderd nadat de periode tussen het uitwijken of de max-timeout is verlopen. Grote toegangslijsten degraderen pakketswitchprestaties.

Wanneer gebruiken Lock-and-Key Access

Hier worden twee voorbeelden gegeven van het gebruik van toegang op slot en sleutel:

- Wanneer u wilt dat een externe host via het internet toegang heeft tot een host in uw internetwerk. Toegang op slot en sleutel beperkt de toegang tot voorbij uw firewall op een individuele host of netto basis.
- Wanneer u een subset van hosts op een netwerk wilt gebruiken om toegang te krijgen tot een host op een extern netwerk dat door een firewall wordt beschermd. Met toegang op slot en sleutel kunt u slechts een gewenste set hosts toegang verkrijgen door ze via een TACACS+- of RADIUS-server te laten authenticeren.

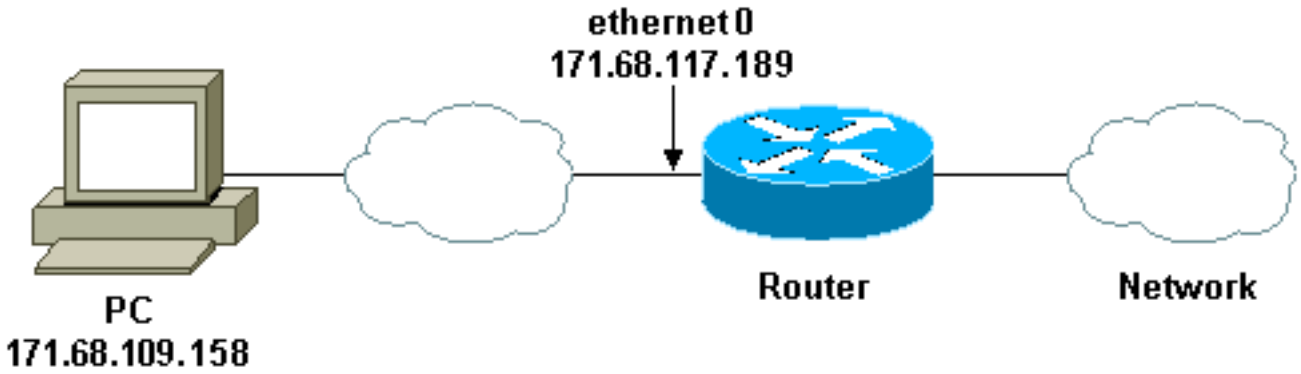
Handeling met vergrendeling en toegang rechtstreeks

Dit proces beschrijft de toegangscontrole op de vergrendeling en de toets.

1. Een gebruiker opent een Telnet-sessie naar een grensrouter die is geconfigureerd voor toegang op slot en sleutel.
2. De Cisco IOS-software ontvangt het Telnet-pakket. Het voert een gebruikersverificatieproces uit. De gebruiker moet de authenticatie doorlopen voordat toegang wordt toegestaan. Het authenticatieproces wordt uitgevoerd door de router of een centrale toegangsserver zoals een TACACS+ of RADIUS-server.

Configuratie- en probleemoplossing

Netwerkdiagram



Cisco raadt u aan een TACACS+ server te gebruiken voor uw verificatiezoekproces. TACACS+ biedt verificatie-, autorisatie- en boekhouddiensten. Het biedt ook protocolondersteuning, protocolspecificatie en een gecentraliseerde beveiligingsdatabase.

U kunt de gebruiker op de router of met een TACACS+- of RADIUS-server voor echt maken.

OPMERKING: Deze opdrachten zijn mondiaal, tenzij anders aangegeven.

Op de router hebt u een **gebruikersnaam** nodig voor de gebruiker voor lokale verificatie.

```
username test password test
```

Door de **lokale** aanwezigheid van **inlognamen** op de vele lijnen kan deze gebruikersnaam worden gebruikt.

```
line vty 0 4
login local
```

Als u de gebruiker niet vertrouwt op het geven van de **toegangscontrolelijn**, kunt u één van twee dingen doen:

- Associeer de tijdelijke versie met de gebruiker op basis van per gebruiker.

```
username test autocommand access-enable host
timeout 10
```

of

- Dwing alle gebruikers die telnet binnen om de zelfde tijd te hebben.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

Opmerking: de **10** in de syntaxis is van *de* stille tijd van de toegangslijst. Het wordt overbrugd door de absolute time-out in de dynamische toegangslijst.

Defineert een uitgebreide toegangslijst die wordt toegepast wanneer een gebruiker (enige gebruiker) zich in de router inlogt en het **access-enabled** bevel wordt uitgegeven. De maximale absolute tijd voor dit "gat" in het filter is ingesteld op 15 minuten. Na 15 minuten sluit het gat, of iemand het al dan niet gebruikt. De **testlijst** van de naam moet bestaan, maar is niet belangrijk. Beperk de netwerken waartoe de gebruiker toegang heeft, door het bron- of doeladres te configureren (hier is de gebruiker niet beperkt).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Bepaal de toegangslijst die nodig is om alles behalve de mogelijkheid om in de router te tellen (om een gat te openen moet de gebruiker telnet aan de router). Het IP-adres hier is het Ethernet IP-adres van de router.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Er bestaat impliciet een **ontkenning** van **alles** aan het eind (niet hier ingevoerd).

Pas deze toegangslijst toe op de interface waarop de gebruikers verschijnen.

```
interface ethernet1
       ip access-group 120 in
```

Je bent klaar.

Dit is hoe het filter er nu uitziet op de router:

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

De gebruikers die toegang tot uw intern netwerk krijgen kunnen niets zien tot zij telnet aan de router.

Opmerking: 10 hier is de *stille* tijd van de toegangslijst. Het wordt overbrugd door de absolute

time-out in de dynamische toegangslijst.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

Het filter ziet er zo uit.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Er zit een gat in het filter voor deze gebruiker op basis van het IP-adres van de bron. Als iemand anders dit doet, zie je *twee gaten*.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Deze gebruikers kunnen volledige IP toegang tot om het even welk bestemming IP adres van hun *bron* IP adres hebben.

TACACS+ gebruiken

TACACS+ configureren

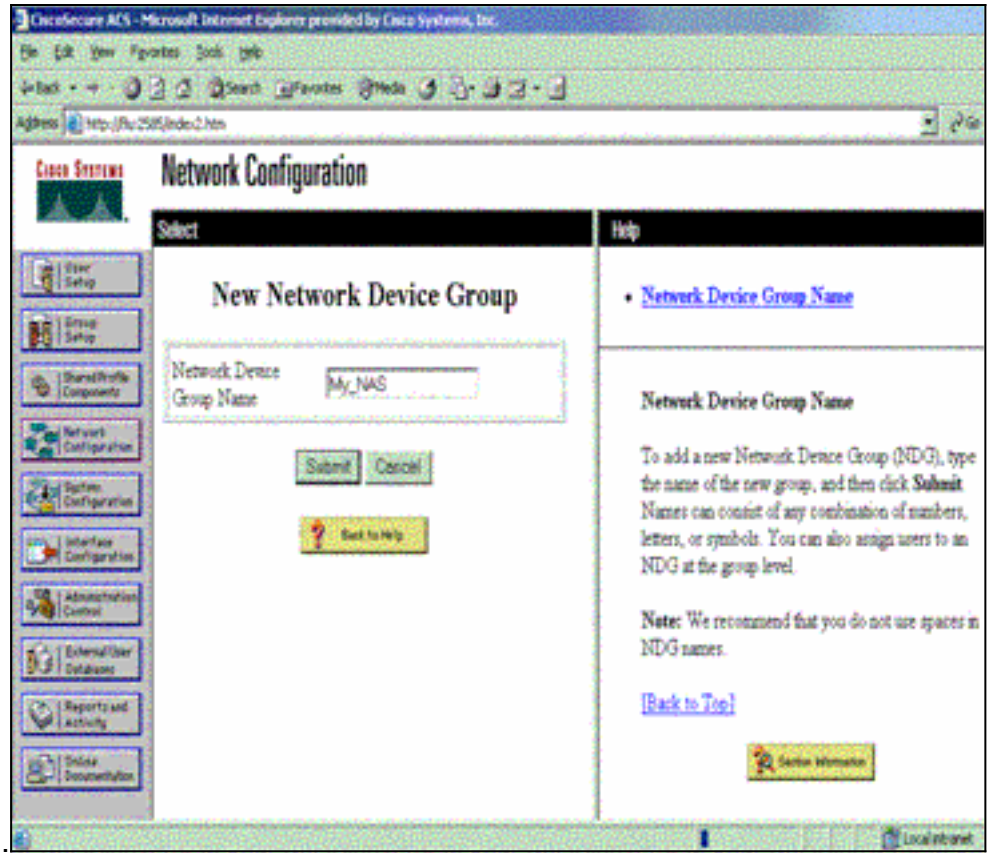
Configureer een TACACS+ server om verificatie en autorisatie op de TACACS+ server af te dwingen zodat deze TACACS+ kan gebruiken, zoals deze uitvoer aantoont:

```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

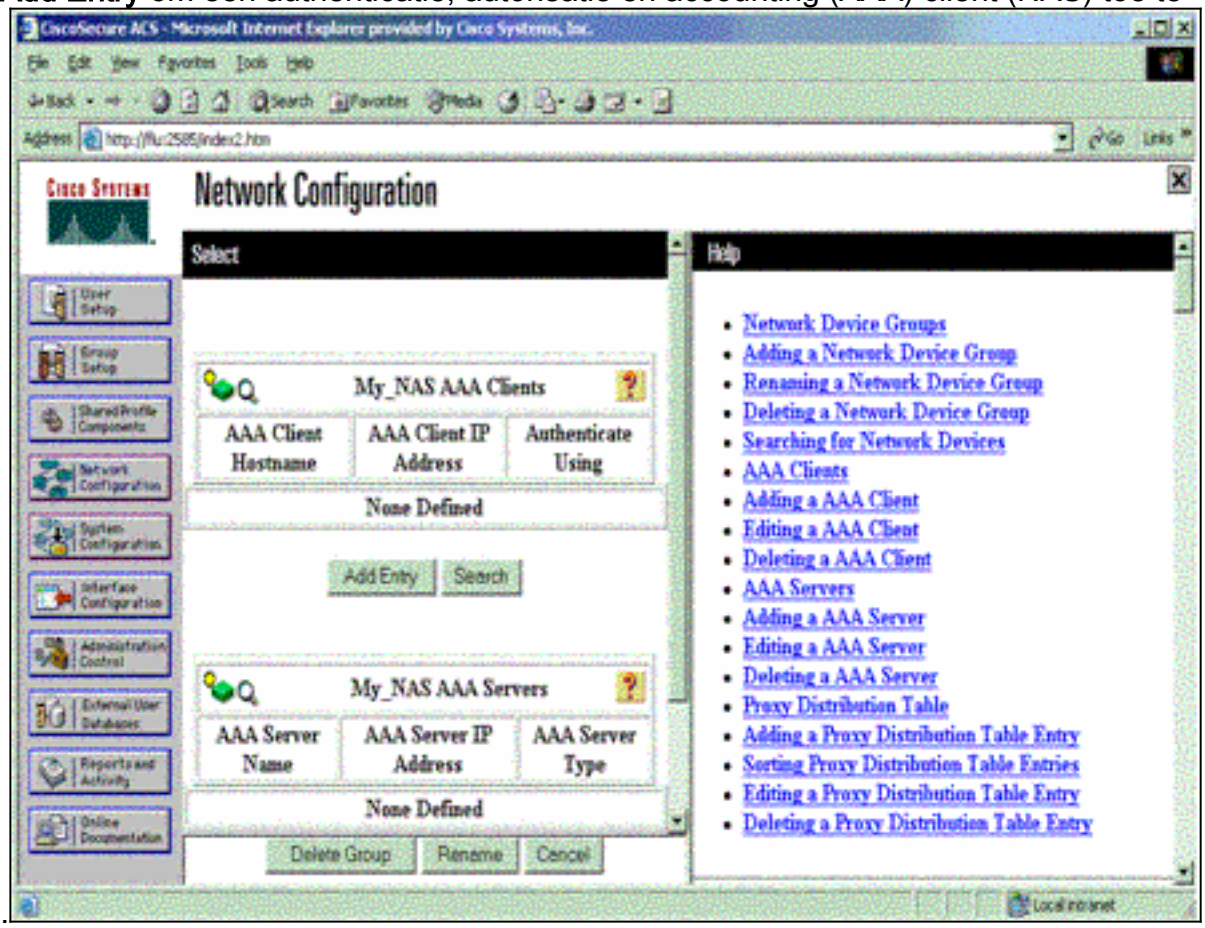
Voltooi deze stappen om TACACS+ te configureren op Cisco Secure ACS voor Windows:

1. Open een webbrowser. Voer het adres in van uw ACS-server, die in de vorm van **http://** is*<IP_adres of DNS_name>:2002*. (Dit voorbeeld gebruikt een standaardpoort van 2002.) Inloggen als beheerder.
2. Klik op **Netwerkconfiguratie**. Klik op **Add Entry** om een Network Devices Group te maken die de netwerktoegangsservers (NAS) bevat. Voer een naam in voor de groep en klik op

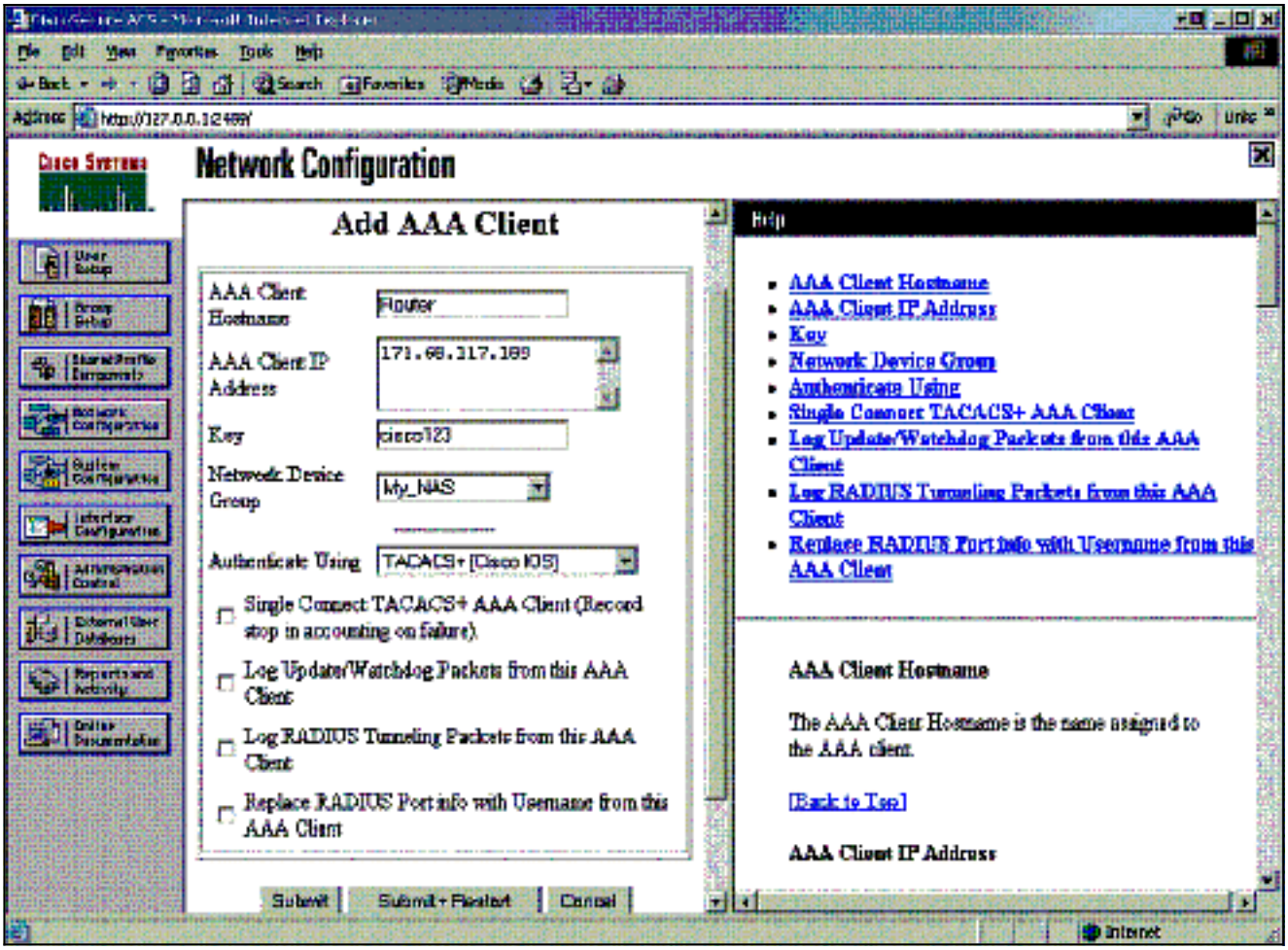
Indienen.



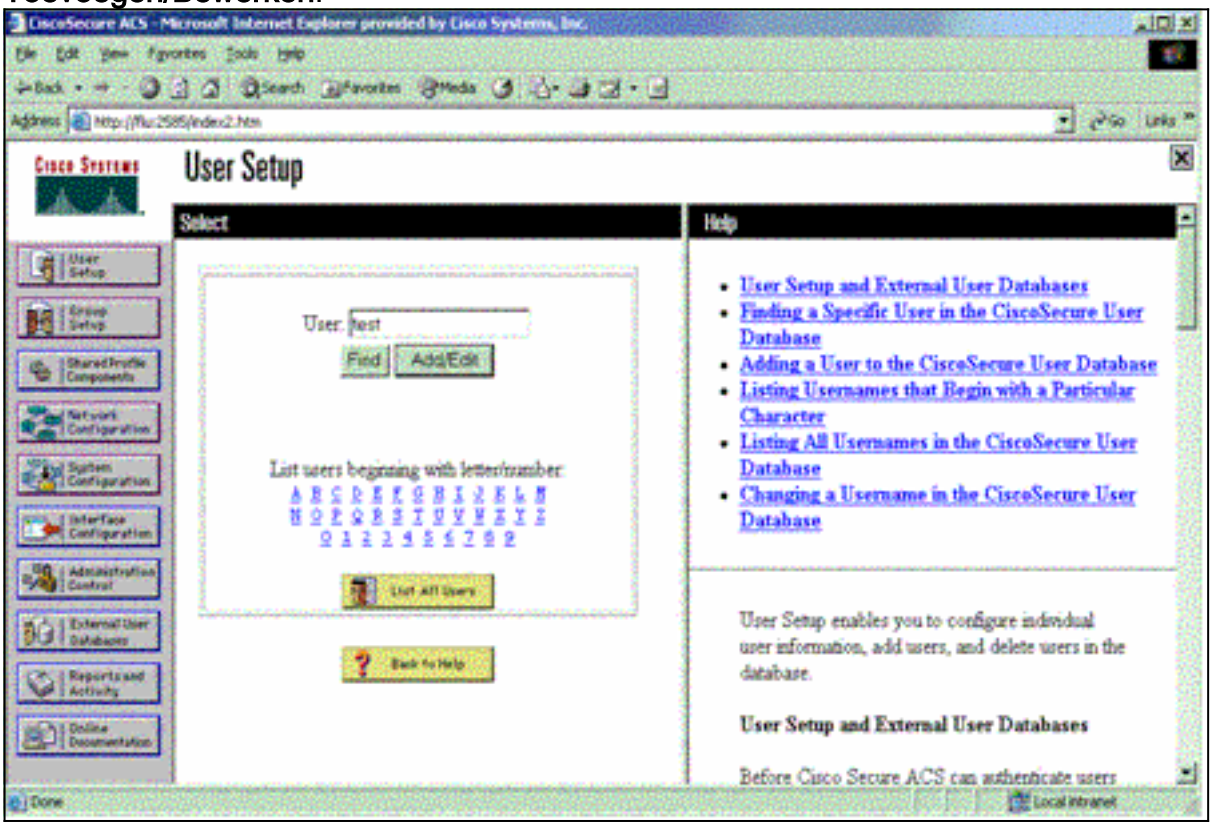
3. Klik op **Add Entry** om een authenticatie, autorisatie en accounting (AAA) client (NAS) toe te voegen.



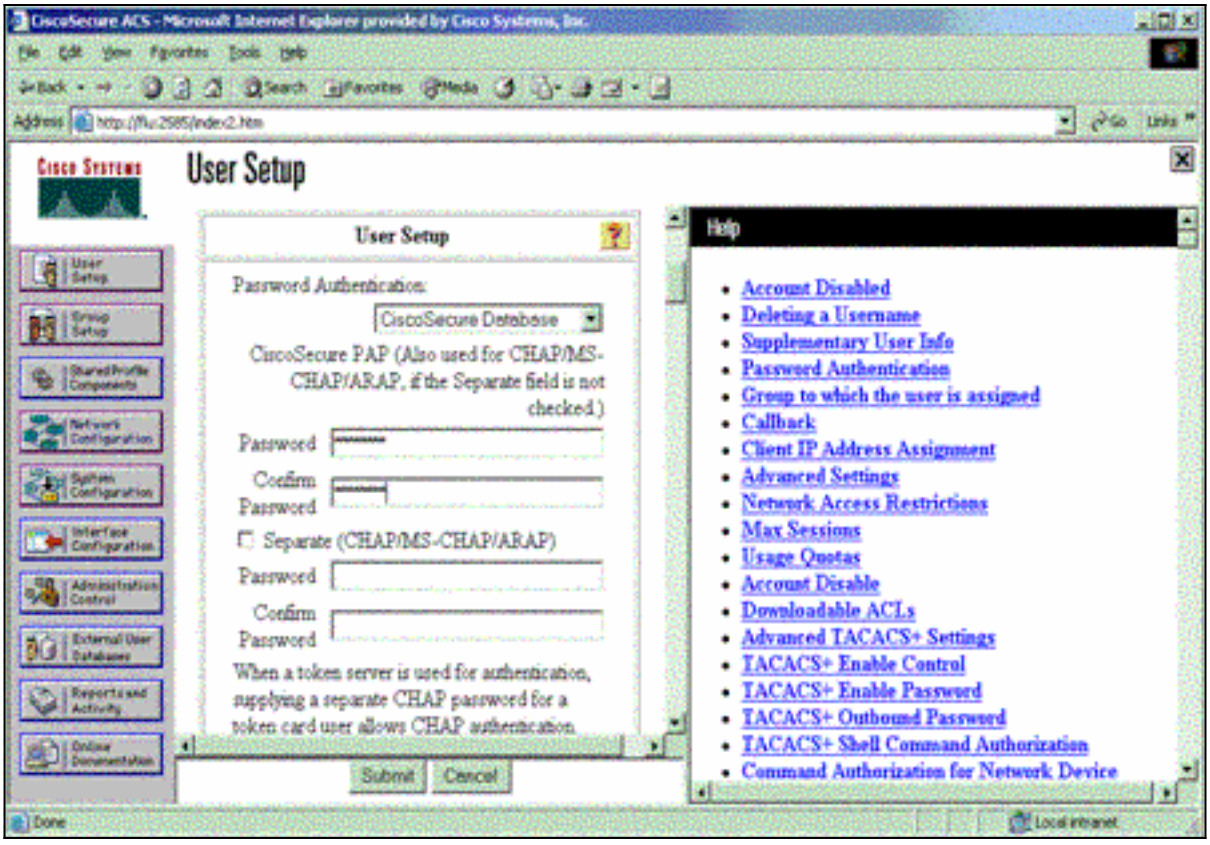
4. Voer de naam van de host in, het IP-adres en de toets die wordt gebruikt om de communicatie tussen de AAA-server en de NAS te versleutelen. Selecteer **TACACS+ (Cisco IOS)** als de verificatiemethode. Wanneer u klaar bent, klikt u op **Inzenden +**Herstart om de wijzigingen toe te
passen.



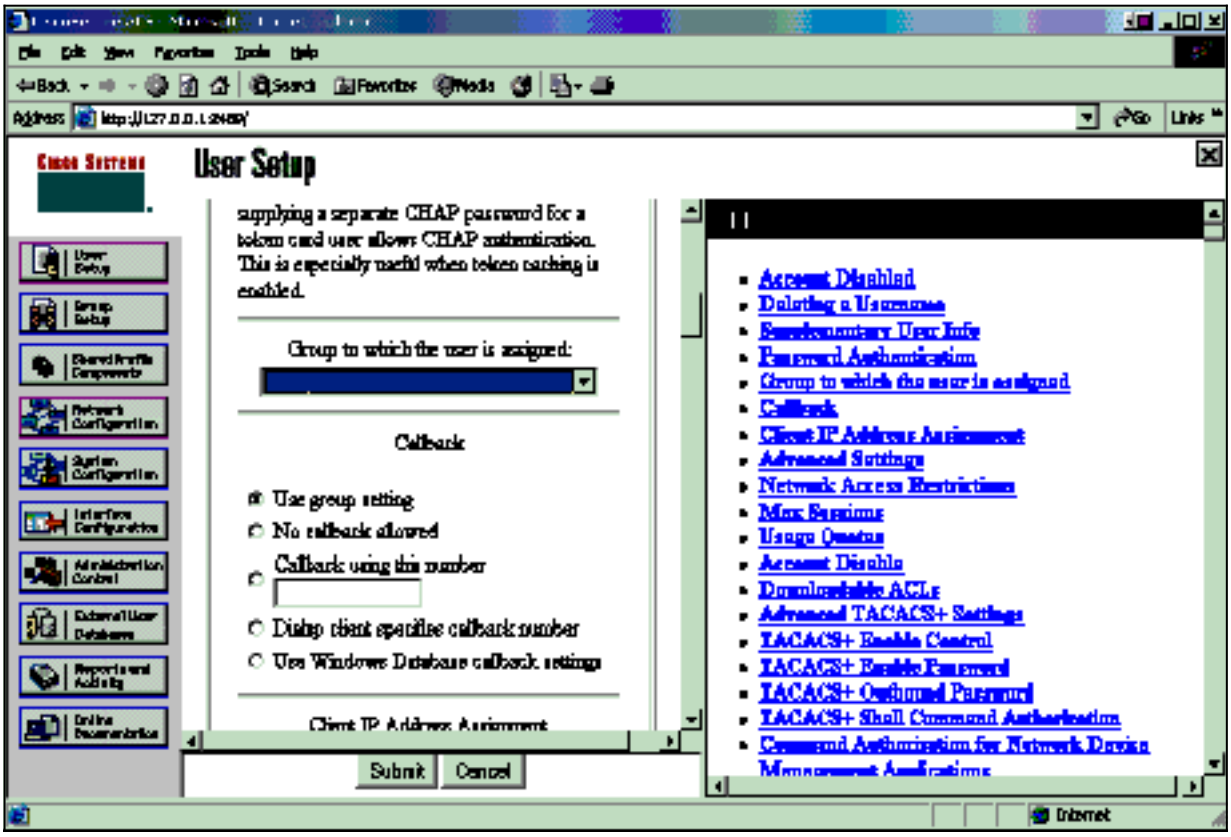
5. Klik op **Gebruikersinstelling**, voer een gebruikersID in en klik op **Toevoegen/Bewerken**.



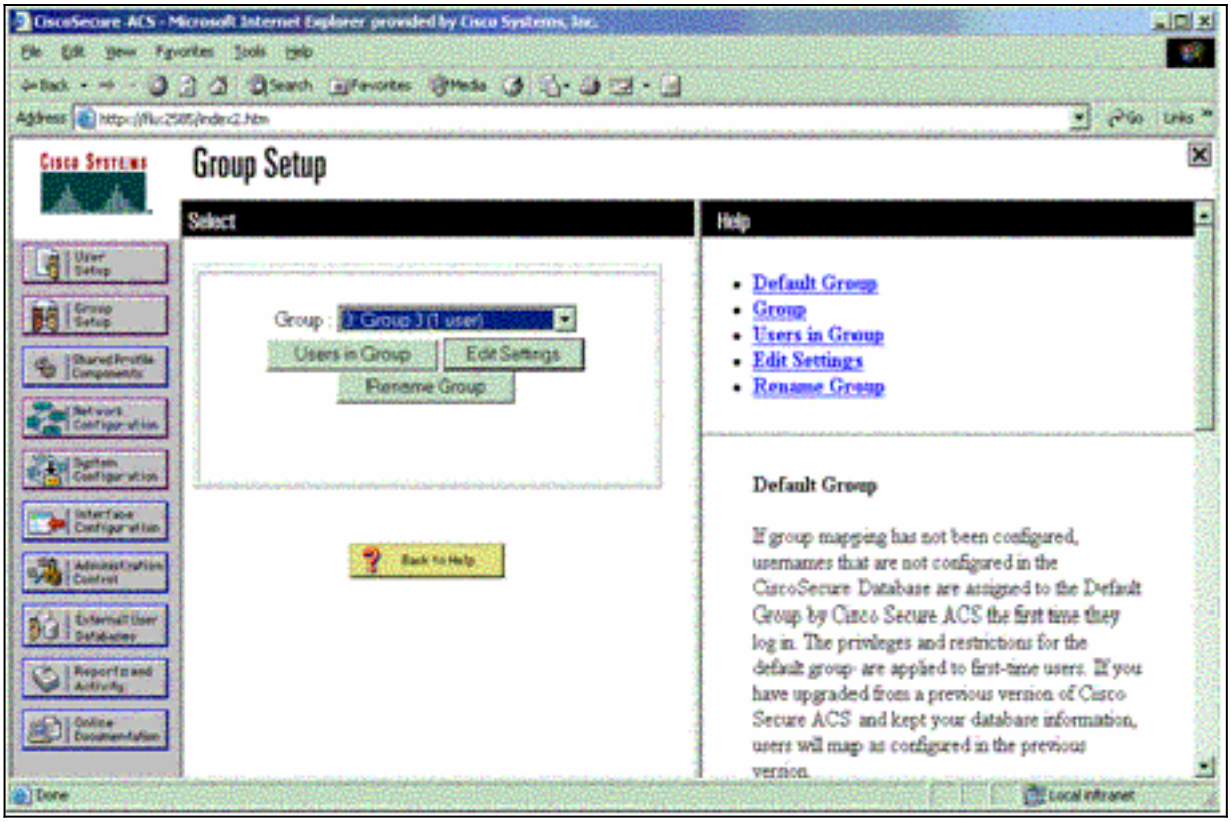
6. Kies een database om de gebruiker te authenticeren. (In dit voorbeeld is de gebruiker "test" en wordt de interne database van het ACS gebruikt voor authenticatie). Voer een wachtwoord in voor een gebruiker en bevestig het wachtwoord.



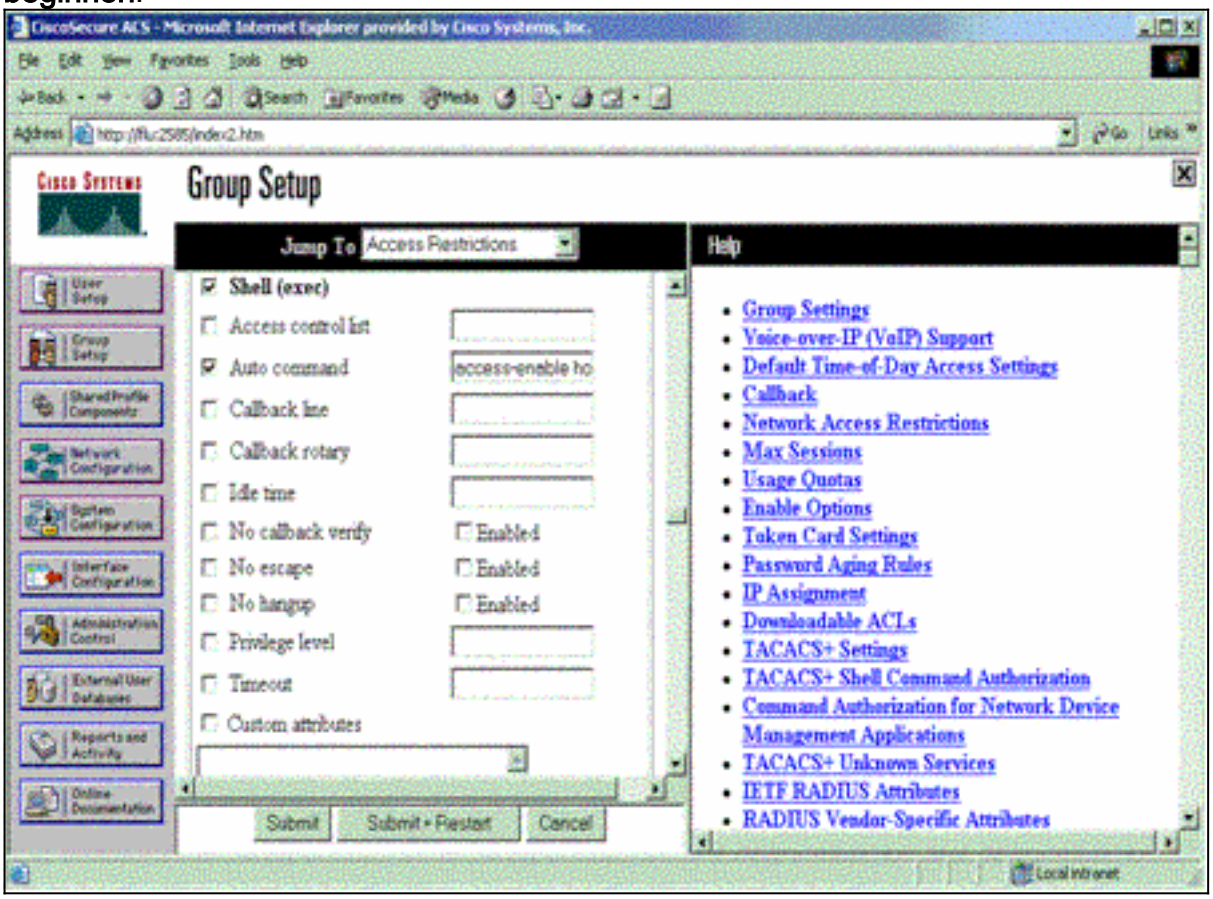
7. Kies de groep waaraan de gebruiker is toegewezen en controleer de **groepsinstelling Gebruik**. Klik op **Inzenden**.



8. Klik op **Groepsinstallatie**. Selecteer het groep waaraan de gebruiker in stap 7 is toegewezen. Klik op **Instellingen bewerken**.



9. Scrolt naar het gedeelte TACACS+ instellingen. Controleer het vakje voor **Shell exec**. Controleer het vakje voor **automatische opdracht**. Typ de auto-opdracht die moet worden uitgevoerd nadat de gebruiker met succes toestemming heeft gegeven. (Dit voorbeeld gebruikt de **access-enabled host timeout 10-**opdracht.) Klik op **Inzenden+Opnieuw beginnen**.



[Probleemoplossing voor TACACS+]

Gebruik deze **debug** opdrachten in de NAS om problemen met TACACS+ op te lossen.

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

- **debug van Tacacs-verificatie**—informatie over het TACACS+-verificatieproces. Alleen beschikbaar in bepaalde versies van de software. Indien niet beschikbaar, **debug tacacs** slechts.
- **debug van Tacacs autorisatie**—informatie over de Tacacs+ autorisatieprocedure. Alleen beschikbaar in bepaalde versies van de software. Indien niet beschikbaar, **debug tacacs** slechts.
- **debug van tacacs gebeurtenissen**—informatie van het TACACS+ hulpproces wordt weergegeven. Alleen beschikbaar in bepaalde versies van de software. Indien niet beschikbaar, **debug tacacs** slechts.

Gebruik deze opdrachten om AAA-problemen op te lossen:

- **debug van verificatie**—informatie over AAA/TACACS+-verificatie wordt weergegeven.
- **debug van autorisatie**—informatie over AAA/TACACS+ autorisatie wordt weergegeven.

De steekproef **debug** uitvoer hier toont een succesvol authenticatie- en vergunningsproces op de ACS TACACS+ server.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
```

```
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

RADIUS gebruiken

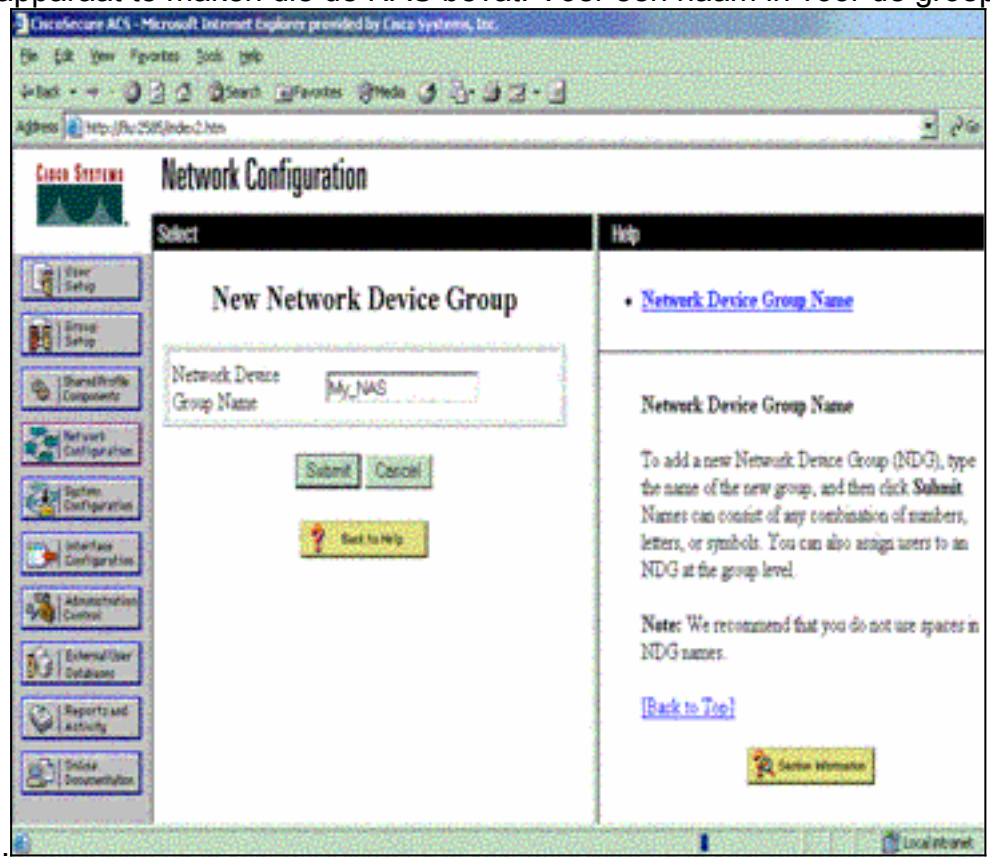
RADIUS configureren

Om RADIUS te gebruiken, moet u een RADIUS-server configureren om verificatie op de RADIUS-server af te dwingen, waarbij de autorisatie (de autoopdracht) moet worden verstuurd in een leverancierspecifieke eigenschap 26, zoals hier wordt getoond:

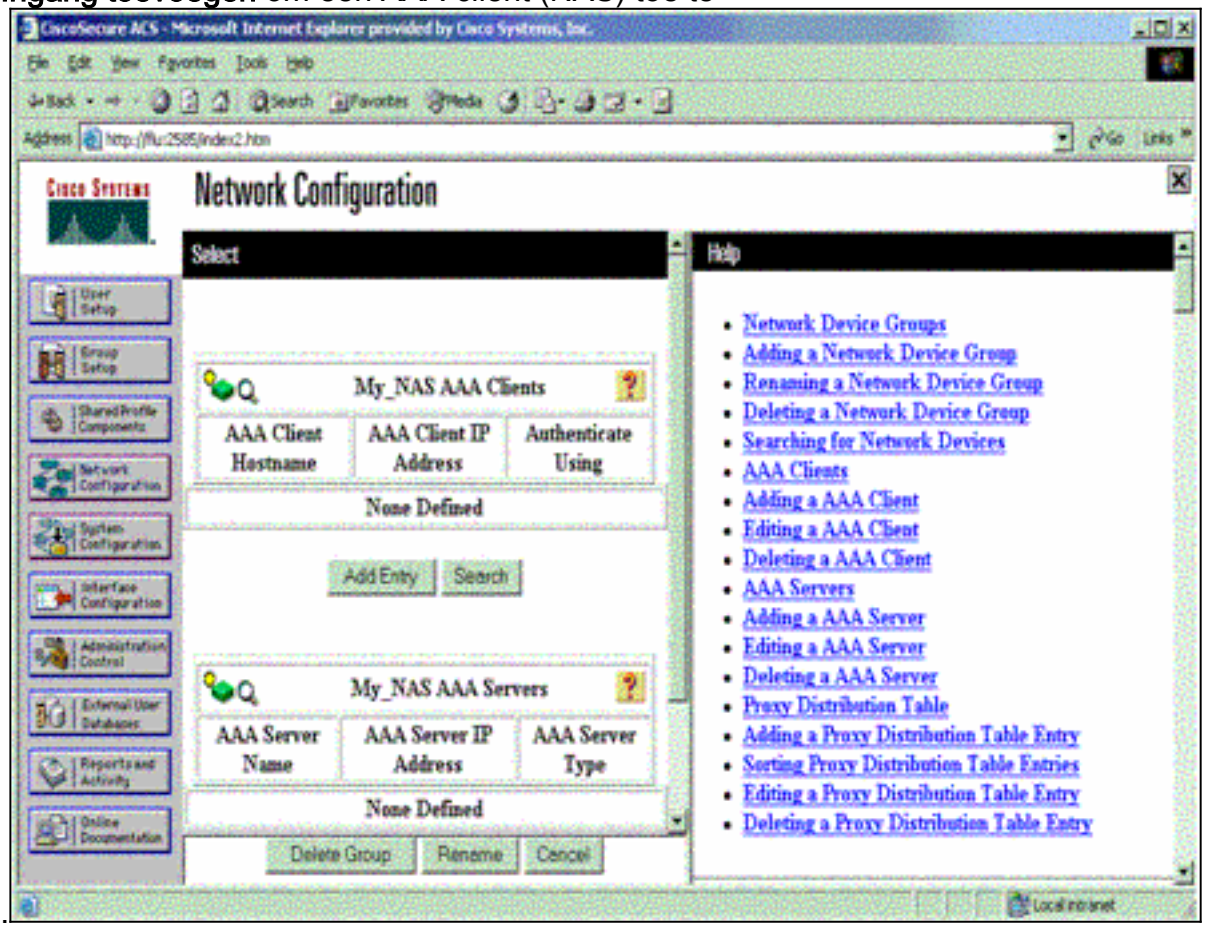
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Voltooi deze stappen om RADIUS op Cisco Secure ACS voor Windows te configureren:

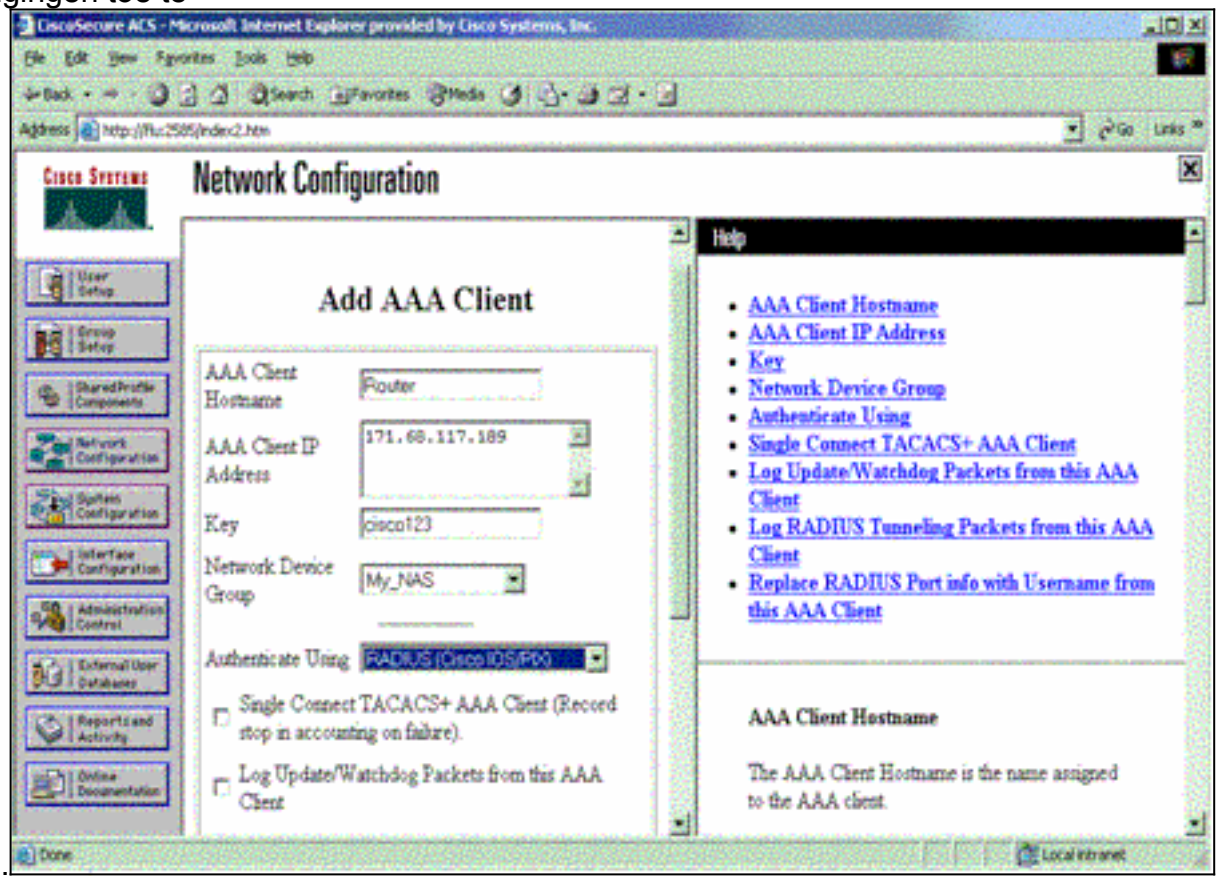
1. Open een webbrowser en voer het adres in van uw ACS-server, die in de vorm is van **http://*<IP_adres of DNS_name>*:2002**. (Dit voorbeeld gebruikt een standaardpoort van 2002.) Inloggen als beheerder.
2. Klik op **Netwerkconfiguratie**. Klik op **Ingang toevoegen** om een groep van het Netwerkapparaat te maken die de NAS bevat. Voer een naam in voor de groep en klik op **Indienen**.



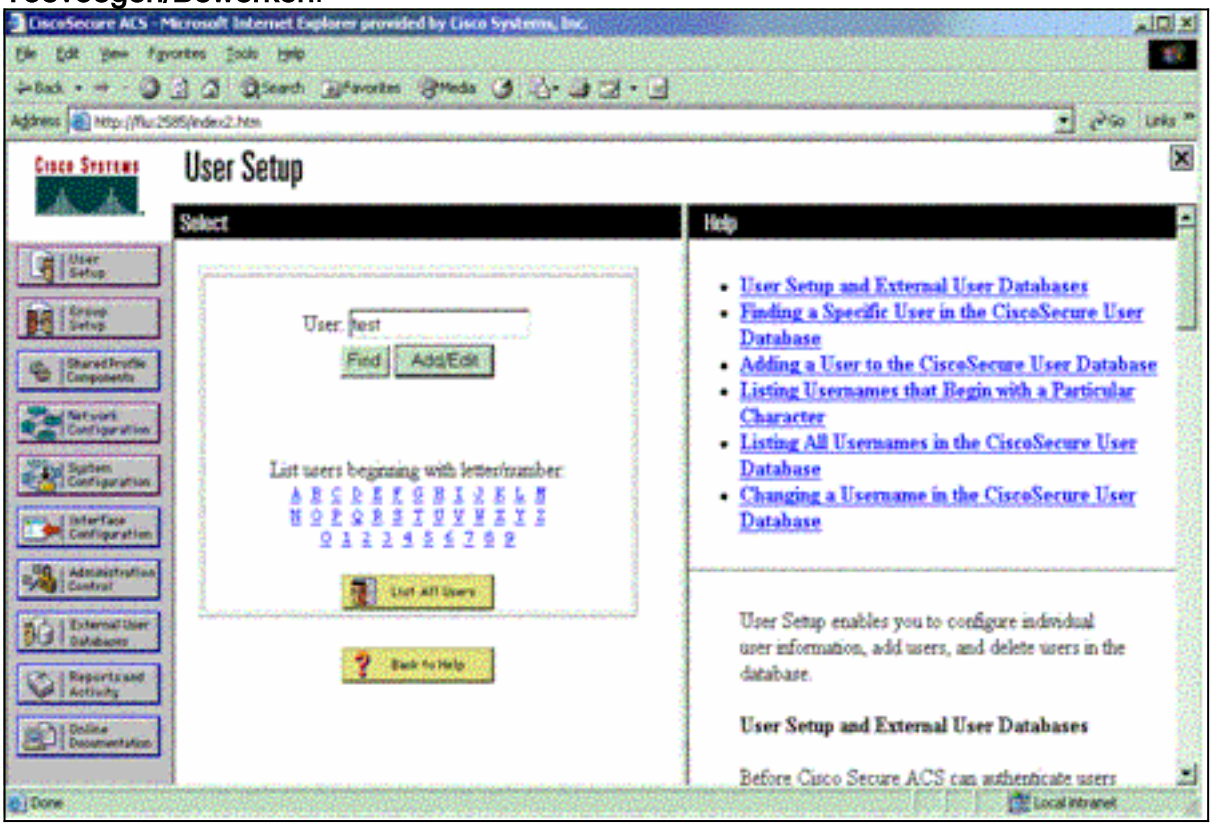
3. Klik op **Ingang toevoegen** om een AAA-client (NAS) toe te voegen.



4. Voer de naam van de host in, het IP-adres en de toets die wordt gebruikt om de communicatie tussen de AAA-server en de NAS te versleutelen. Selecteer **RADIUS (Cisco IOS/PIX)** als de verificatiemethode. Wanneer u klaar bent, klikt u op **Inzenden +**Herstart om de wijzigingen toe te passen.

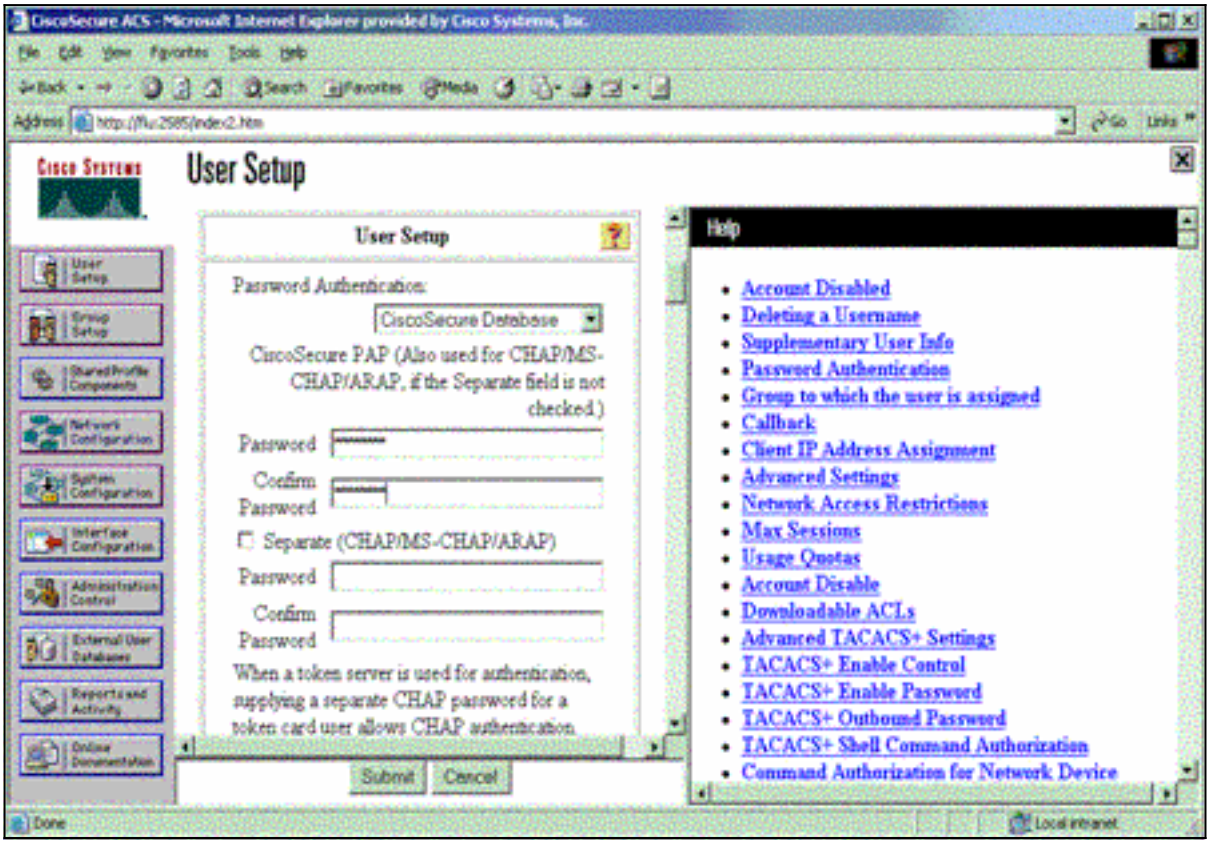


5. Klik op **Gebruikersinstelling**, voer een gebruikersID in en klik op **Toevoegen/Bewerken**.

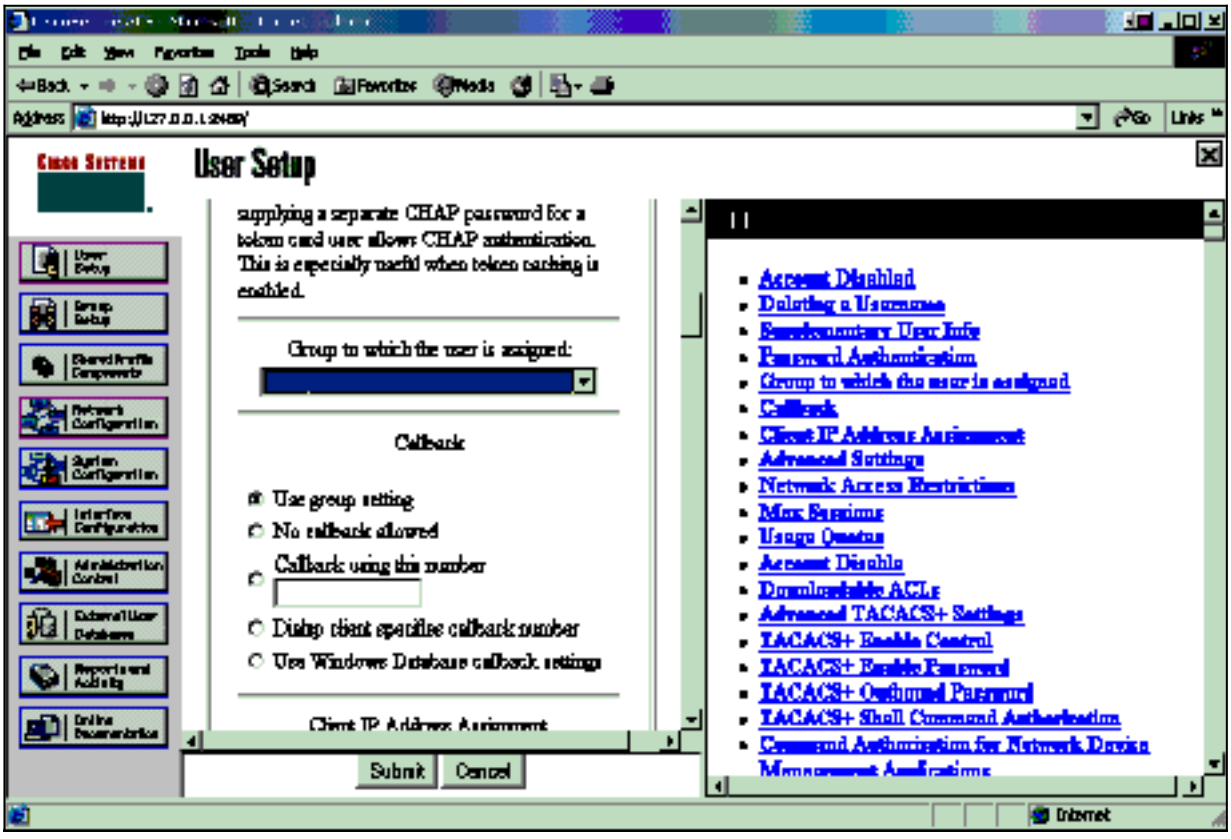


6. Kies een database om de gebruiker te authenticeren. (In dit voorbeeld is de gebruiker "test" en wordt de interne database van het ACS gebruikt voor authenticatie). Voer een

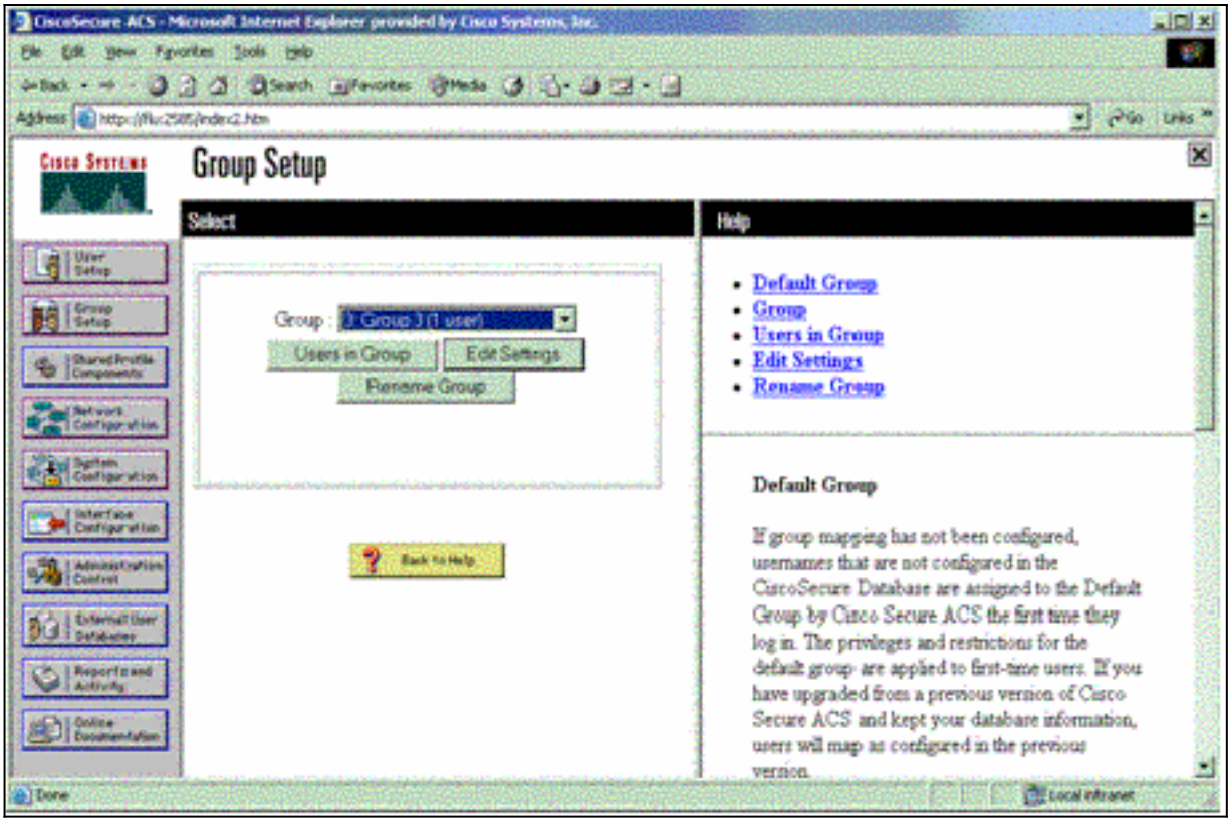
wachtwoord in voor een gebruiker en bevestig het wachtwoord.



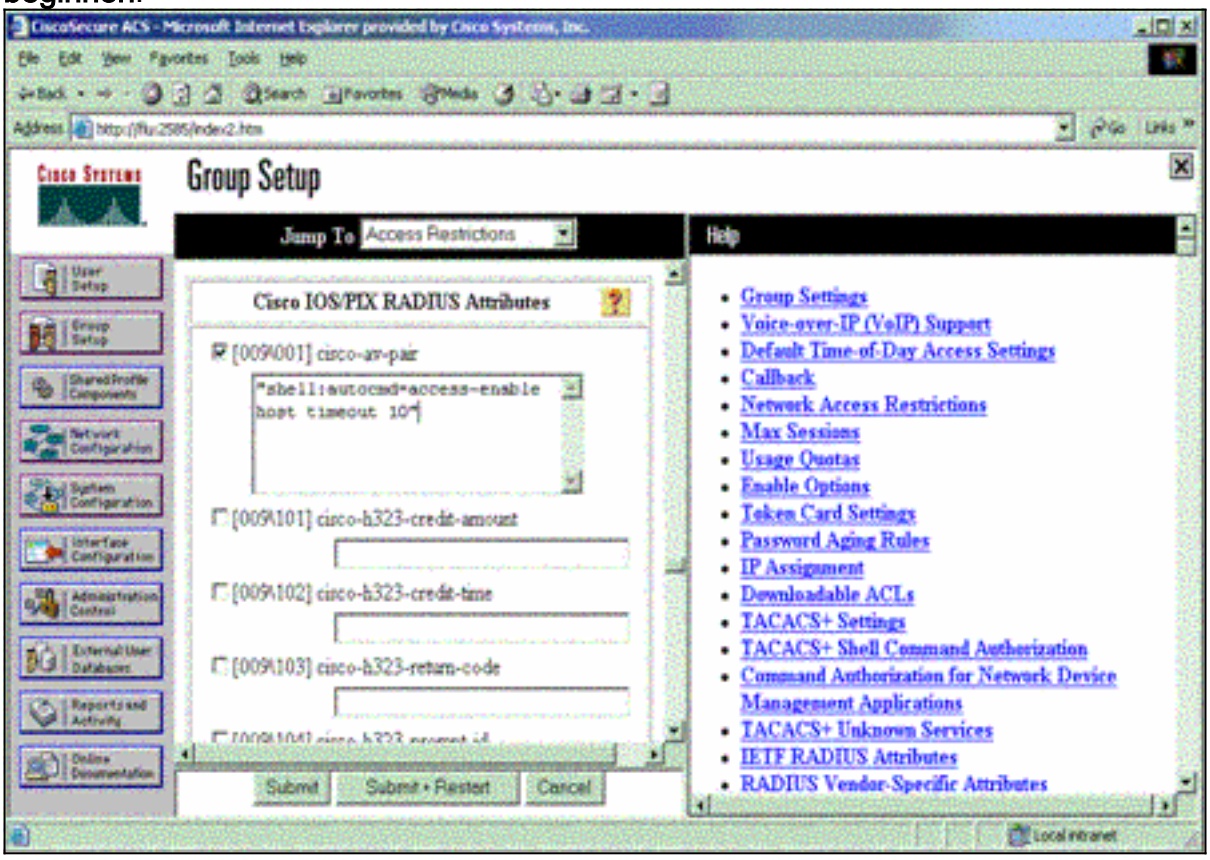
7. Kies de groep waaraan de gebruiker is toegewezen en controleer de **groepsinstelling Gebruik**. Klik op **Inzenden**.



8. Klik op **Groepsinstallatie** en selecteer de groep waaraan de gebruiker in de vorige stap is toegewezen. Klik op **Instellingen bewerken**.



9. Scrolt naar het gedeelte Cisco IOS/PIX RADIUS-kenmerken. Controleer het vakje voor **cisco-av-paar**. Typ de opdracht **shell** die moet worden uitgevoerd na succesvolle toestemming van de gebruiker. (Dit voorbeeld gebruikt **shell:autocmd=access-enabled host timeout 10**.) Klik op **Inzenden+Opnieuw beginnen**.



Probleemoplossing met RADIUS

Gebruik deze **debug** opdrachten in de NAS om RADIUS-problemen op te lossen.

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

- **debug straal**—informatie die bij RADIUS is gekoppeld.

Gebruik deze opdrachten om AAA-problemen op te lossen:

- **debug van verificatie**—informatie over AAA/TACACS+-verificatie wordt weergegeven.
- **debug van autorisatie**—informatie over AAA/TACACS+ autorisatie wordt weergegeven.

De voorbeelduitvoer **debug-**uitvoer hier laat een succesvol authenticatie- en autorisatieproces zien bij de ACS die voor RADIUS zijn ingesteld.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=======================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                        [tty]
 RADIUS(00000003): Storing nasport 66 in rad_db
 RADIUS/ENCODE(00000003): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
 RADIUS(00000003): Config NAS IP: 0.0.0.0
 RADIUS/ENCODE(00000003): acct_session_id: 1
 RADIUS(00000003): sending
 RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
   for Radius-Server 10.48.66.53
 RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
   id 21645/1, len 77
 RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
   BE B5 07 BD E9 05 5B 5D
 RADIUS:  User-Name           [1]   7   "test"
 RADIUS:  User-Password       [2]   18  *
 RADIUS:  NAS-Port            [5]   6   66
 RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
 RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
 RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
 RADIUS: Received from id 21645/1 10.48.66.53:1645,
   Access-Accept, len 93
 RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
   68 4B C3 FC 25 21 47 CD
 RADIUS:  Vendor, Cisco       [26]  51
 RADIUS:   Cisco AVpair       [1]   45
   "shell:autocmd=access-enable host timeout 10"
 RADIUS:  Class               [25]  22
 RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
   [CISCOACS:ac127c0]
 RADIUS:   31 2F 36 36                [1/66]
 RADIUS(00000003): Received from id 21645/1
 AAA/AUTHOR/EXEC(00000003): processing AV
```

```
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Gerelateerde informatie

- Cisco IOS-beveiliging op slot en sleutel
- Ondersteuningspagina voor TACACS/TACACS+
- TACACS+ in IOS-documentatie
- RADIUS-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems