Configuratievoorbeeld van ACS Shell-opdrachtautorisatie voor IOS en ASA/PIX/FWSM

Inhoud

Inleiding

Dit document beschrijft hoe u de shell-autorisatiesets in Cisco Secure Access Control Server (ACS) voor AAA-clients kunt configureren, zoals Cisco IOS®-routers of -switches en Cisco security applicaties (ASA/PIX/FWSM) met TACACS+ als autorisatieprotocol.

Opmerking: ACS Express ondersteunt opdrachtautorisatie niet.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat de basisconfiguraties zijn ingesteld in zowel AAA-clients als ACS.

In ACS, kies **Interfaceconfiguratie > Geavanceerde Opties**, en zorg ervoor dat het controlevakje **Per-gebruiker van TACACS+/RADIUS-kenmerken** is ingeschakeld.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Secure Access Control Server (ACS) waarop de softwareversie 3.3 en hoger wordt uitgevoerd.

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.

Conventies

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

Opdrachtautorisatiesets

Opdrachtautorisatiesets bieden een centraal mechanisme om de autorisatie te controleren van elk commando dat op een netwerkapparaat wordt afgegeven. Deze eigenschap verbetert zeer de schaalbaarheid en beheersbaarheid die worden vereist om vergunningsbeperkingen te plaatsen.

In ACS omvatten de standaard opdrachtautorisatiesets Shell Command Autorisatiesets en PIX Command Autorisatiesets. Cisco-toepassingen voor apparaatbeheer, zoals CiscoWorks Management Center voor firewalls, kunnen ACS instrueren om extra types opdrachtautorisatiesets te ondersteunen.

Opmerking: voor de autorisatiesets voor PIX-commando is het nodig dat het verzoek voor TACACS+ opdrachtautorisatie de service als *pixshell* identificeert. Controleer dat deze service is geïmplementeerd in de versie van PIX OS die uw firewalls gebruiken. als dit niet het geval is, gebruikt u Shell Command Authorisation Sets om de opdrachtautorisatie voor PIX-apparaten uit te voeren. Zie Een Shell Command Authorisation Set configureren voor een gebruikersgroep voor meer informatie.

Opmerking: vanaf PIX OS versie 6.3 is de pixshell-service niet geïmplementeerd.

Opmerking: met de Cisco security applicaties (ASA/PIX) kan de gebruiker tijdens de aanmelding niet rechtstreeks in de activeringsmodus worden geplaatst. De gebruiker moet handmatig de inschakelmodus invoeren.

Om meer controle van apparaat-ontvangen administratieve Telnet-sessies aan te bieden, kan een netwerkapparaat dat TACACS+ gebruikt toestemming voor elke opdrachtregel aanvragen voordat deze wordt uitgevoerd. U kunt een verzameling opdrachten definiëren die voor uitvoering door een bepaalde gebruiker op een bepaald apparaat zijn toegestaan of geweigerd. ACS heeft deze mogelijkheid verder verbeterd met deze functies:

- **Herbruikbare Named Command Autorisatiesets**—Zonder direct een gebruiker of gebruikersgroep aan te halen, kunt u een benoemde set commando-autorisaties maken. U kunt meerdere opdrachtautorisatiesets definiëren om verschillende toegangsprofielen af te

bakenen. Voorbeeld:Een *Help desk* commando autorisatieset kan toegang toestaan tot high-level browsing commando's, zoals **show run**, en ontkennen elke configuratie commando's.Een autorisatieset voor *alle netwerkengineers* kan een beperkte lijst van toegestane opdrachten bevatten voor elke netwerkengineer in de onderneming.Een autorisatieset voor *lokale netwerkengineers* kan alle opdrachten toestaan (en kan ook IP-adresconfiguratieopdrachten bevatten).

- **Gedetailleerdheid van FineConfiguration**: u kunt associaties maken tussen benoemde opdrachtautorisatiesets en netwerkapparaatgroepen (NDG's). U kunt dus verschillende toegangsprofielen definiëren voor gebruikers, afhankelijk van de netwerkapparaten waartoe ze toegang hebben. U kunt dezelfde opdrachtautorisatieset koppelen aan meerdere NDG's en deze voor meerdere gebruikersgroepen gebruiken. ACS dwingt gegevensintegriteit af. Benoemde opdrachtautorisatiesets worden bewaard in de interne ACS-database. U kunt de ACS-back-up- en terugzetfuncties gebruiken om er back-ups van te maken en ze te herstellen. U kunt opdrachtautorisatiesets ook repliceren naar secundaire ACS'en, samen met andere configuratiegegevens.

Voor opdrachtautorisatietypen die Cisco-apparaatbeheertoepassingen ondersteunen, zijn de voordelen vergelijkbaar wanneer u opdrachtautorisatiesets gebruikt. U kunt opdrachtautorisatiesets toepassen op ACS-groepen die gebruikers van de apparaatbeheertoepassing bevatten om autorisatie van verschillende rechten in een apparaatbeheertoepassing af te dwingen. De ACS-groepen kunnen corresponderen met verschillende rollen binnen de apparaatbeheertoepassing en u kunt verschillende opdrachtautorisatiesets toepassen op elke groep, zoals van toepassing.

ACS heeft drie opeenvolgende stadia van bevelvergunning het filtreren. Elk verzoek van de bevelvergunning wordt beoordeeld in de vermelde orde:

1. **Command Match**-ACS bepaalt of de opdracht die wordt verwerkt overeenkomt met een opdracht die in de opdrachtautorisatieset wordt vermeld. Als de opdracht niet is gekoppeld, wordt de opdrachtautorisatie bepaald door de instelling Onovereenkomende opdrachten: *toestaan* of *weigeren*. Anders, als het bevel wordt aangepast, blijft de evaluatie verdergaan.
2. **Argument Match**-ACS bepaalt of de gepresenteerde opdrachtargumenten overeenkomen met de opdrachtargumenten die in de opdrachtautorisatieset worden vermeld.Als er geen argument is gevonden, wordt de opdrachtautorisatie bepaald door of de optie Onovereenkomende args toestaan is ingeschakeld. Indien onovertroffen argumenten zijn toegestaan, is de opdracht geautoriseerd en eindigt de evaluatie; anders is de opdracht niet geautoriseerd en eindigt de evaluatie.Als alle argumenten worden aangepast, gaat de evaluatie verder.
3. **Argument Beleid**—Zodra ACS bepaalt dat de argumenten in de commando match argumenten in de commando autorisatie set, ACS bepaalt of elk commando argument expliciet is toegestaan. Als alle argumenten expliciet zijn toegestaan, verleent ACS opdrachtautorisatie. Als er geen argumenten zijn toegestaan, ontkent ACS de opdrachtautorisatie.

Een Shell Command Authorisation Set toevoegen

Deze sectie omvat deze scenario's die beschrijven hoe een reeks van de bevelvergunning toe te voegen:

- Scenario 1: Voorrecht voor lees-schrijftoegang of volledige toegang
- Scenario 2: Voorrecht voor alleen-lezen toegang
- Scenario 3: Bevoegdheid voor beperkte toegang

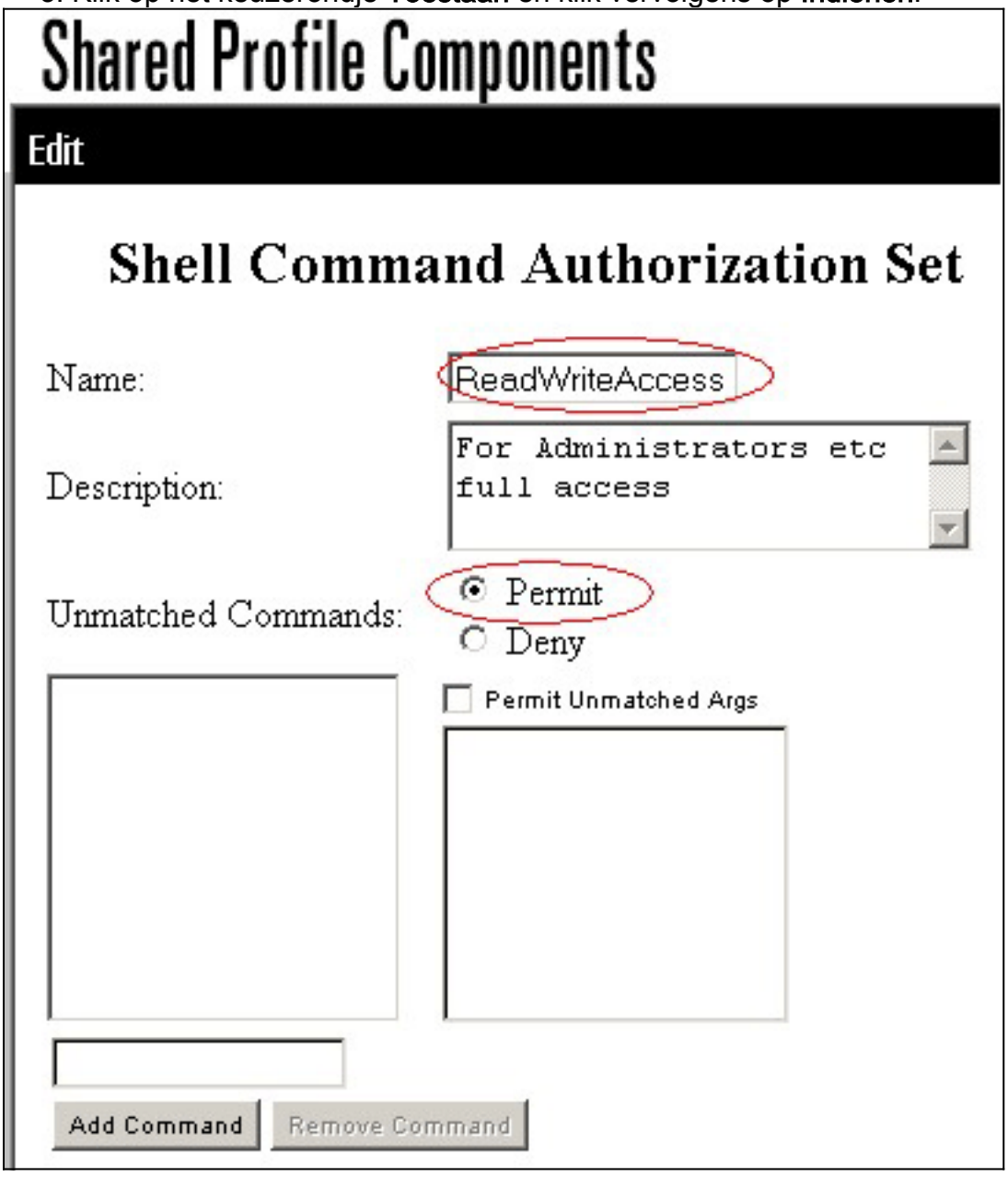
Opmerking: Raadpleeg het gedeelte Een opdrachtautorisatie toevoegen in de Gebruikershandleiding voor Cisco Secure Access Control Server 4.1 voor meer informatie over het maken van opdrachtautorisatiesets. Zie Een opdrachtautorisatieset bewerken en een opdrachtautorisatieset verwijderen voor meer informatie over het bewerken en verwijderen van opdrachtautorisatiesets.

Scenario 1: Voorrecht voor lees-schrijftoegang of volledige toegang

In deze scenario's krijgen gebruikers lees-schrijftoegang (of volledige toegang).

Configureer in het gedeelte Shell Command Authorisation Set van het venster Shared Profile Components deze instellingen:

1. Voer in het veld Naam **ReadWriteAccess** in als de naam van de opdrachtautorisatieset.
2. Typ in het veld Description een beschrijving voor de opdrachtautorisatieset.
3. Klik op het keuzerondje **Toestaan** en klik vervolgens op **Indienen**.

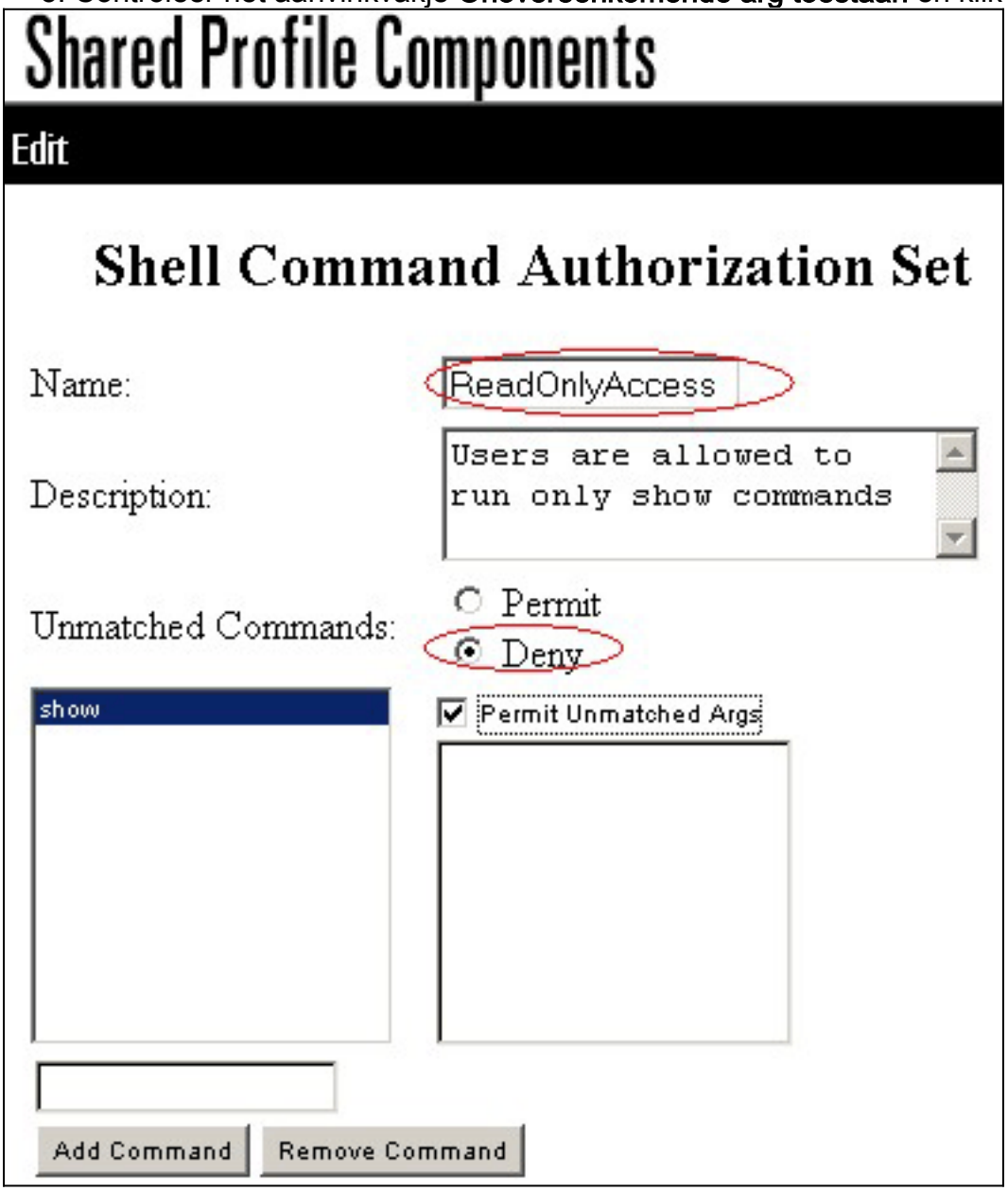


Scenario 2: Voorrecht voor alleen-lezen toegang

In deze scenario's, kunnen de gebruikers slechts gebruiken **tonen** bevelen.

Configureer in het gedeelte Shell Command Authorisation Set van het venster Shared Profile Components deze instellingen:

1. Voer in het veld Naam **ReadOnlyAccess** in als de naam van de opdrachtautorisatieset.
2. Typ in het veld Description een beschrijving voor de opdrachtautorisatieset.
3. Klik op het keuzerondje **Deny**.
4. Voer de **opdracht show** in in het veld boven de knop Opdracht toevoegen en klik vervolgens op **Opdracht toevoegen**.
5. Controleer het aanvinkvakje **Onovereenkomende arg toestaan** en klik op **Indienen**



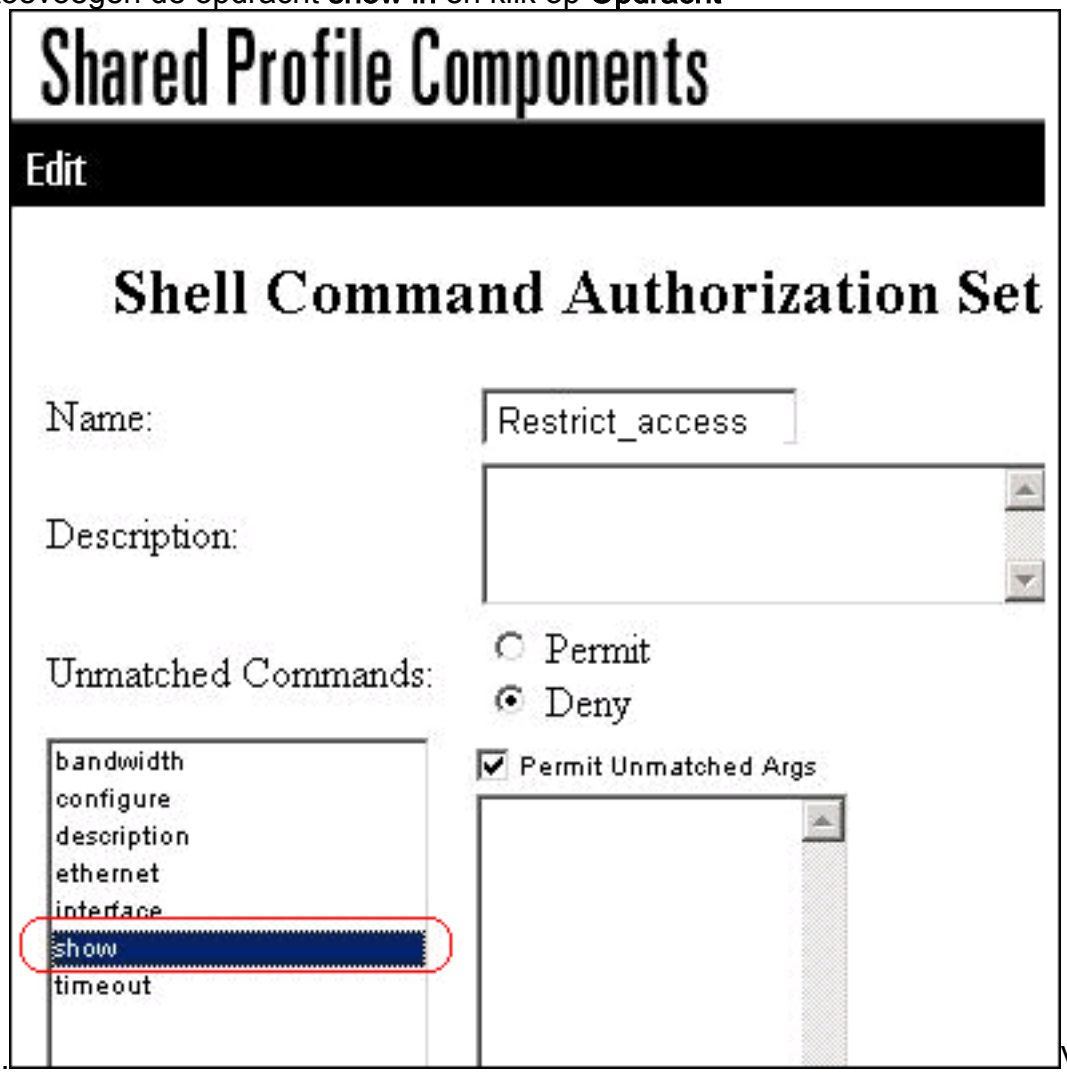
Scenario 3: Bevoegdheid voor beperkte toegang

In dit scenario kunnen gebruikers selectieve opdrachten gebruiken.

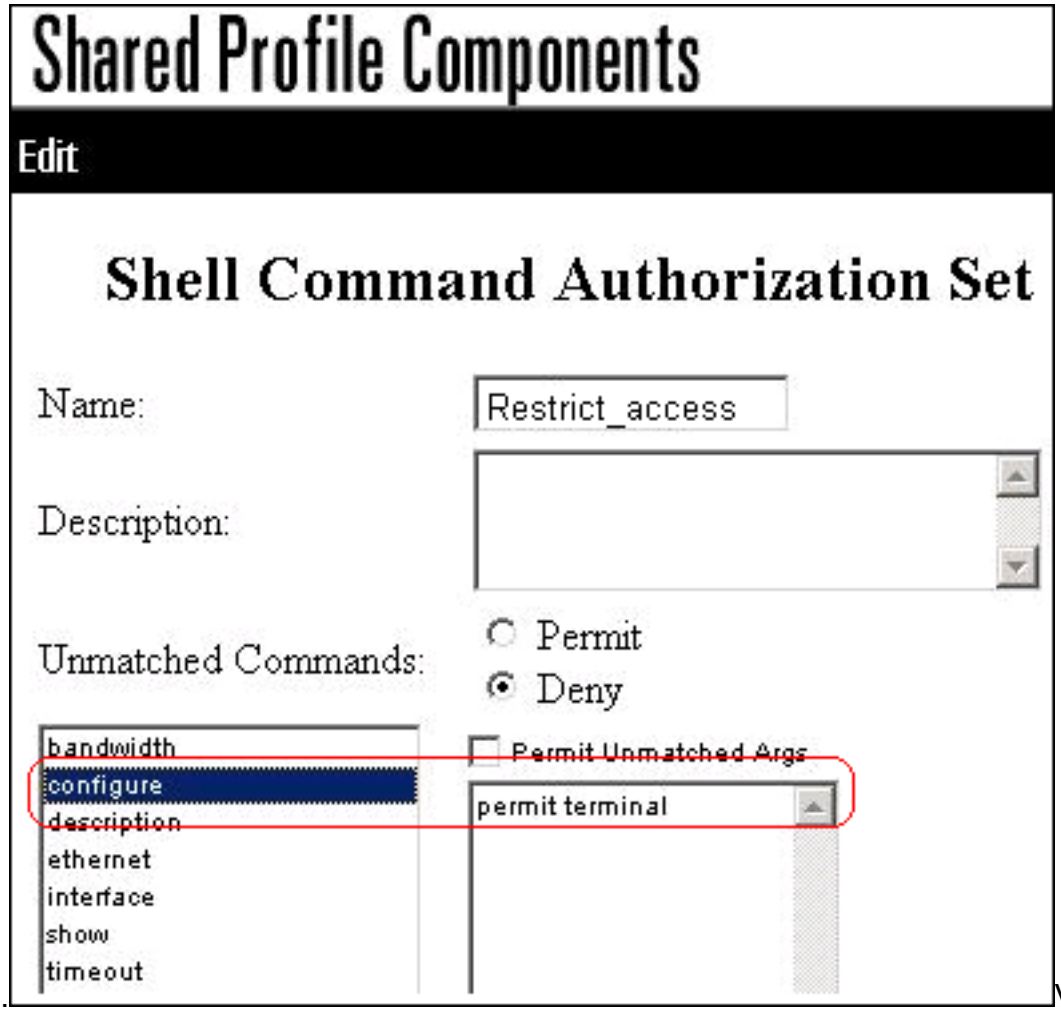
Configureer in het gedeelte Shell Command Authorisation Set van het venster Shared Profile

Components deze instellingen:

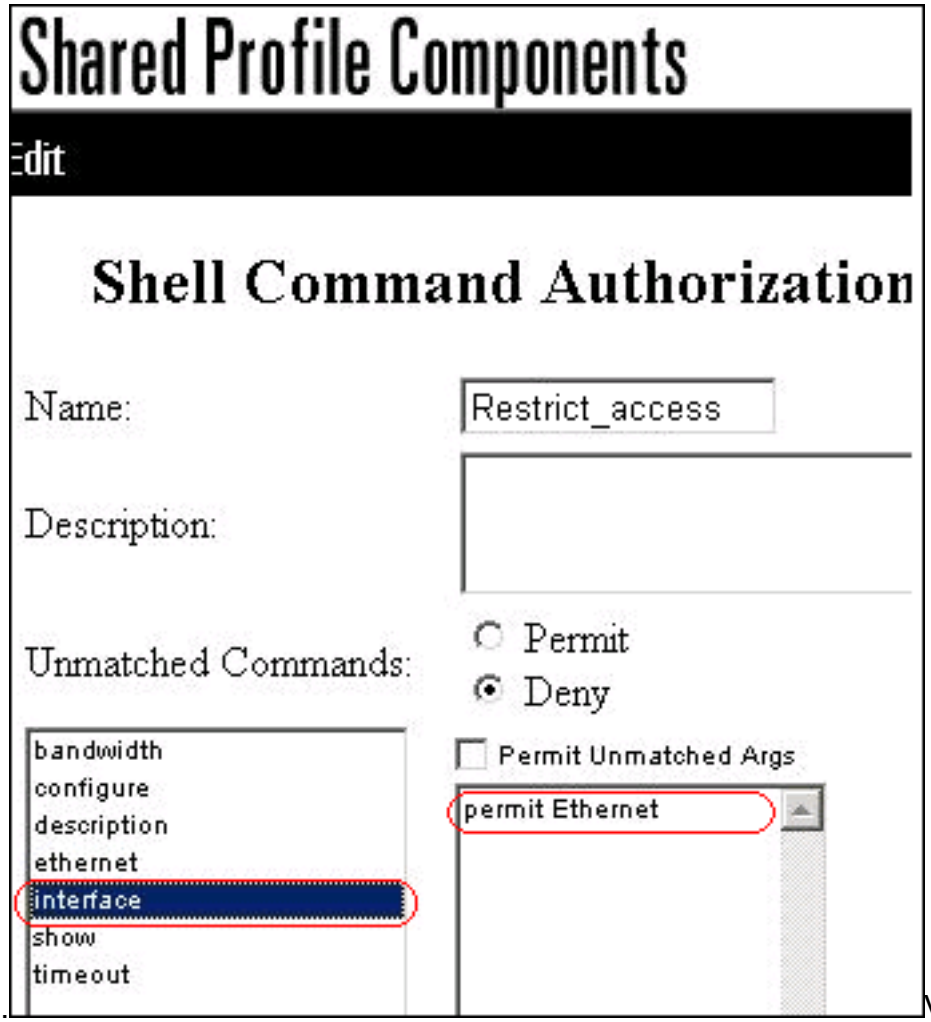
1. Voer in het veld Naam **Restrictie_access in** als de naam van de opdrachtautorisatieset.
2. Klik op het keuzerondje **Deny**.
3. Voer de opdrachten in die u op de AAA-clients wilt toestaan.Voer in het veld boven de knop Opdracht toevoegen de opdracht **show in** en klik op **Opdracht**



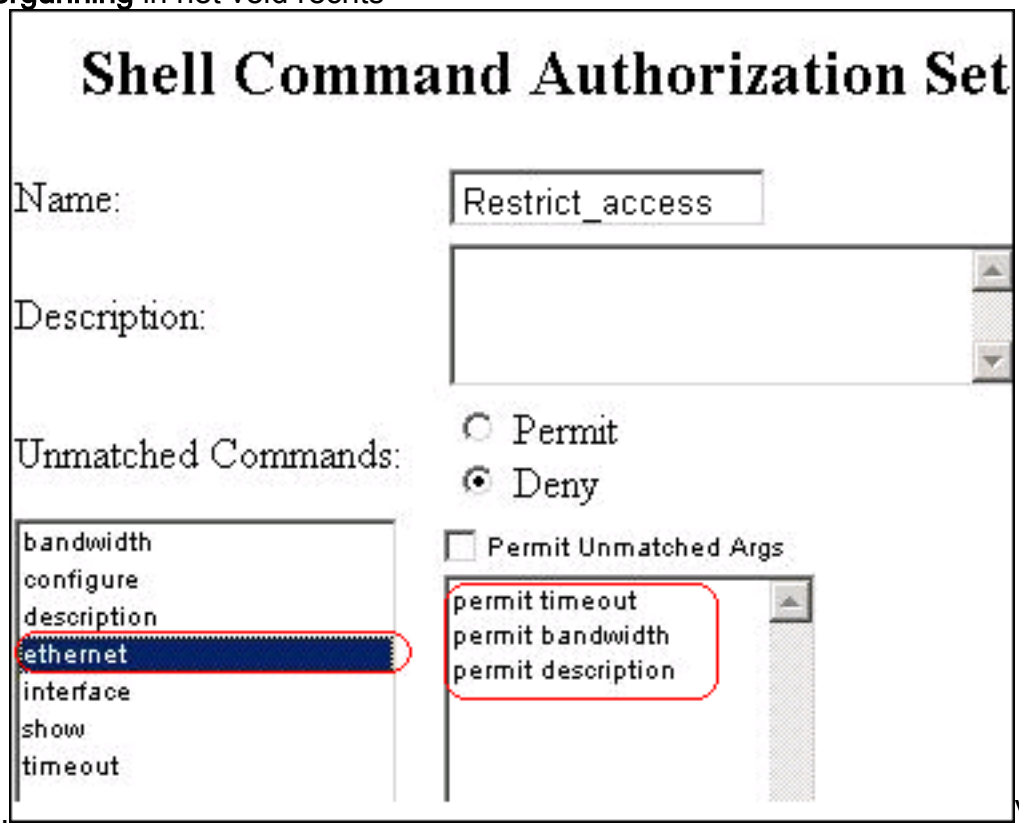
toevoegen.Voer de **configuratie-**opdracht in en klik op **Opdracht toevoegen**.Selecteer de opdracht **Configure** en voer de **vergunningsterminal** rechts in het veld



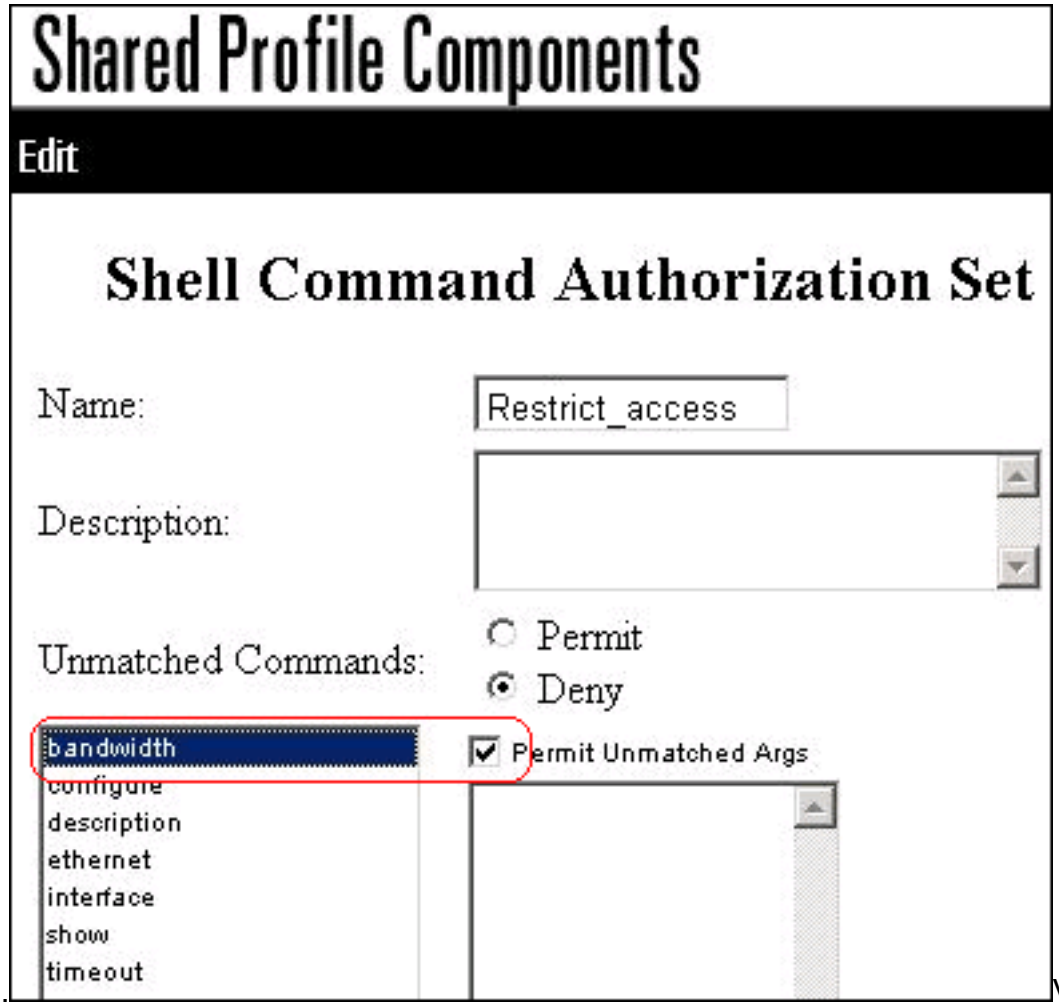
in.Voer de **interfaceopdracht in** en klik op **Opdracht toevoegen**.Selecteer de **interfaceopdracht** en voer **vergunning Ethernet** in het veld rechts



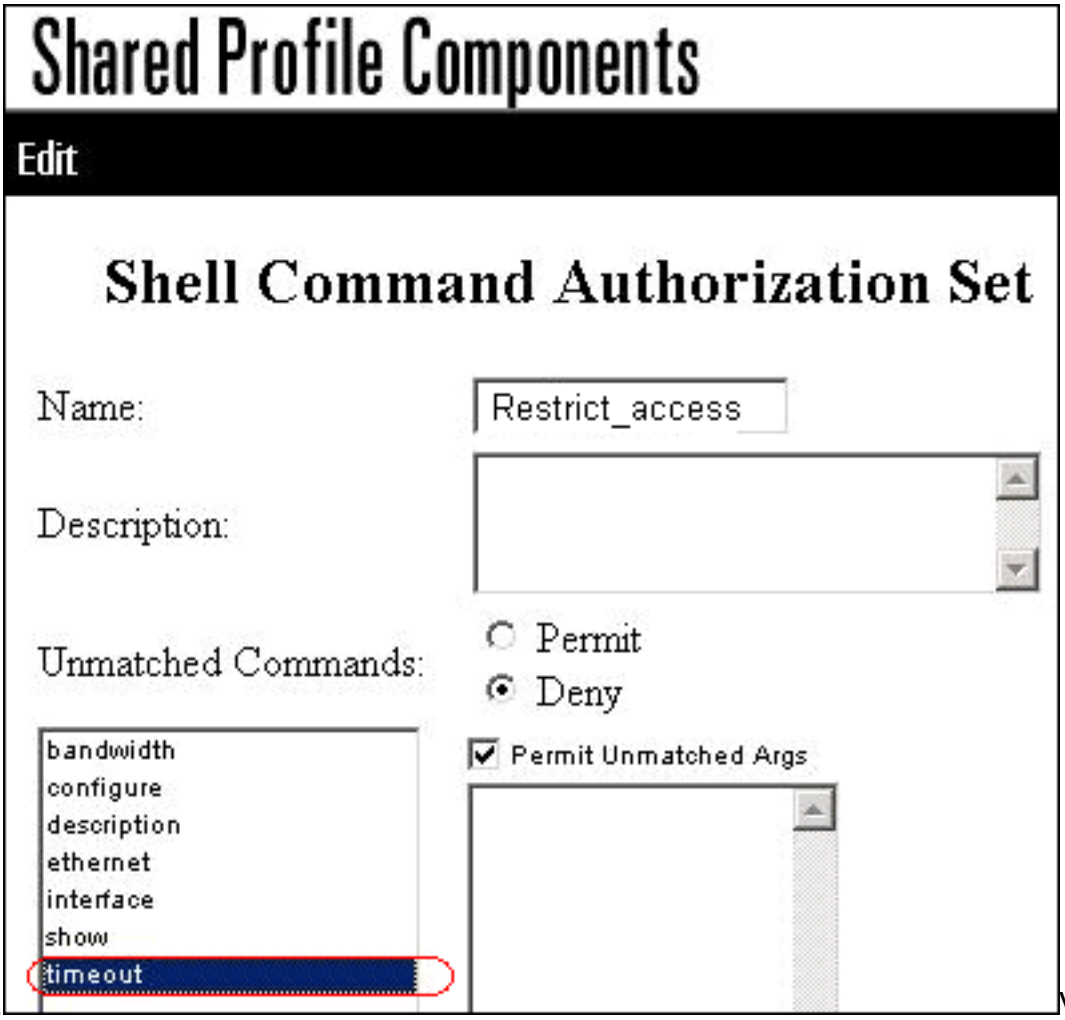
in. Voer de **Ethernet-**opdracht in en klik op **Opdracht toevoegen**.Selecteer de **interfaceopdracht** en voer de **time-out van de vergunning**, de **bandbreedte van de vergunning** en de **beschrijving van de vergunning** in het veld rechts



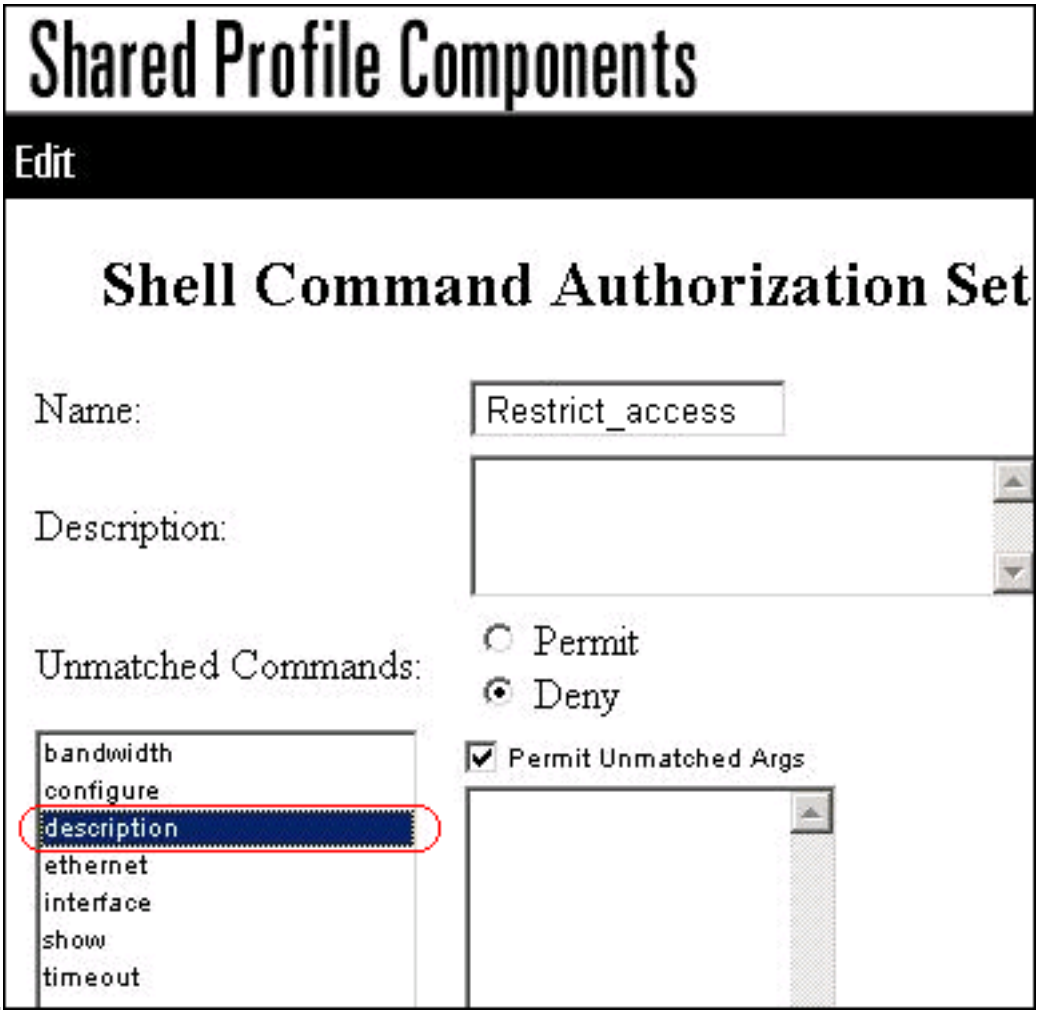
in. Voer de opdracht **bandbreedte in** en klik op **Opdracht**



toevoegen.Voer de opdracht **timeout in** en klik op **Add**



Command. Voer de opdracht **Description in** en klik op **Add**



Command.

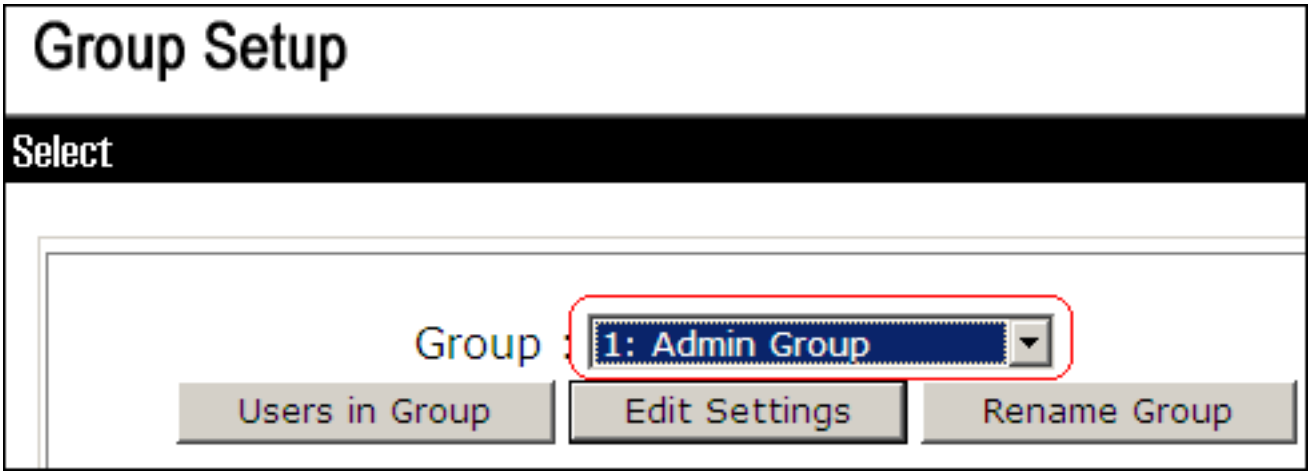
4. Klik op **Verzenden**.

Associeer de Shell Command Authorisation Set naar Gebruikersgroep

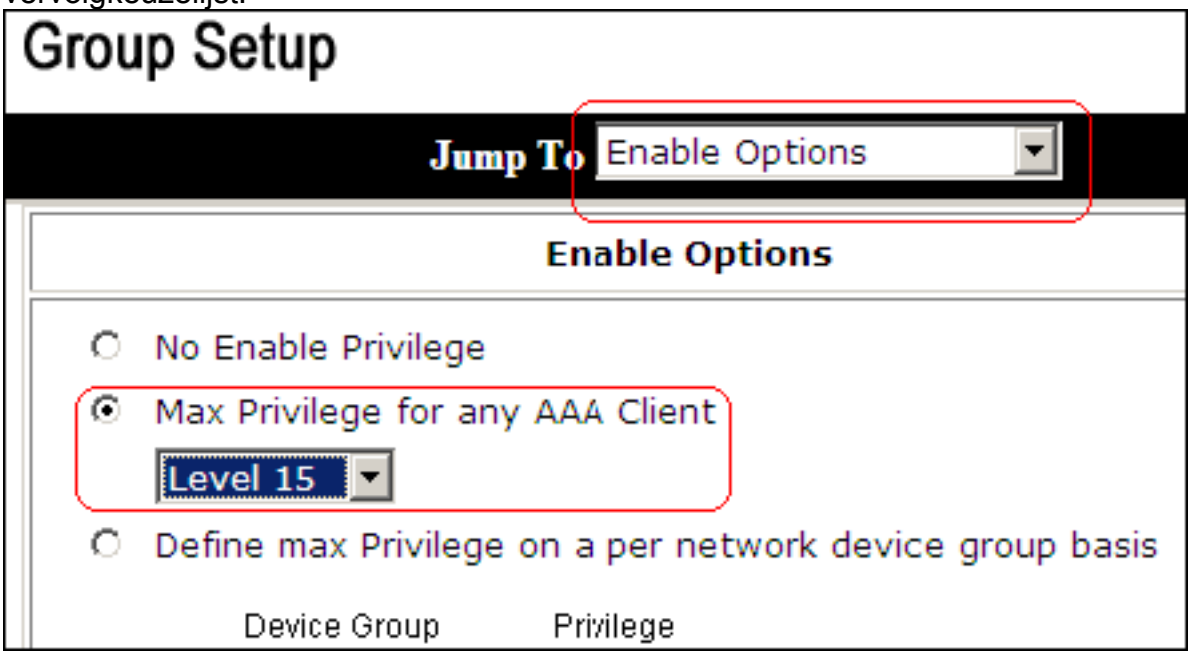
Raadpleeg de autorisatieset voor Shell-commando configureren voor een gebruikersgroepsectie van de gebruikershandleiding voor Cisco Secure Access Control Server 4.1 voor meer informatie over het configureren van de configuratie van de autorisatieset voor shell-opdrachten voor gebruikersgroepen.

Koppel de Shell Command Authorisation Set (ReadWrite Access) aan Gebruikersgroep (Admin Group)

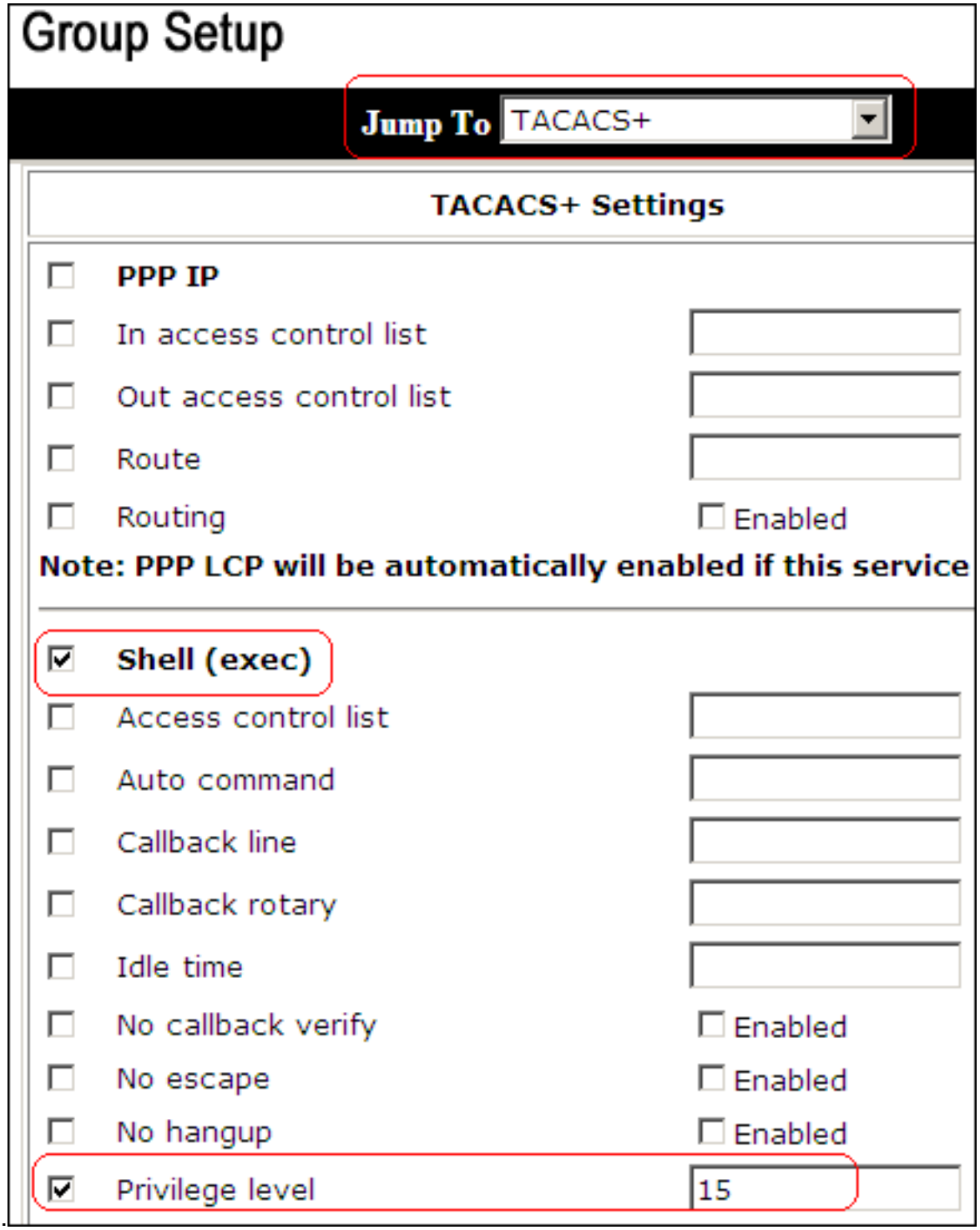
1. Klik in het ACS-venster op **Group Setup** en kies **Admin Group** in de vervolgkeuzelijst Group.



2. Klik op **Instellingen bewerken**.
3. Kies **Opties inschakelen** in de vervolgkeuzelijst **Jump** to.
4. Klik in het gebied Opties inschakelen op het keuzerondje **Max Privilege for any AAA client** en kies **Niveau 15** in de vervolgkeuzelijst.

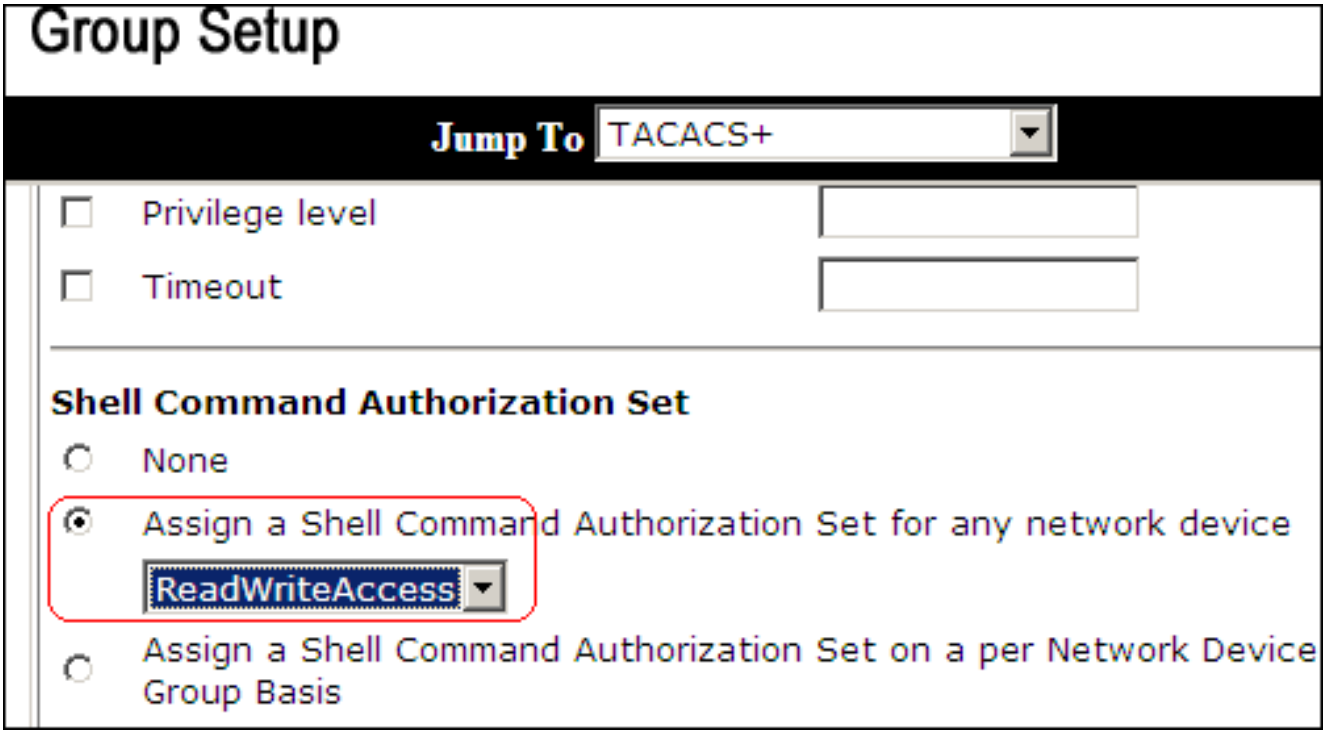


5. Kies **TACACS+** in de vervolgkeuzelijst Jump To.
6. In het gebied met TACACS+ instellingen vinkt u het aanvinkvakje **Shell (exec)** aan, vinkt u het aanvinkvakje **Privilege level** aan en voert u **15** in het veld Privilege level



in.

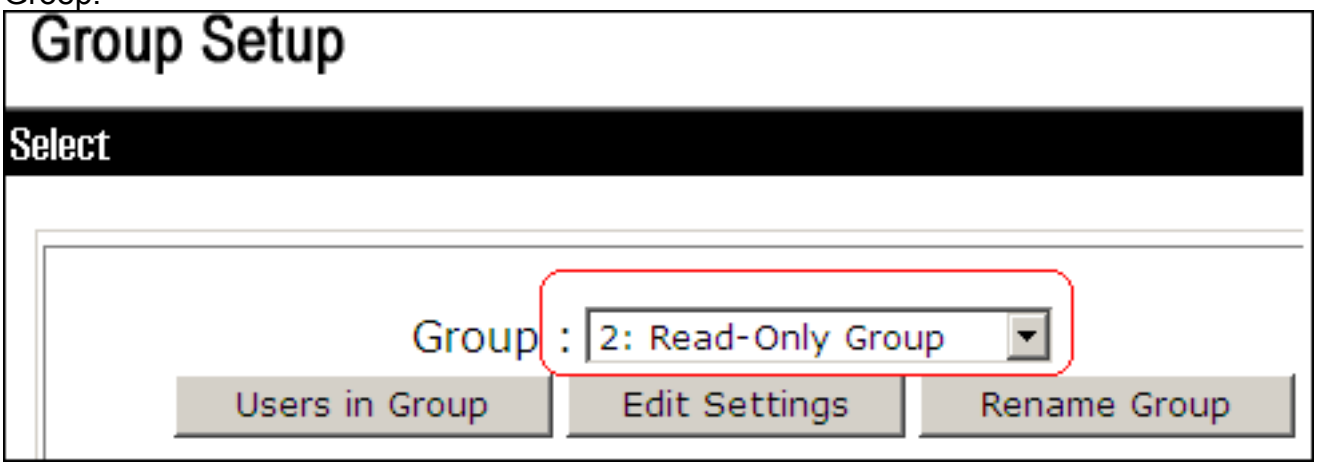
7. Klik in het gebied Shell Command Authorisation Set op de radioknop **Assign a Shell Command Authorisation Set voor elk netwerkapparaat** en kies **ReadWriteAccess** uit de vervolgkeuzelijst.



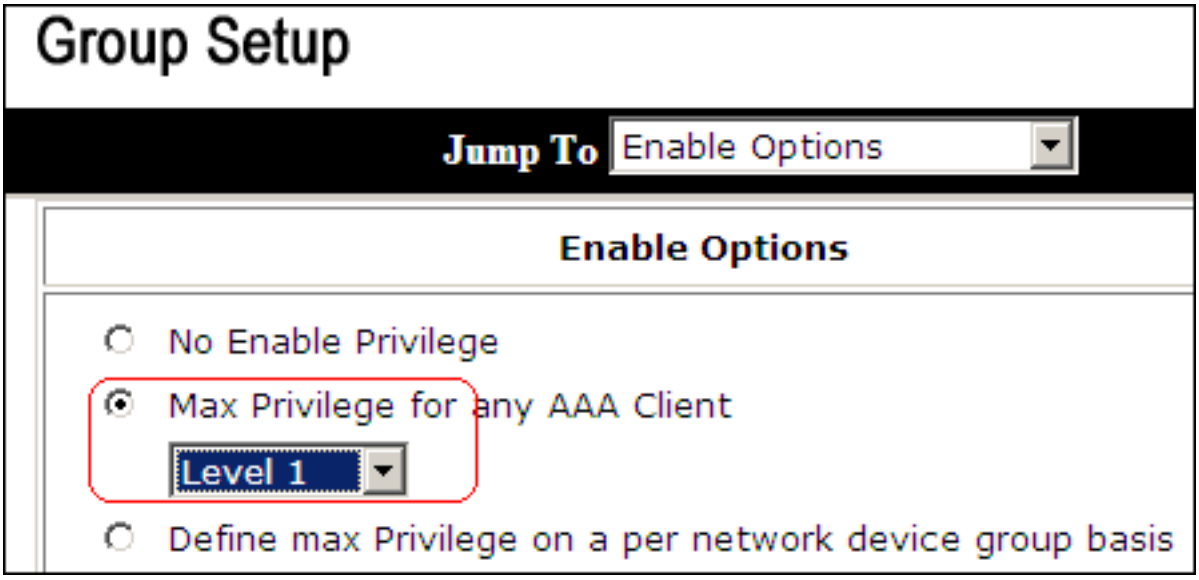
8. Klik op **Submit (Verzenden)**

Koppel de Shell Command Authorisation Set (ReadOnly Access) aan Gebruikersgroep (Alleen-lezen groep)

1. Klik in het ACS-venster op **Group Setup** en kies **Alleen-lezen groep** in de vervolgkeuzelijst Groep.

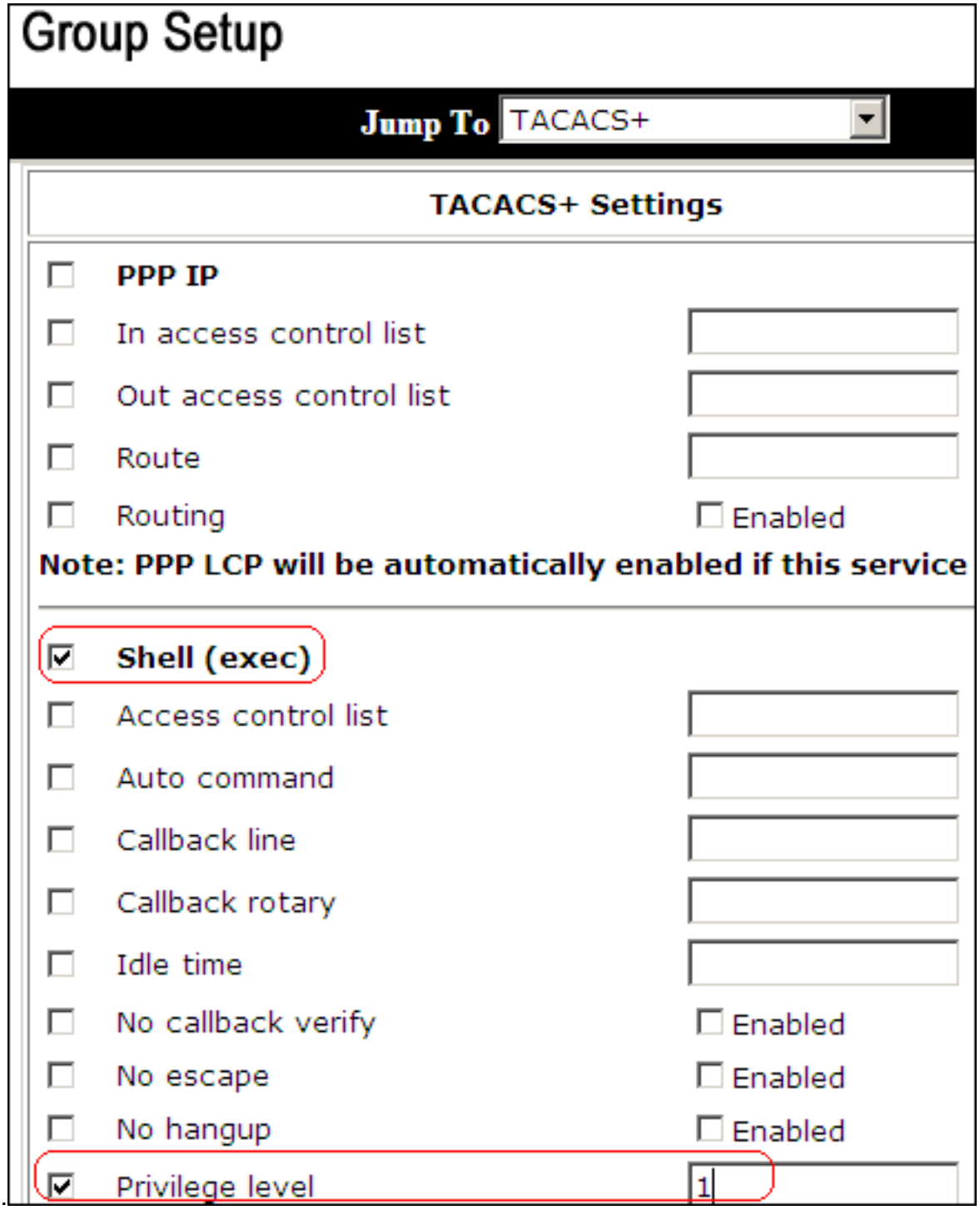


2. Klik op **Instellingen bewerken**.
3. Kies **Opties inschakelen** in de vervolgkeuzelijst **Jump** to.
4. Klik in het gebied Opties inschakelen op het keuzerondje **Max Privilege for any AAA client** en kies **niveau 1** in de vervolgkeuzelijst.



5. In het gebied met TACACS+ instellingen schakelt u het aanvinkvakje **Shell (exec) in**, schakelt u het aanvinkvakje **Privilege-niveau in** en voert u **1** in het veld Privilege-niveau

in.



6. Klik in het gebied Shell Command Authorisation Set op de radioknop **Assign a Shell Command Authorisation Set voor elk netwerkapparaat** en kies **ReadOnlyAccess** in de vervolgkeuzelijst.

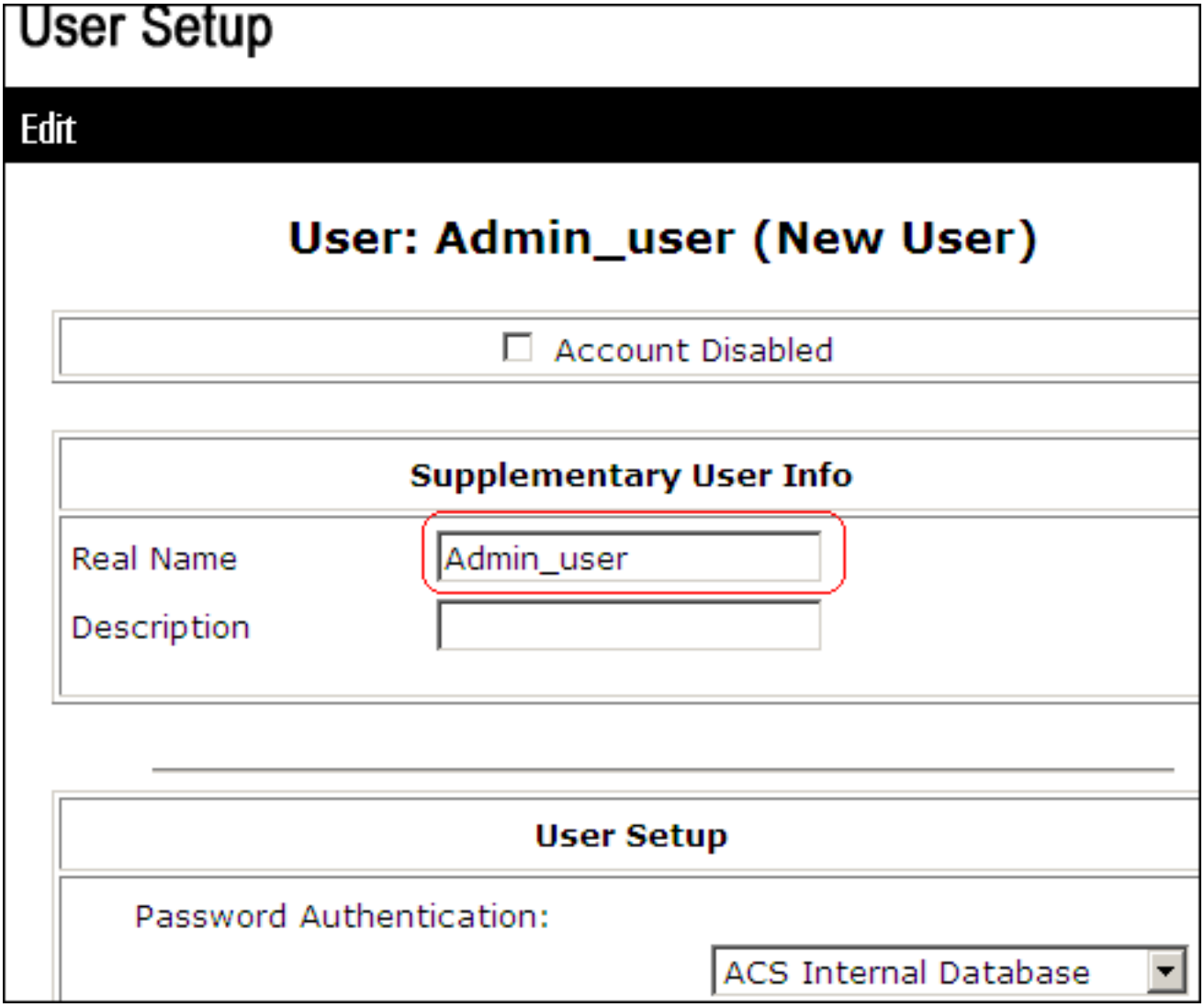
7. Klik op **Submit (Verzenden)**

Koppel de Shell Command Authorisation Set (Restricto_access) aan Gebruiker

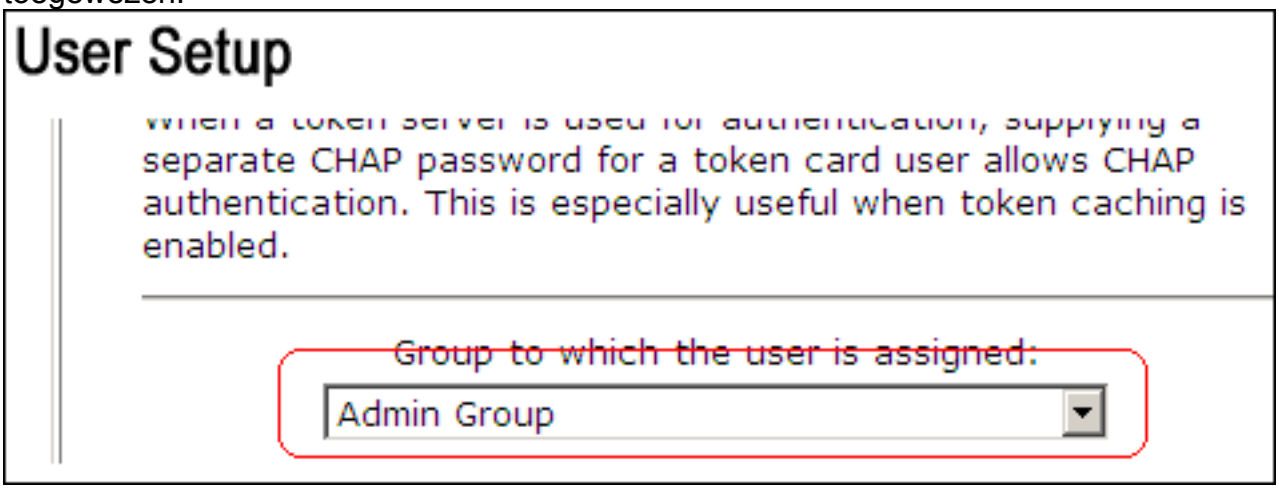
Raadpleeg de autorisatieset voor Shell-commando configureren voor een gebruikerssectie van de Gebruikersgids voor Cisco Secure Access Control Server 4.1 voor meer informatie over het configureren van de configuratie van de autorisatieset voor shell-opdrachten voor gebruikers.

Opmerking: Instellingen op gebruikersniveau negeren instellingen op groepsniveau in ACS, wat betekent dat als de gebruiker shell commando autorisatie ingesteld in de instellingen op gebruikersniveau heeft, het de instellingen op groepsniveau overtreedt.

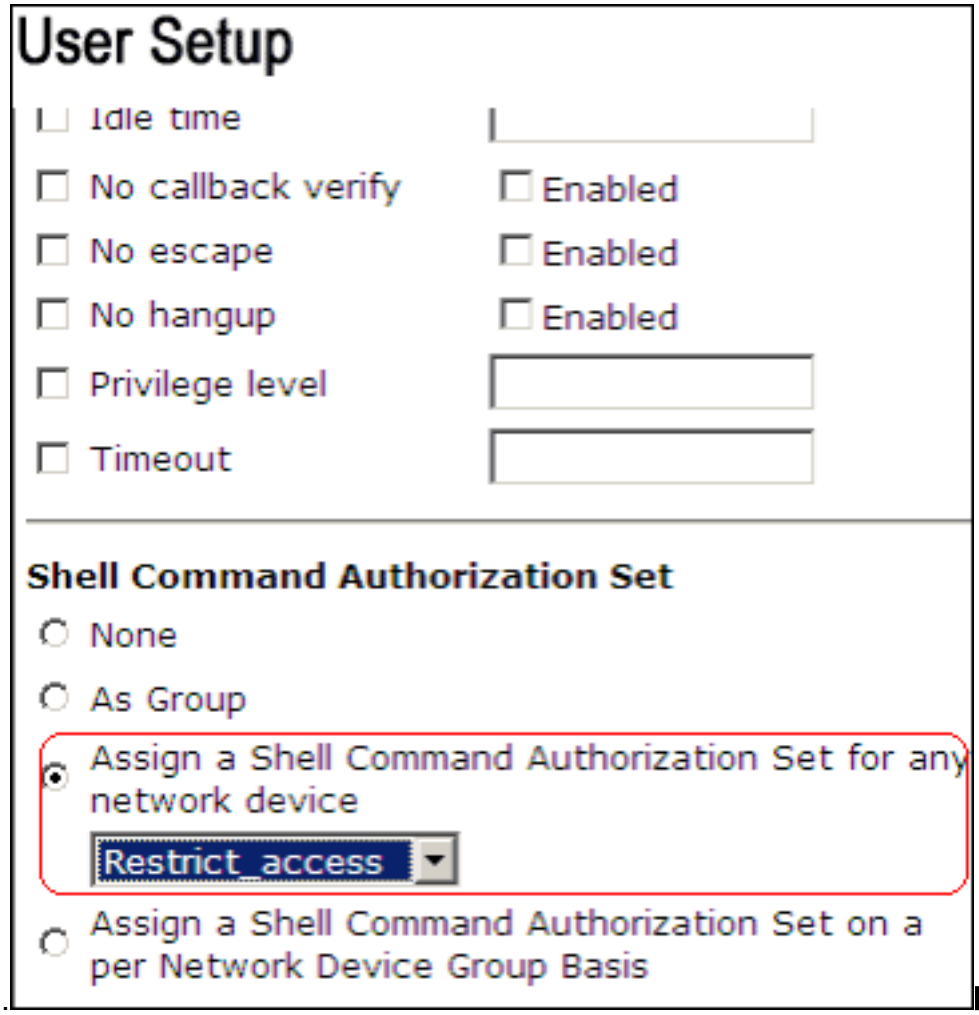
1. Klik op **Gebruikersinstelling > Toevoegen/bewerken** om een nieuwe gebruiker met de naam *Admin_user* te maken die deel uitmaakt van de Admin-groep.



2. Kies **Admin Group** in de groep waaraan de gebruiker vervolgkeuzelijst is toegewezen.



3. Klik in het gebied Shell Command Authorisation Set op de radioknop **Assign a Shell Command Authorisation Set voor elk netwerkapparaat** en kies **Restrict_access** in de vervolgkeuzelijst.**Opmerking:** in dit scenario maakt deze gebruiker deel uit van de Admin Group. De *Restricted_access* shell autorisatieset is van toepassing; de *ReadWrite Access* shell autorisatieset is niet van



toepassing.**N.B.:** Controleer in het gedeelte TACACS+ (Cisco) van het gebied Interface Configuration dat de optie **Shell (exec)** is geselecteerd in de kolom Gebruiker.

IOS-routerconfiguratie

Naast uw vooraf ingestelde configuratie zijn deze opdrachten vereist op een IOS-router of switch om opdrachtautorisatie via een ACS-server te implementeren:

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

ASA/PIX/FWSM-configuratie

Naast uw vooraf ingestelde configuratie zijn deze opdrachten vereist op ASA/PIX/FWSM om opdrachtautorisatie via een ACS-server te implementeren:

```
aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

Opmerking: het is niet mogelijk het RADIUS-protocol te gebruiken om de toegang van gebruikers

tot ASDM voor alleen-lezen doeleinden te beperken. Aangezien de RADIUS-pakketten verificatie en autorisatie op hetzelfde moment bevatten, hebben alle gebruikers die zijn geverifieerd op de RADIUS-server een prioriteitsniveau van 15. U kunt dit bereiken via TACACS met de implementatie van opdrachtautorisatiesets.

Opmerking: ASA/PIX/FWSM doen er lang over om elk getypt commando uit te voeren, zelfs als ACS niet beschikbaar is om commando-autorisatie uit te voeren. Als ACS niet beschikbaar is en ASA de opdrachtautorisatie heeft geconfigureerd, zal ASA nog steeds de opdrachtautorisatie aanvragen voor elke opdracht.

Problemen oplossen

Fout: opdrachtautorisatie is mislukt

Probleem

Nadat u via TACACS-logboekregistratie bent aangemeld bij de firewall, werken opdrachten niet. Wanneer u een opdracht invoert, wordt deze fout ontvangen: `opdrachtautorisatie is mislukt.`

Oplossing

Voer de volgende stappen uit om dit probleem op te lossen:

1. Zorg ervoor dat de juiste gebruikersnaam wordt gebruikt en dat alle vereiste rechten aan de gebruiker worden toegewezen.
2. Als de gebruikersnaam en de rechten correct zijn, verifieert dat ASA connectiviteit met ACS heeft en dat ACS actief is.

Opmerking: deze fout kan ook optreden als de beheerder per ongeluk opdrachtautorisatie heeft ingesteld voor lokale gebruikers en TACACS-gebruikers. In dit geval, voer een wachtwoordherstel uit om de kwestie op te lossen.

Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Referenties voor Cisco Secure PIX-firewall-opdracht
- Security-meldingen uit het productveld (inclusief PIX)
- Requests for Comments (RFC's)
- Ondersteuning voor Cisco Secure Control Access Control Server
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.