RADIUS-configuratie met Cisco 2000/3000 Series beheerde Switches en Windows-server 2008

Doel

Remote Authorisation Dial-in User Service (RADIUS) biedt een robuuste manier van authenticatie van gebruikers om toegang tot een netwerkdienst mogelijk te maken. Daarom bieden RADIUS-servers een gecentraliseerd toegangsbeheer, waarbij de serverbeheerder beslist of een specifiek segment al dan niet met RADIUS wordt geverifieerd. In dit artikel worden de algemene stappen beschreven om RADIUS in een client/server-omgeving op te zetten, waarbij de client wordt vertegenwoordigd door de Cisco 200/300 Series beheerde Switch en de server een Windows Server 2008 met RADIUS ingeschakeld uitvoert.

Toepasselijke apparaten

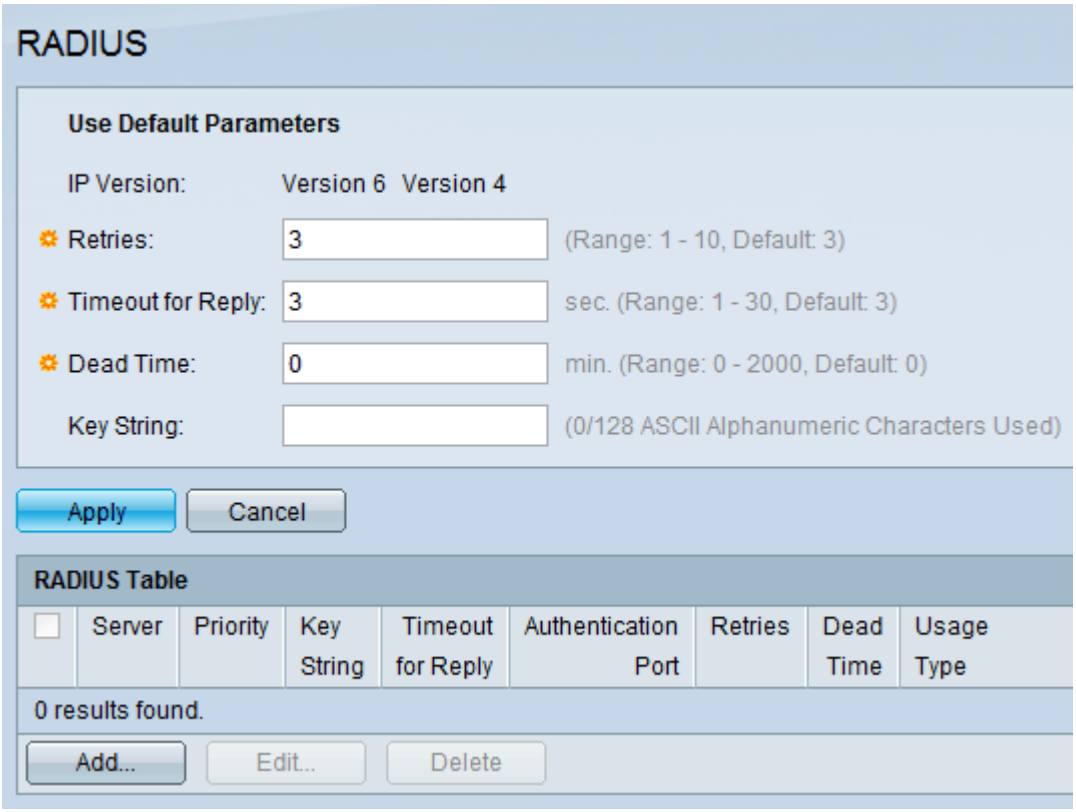
- Cisco 2600/3600 Series beheerde Switches

Stapsgewijze procedure

De configuratie vindt plaats in twee delen. Eerst moeten we de switch instellen als een RADIUS-client, dan moeten we de server correct instellen voor RADIUS.

RADIUS-instelling op de switch

Stap 1. Kies in het configuratiehulpprogramma SG200/300 Series **Security > RADIUS**. De pagina *RADIUS* wordt geopend:

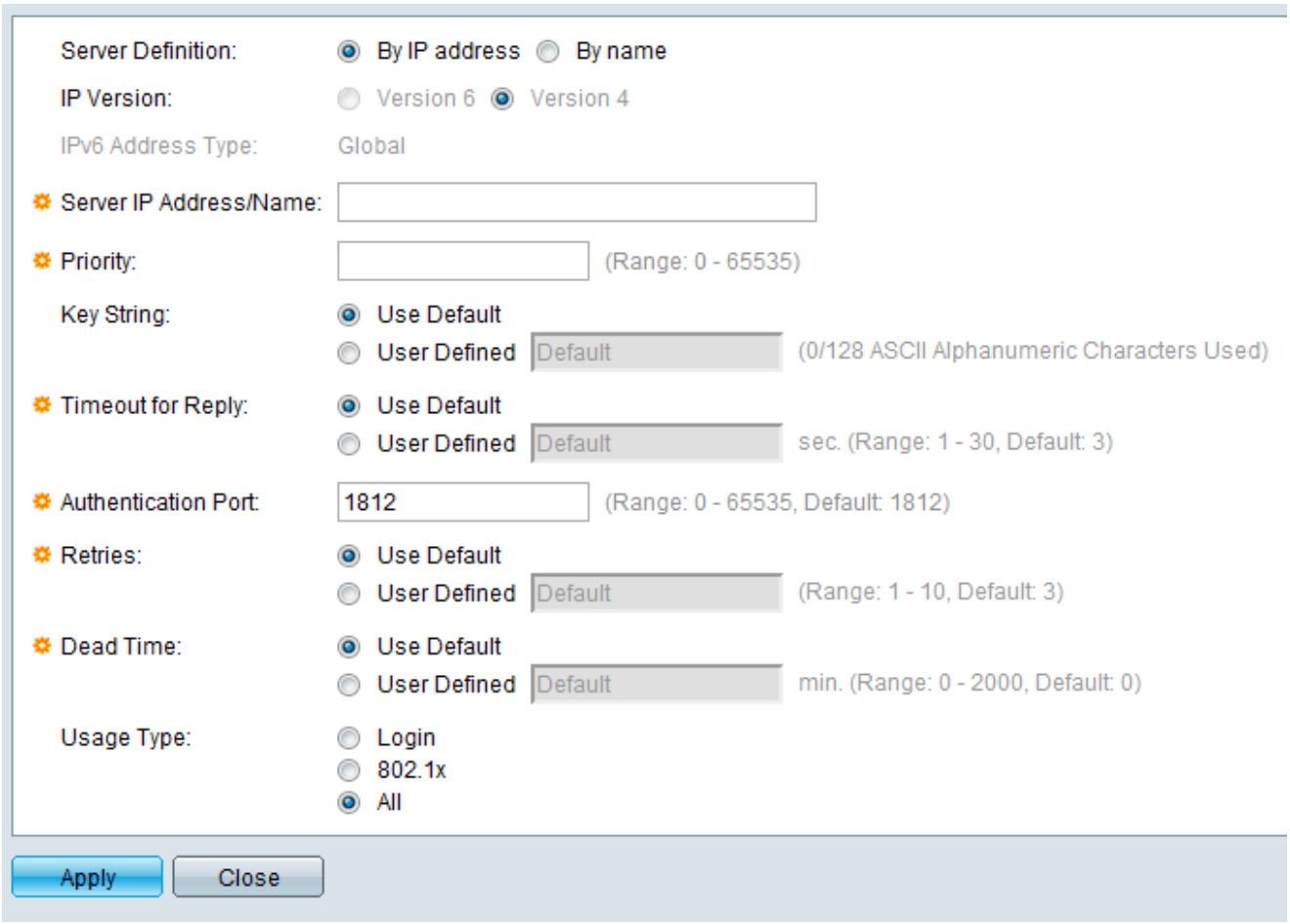


Stap 2. Voer de standaardinstellingen voor RADIUS in.

- IP Versie - Hier wordt de ondersteunde IP-versie weergegeven.
- Pogingen — Voer in dit veld het aantal verzonden aanvragen in dat naar de RADIUS-server wordt verzonden voordat een fout optreedt.
- Time-out voor antwoord — Voer in dit veld de tijd in (in seconden) dat de switch wacht op een antwoord van de RADIUS-server voordat hij een query opnieuw probeert.
- Dode tijd — Voer in dit veld de tijd in minuten in die de switch wacht voordat hij de RADIUS-server omzeilt.
- Key String — Voer in dit veld de standaardstring in die wordt gebruikt voor verificatie en codering tussen de switch en de RADIUS-server. De toets moet overeenkomen met de toets die op de RADIUS-server is ingesteld.

Stap 3. Klik op **Toepassen** om de actieve configuratie van de switch met de RADIUS-instellingen bij te werken.

Stap 4. U moet de RADIUS-server aan de switch toevoegen. Klik op **Add** (Toevoegen). De pagina *RADIUS-server toevoegen* wordt geopend in een nieuw venster:



Stap 5. Voer in de velden de waarden in voor de server. Als u de standaardwaarden wilt gebruiken, selecteert u **Standaard gebruiken** in het gewenste veld.

- Serverdefinitie — In dit veld geeft u aan hoe u verbinding kunt maken met de server, op IP-adres of op naam van de server.
- IP-versie — Als de server wordt geïdentificeerd aan de hand van IP-adres, selecteert u IPv4- of IPv6-adres.
- IPv6-adrestype — In dit veld wordt het algemene type van het IPv6-adres weergegeven.
- IP-adres/naam server — Voer in dit veld het IP-adres of de domeinnaam van de RADIUS-server in.
- Prioriteit — Voer in dit veld de prioriteit van de server in. Als er meer dan één server is geconfigureerd, zal de switch proberen verbinding te maken met elke server volgens deze prioriteitswaarde.
- Key String — Voer in dit veld de standaardstring in die wordt gebruikt voor verificatie en codering tussen de switch en de RADIUS-server. De toets moet overeenkomen met de toets die op de RADIUS-server is ingesteld.
- Time-out voor antwoord — Voer in dit veld de tijd in (in seconden) dat de switch wacht op een antwoord van de RADIUS-server voordat hij een query opnieuw probeert.
- Verificatiepoort — Voer in dit veld het UDP-poortnummer in dat voor de RADIUS-server is ingesteld voor verificatieverzoeken.
- Pogingen — Voer in dit veld het aantal verzonden aanvragen in dat naar de RADIUS-server wordt verzonden voordat een fout optreedt.
- Dode tijd — Voer in dit veld de tijd in minuten in die de switch wacht voordat hij de RADIUS-server omzeilt.
- Gebruikstype — Voer in dit veld het verificatietype van de RADIUS-server in. Er zijn drie

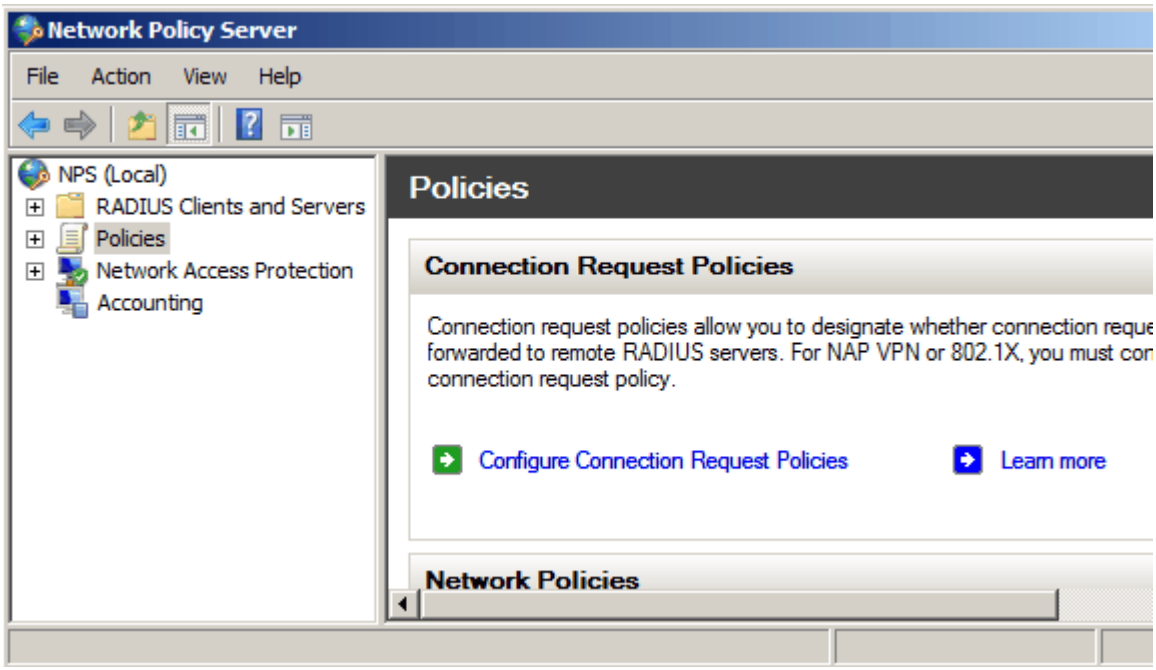
opties:

- Aanmelden — RADIUS-server verifieert gebruikers die de switch willen beheren.
- 802.1X — RADIUS-server wordt gebruikt voor 802.1X-verificatie.
- Alle — RADIUS-servers worden gebruikt voor login en 802.1X-verificaties.

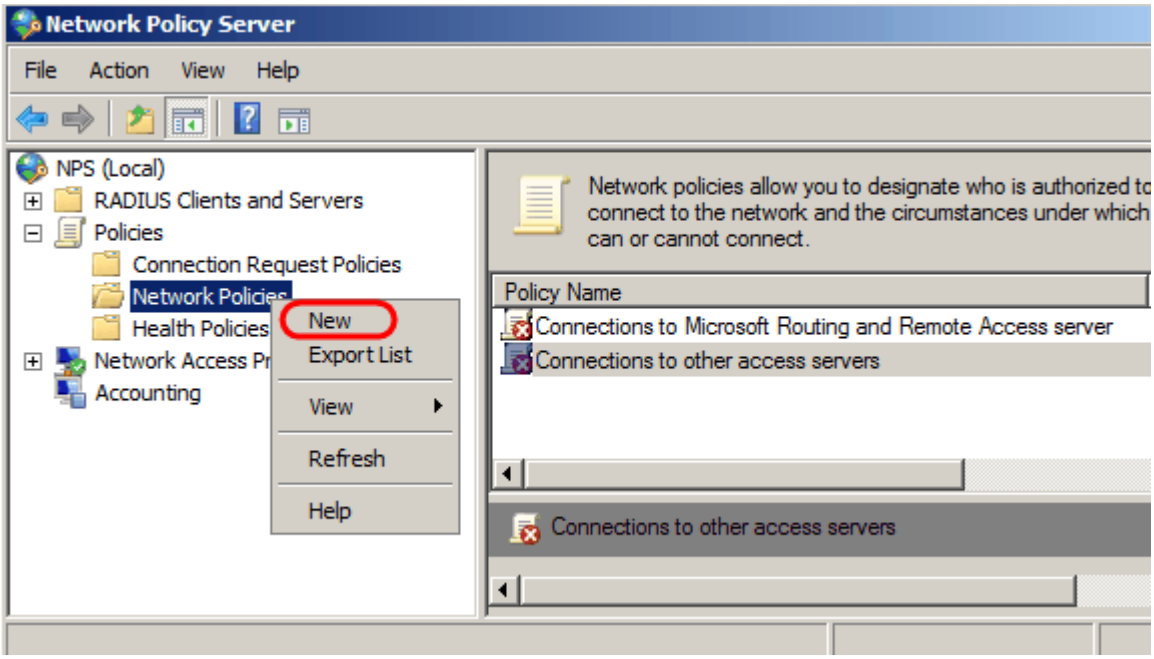
Stap 6. Klik op **Toepassen** om de serverdefinitie toe te voegen aan de actieve configuratie van de switch.

Windows Server 2008 configureren voor RADIUS

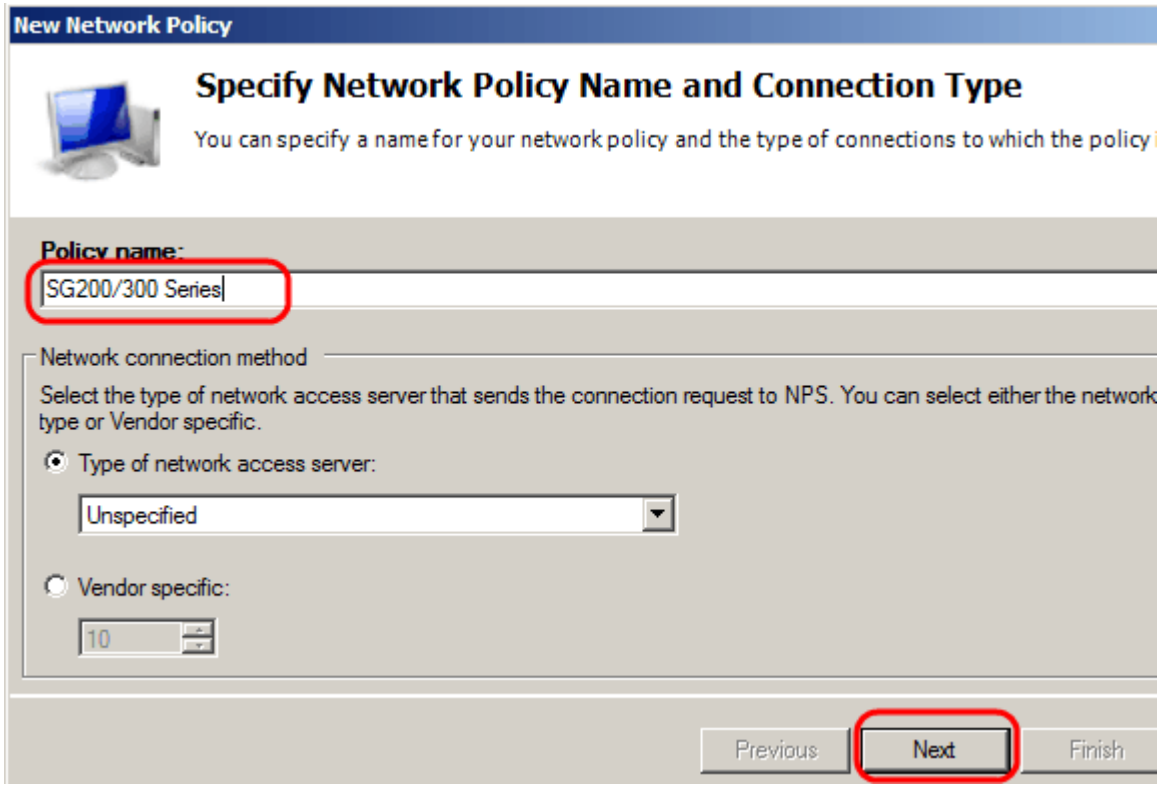
Stap 1. Kies op de Windows Server 2008-machine **Start > Administratieve tools > Network Policy Server**. Het venster *Network Policy Server* opent:



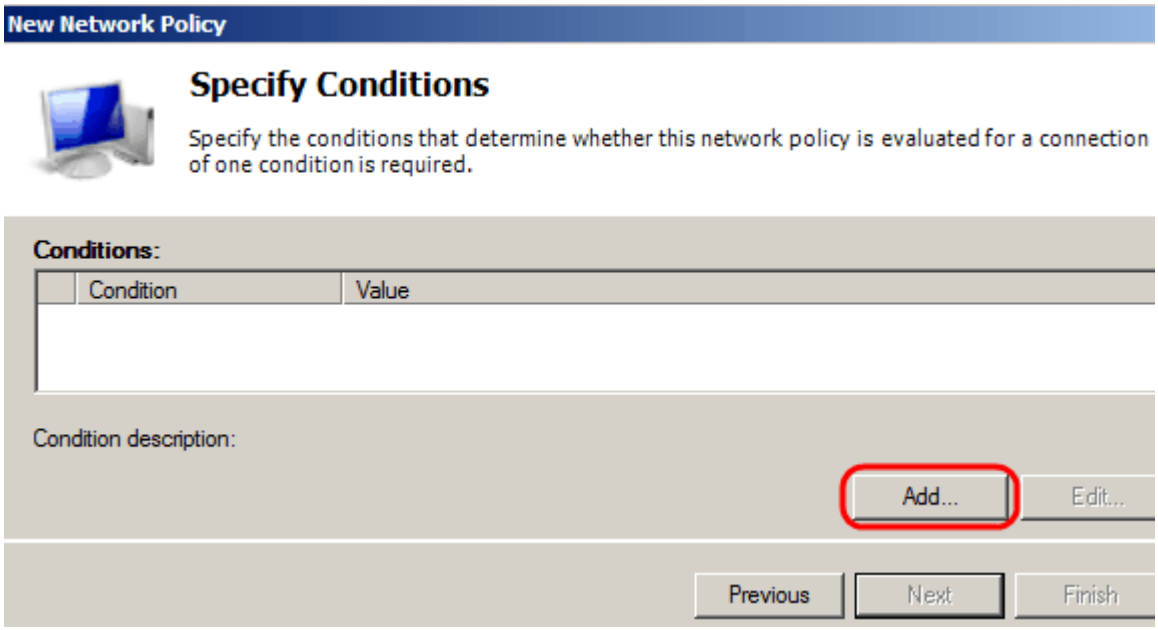
Stap 2. Om de RADIUS-server in te schakelen voor een specifiek segment van het netwerk, moet u een nieuw netwerkbeleid maken. Als u een nieuw netwerkbeleid wilt maken, kiest u **Beleid > Netwerkbeleid**, klikt u met de rechtermuisknop en vervolgens selecteert u **Nieuw**. Het *nieuwe* venster *Netwerkbeleid* wordt geopend:



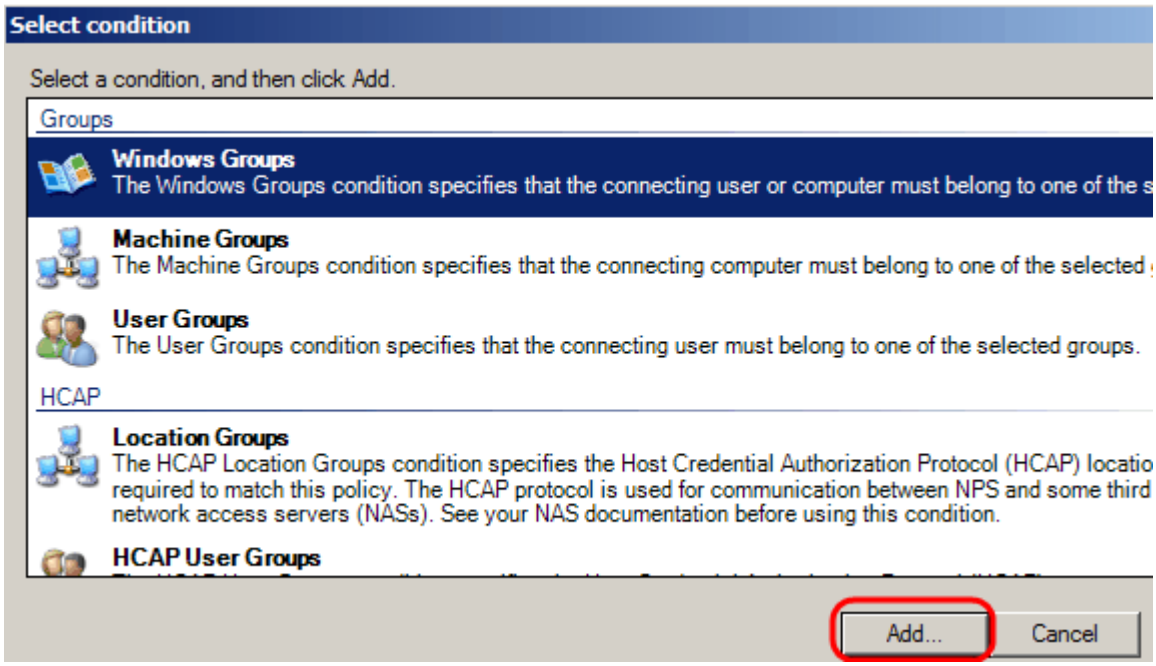
Stap 3. Voer in het veld Beleidsnaam de naam voor het nieuwe beleid in. Klik op **Next** (Volgende).



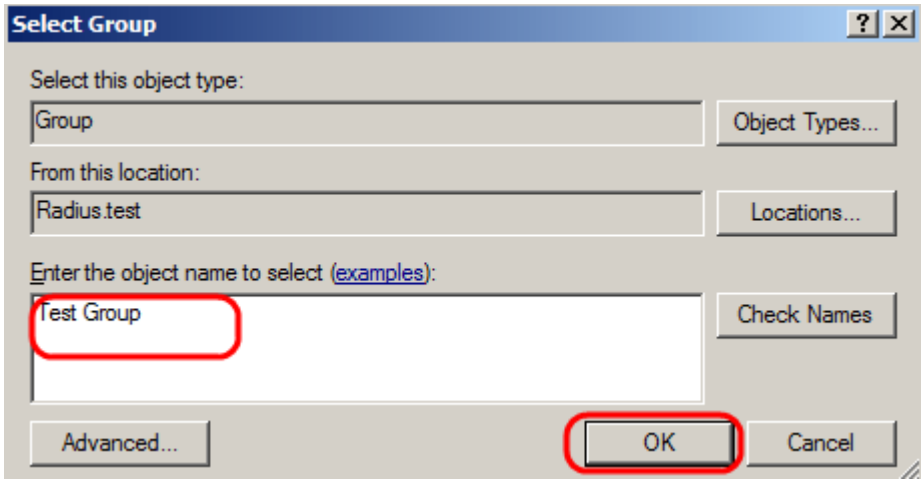
Stap 4. U moet de voorwaarden van dit beleid specificeren. Er zijn twee voorwaarden nodig: aan welk segment van gebruikers de RADIUS-server wordt geïmplementeerd en welke methode wordt gebruikt om verbinding met dit segment te maken. Klik op **Add** om deze voorwaarden toe te voegen.



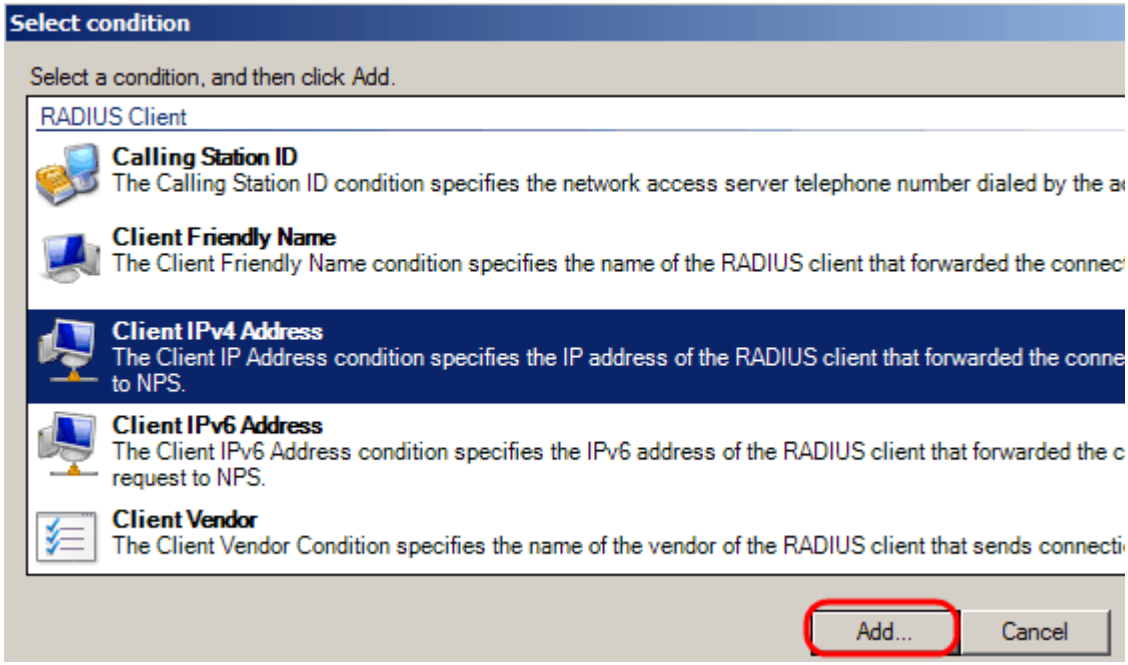
Stap 5. Onder Groepen zijn er drie opties: Windows-groepen, Machinegroepen en Gebruikersgroepen. Kies de groep volgens de instelling van het netwerk en klik op **Toevoegen**. Er wordt een nieuw venster geopend naar gelang de geselecteerde groep. Klik op **Groepen toevoegen**.



Stap 6. Selecteer het objecttype, de locatie en voer de naam van het object in. Klik op **OK** en vervolgens op **OK**. Klik op **Add** om de volgende voorwaarde toe te voegen.

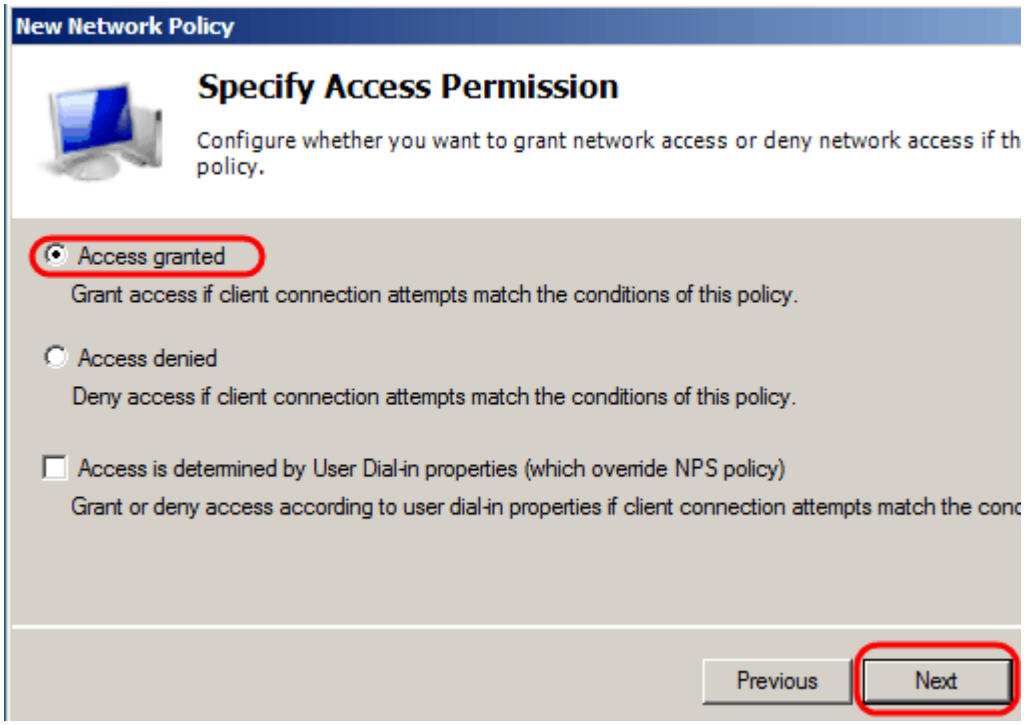


Stap 7. Selecteer onder RADIUS-client de optie IPv4-adres als de methode om de server aan te sluiten op de RADIUS-clients. Dit is in dit geval het IP-adres van de switch. Klik op **Add** (Toevoegen).

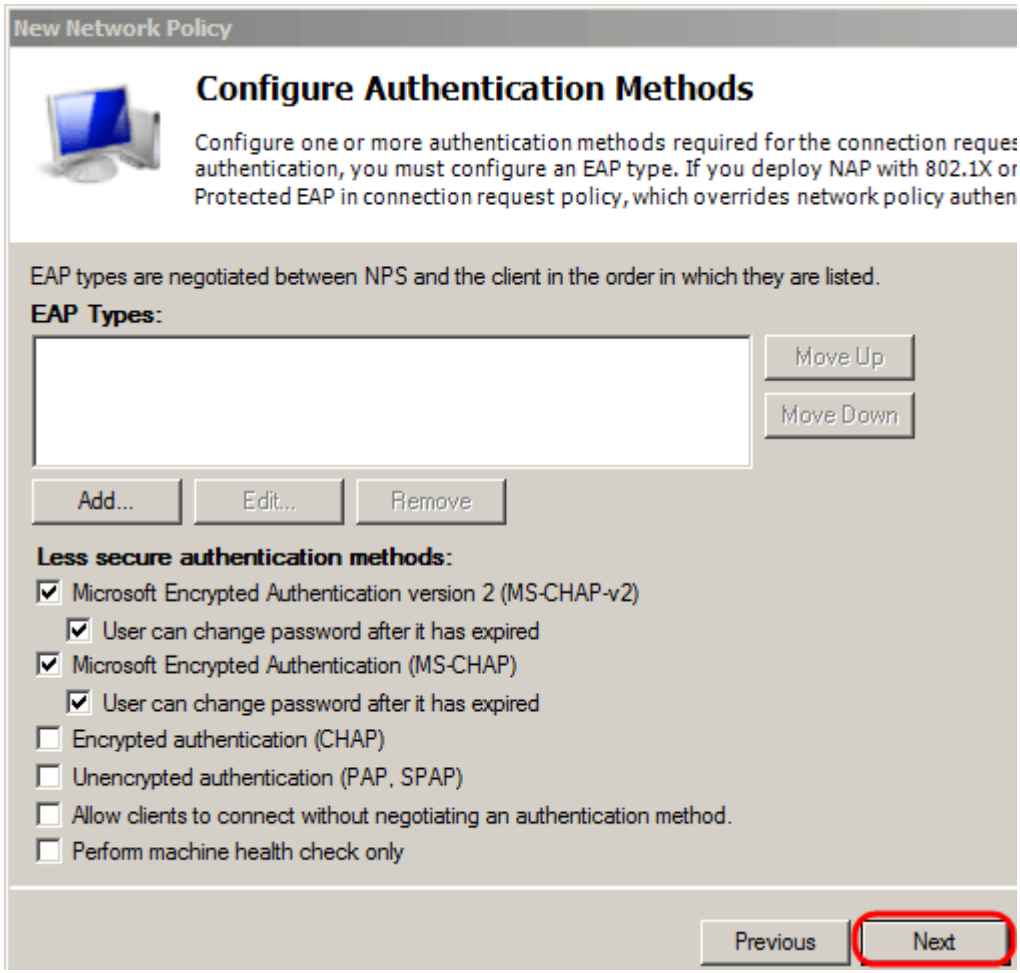


Stap 8. Voer het bijbehorende IP-adres in en klik op **OK**. Er wordt een lijst met toegevoegde voorwaarden weergegeven. Klik op **Volgende**.

Stap 9. Selecteer op de pagina Toegangsrechten opgeven de optie **Toegekende toegang opgeven**. Klik op **Next** (Volgende).



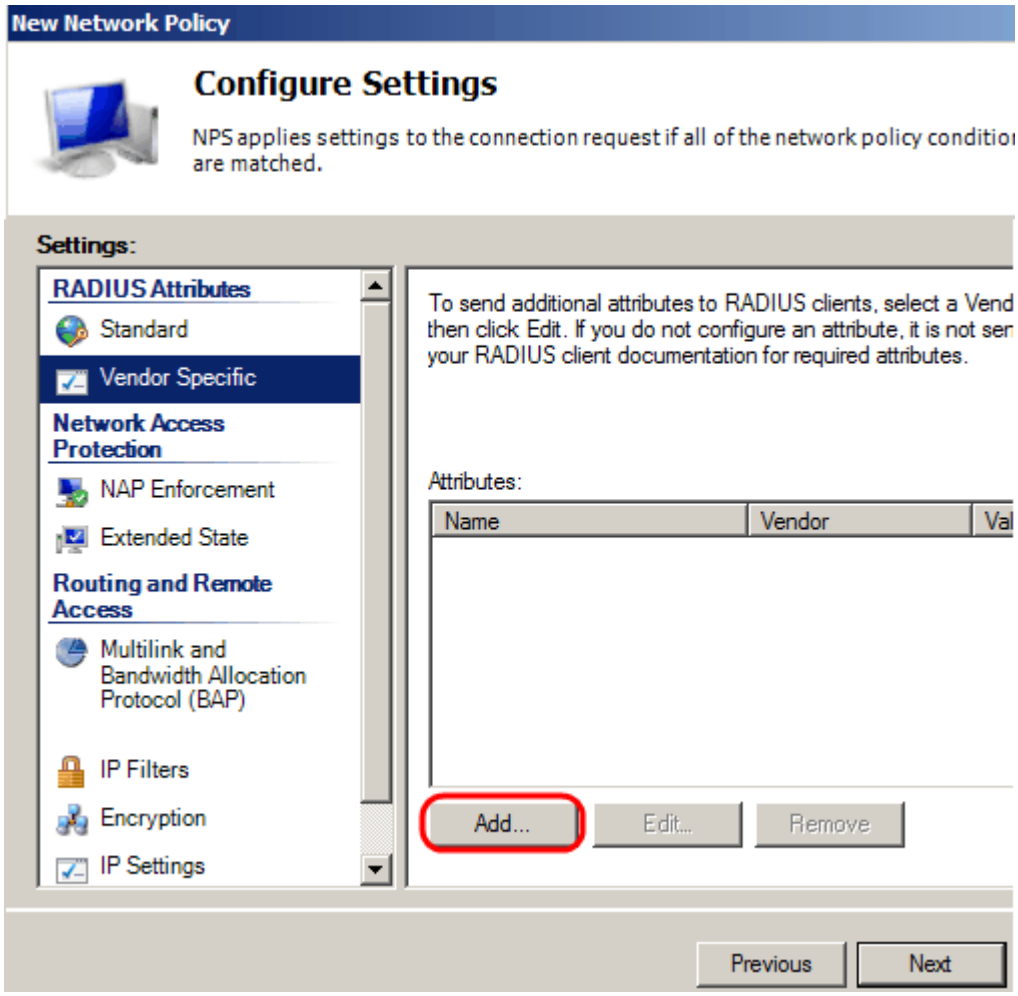
Stap 10. Stel op de verificatiepagina de verificatiemethode in die het best op uw netwerk past. Klik op **Next** (Volgende).



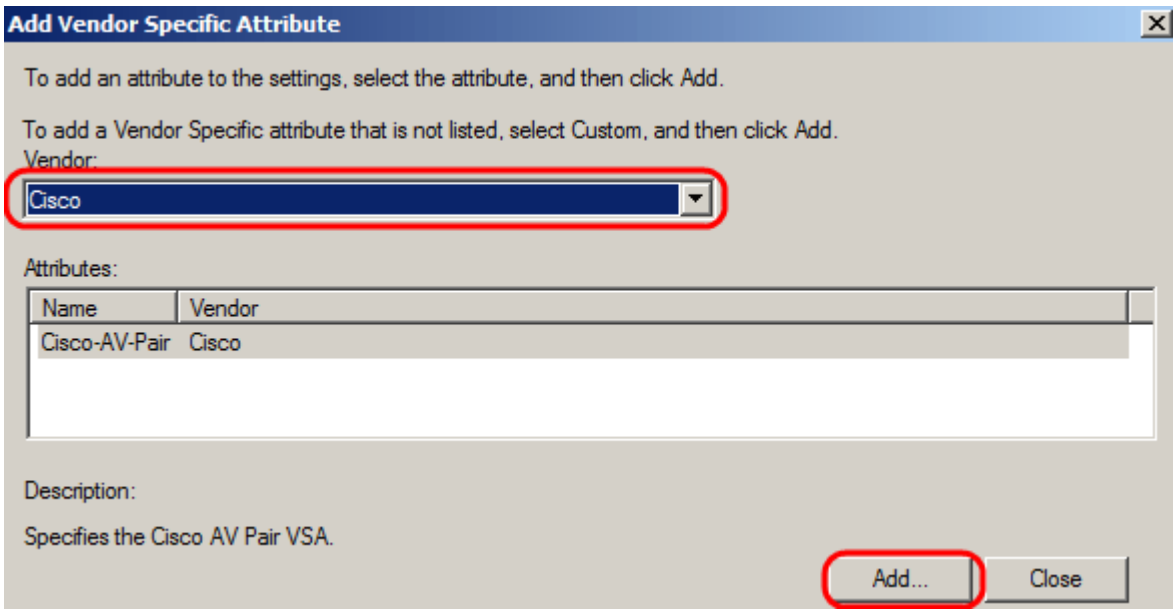
Stap 11. Gebruik in het venster Constricties configureren de standaardwaarden. Klik op **Next** (Volgende).

Stap 12. Klik op de pagina Instellingen configureren onder RADIUS-kenmerken op **Verkoopspecifiek** en klik vervolgens op **Toevoegen**.

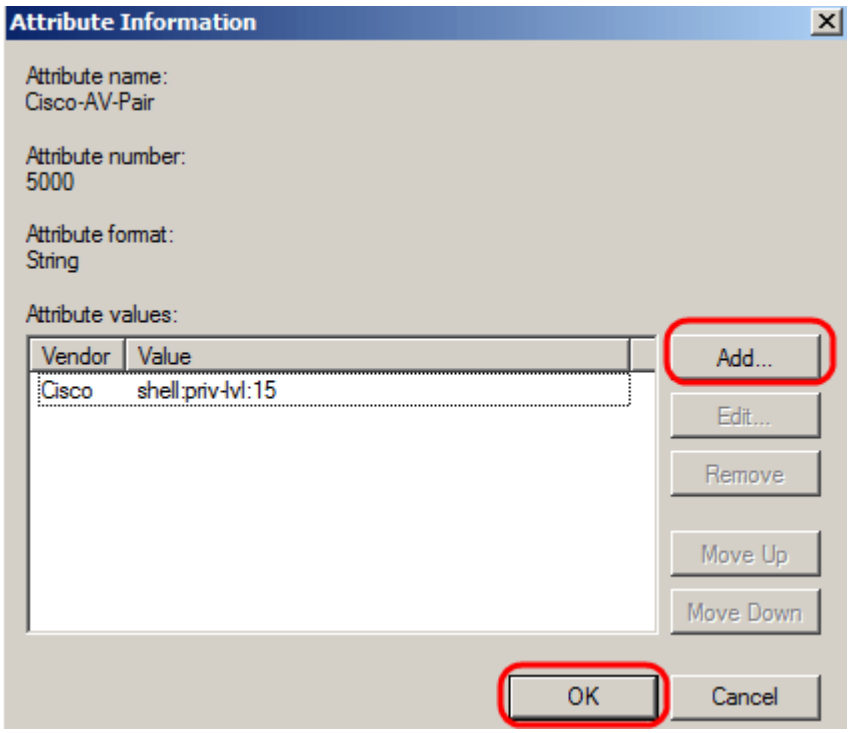
N.B.: De overige instellingen op deze pagina zijn ingesteld op hun standaardwaarden. U hoeft alleen maar te zorgen voor de specifieke instellingen van de leverancier.



Selecteer onder Verkoper **Cisco**. Klik op **Add** (Toevoegen). Het venster *met* de *informatie over kenmerken* wordt geopend.



Klik in het venster Kenmerkinformatie op **Add** en voer de waarde shell:priv-lvl:15 in. Klik op **OK**.



Opmerking:dit is de waarde die door Cisco is toegewezen zodat de RADIUS-server toegang kan verlenen tot het web-based switch Configuration utility.

Klik op **OK** om het venster met de kenmerken te sluiten en klik vervolgens op **Sluiten** om het venster met de specifieke kenmerken van de leverancier toe te voegen. Klik op **Next** (Volgende).

Stap 13. Er wordt een samenvatting van de instellingen voor dit beleid weergegeven. Klik op **Voltooien**. Het netwerkbeleid wordt gemaakt.

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

SG200/300 Series

Policy conditions:

Condition	Value
Windows Groups	RADIUS\Test Group
Client IPv4 Address	192.168.1.10

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous | Next | Finish

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.