Cisco QuickVPN-installatietips voor Windows-besturingssystemen

Bezoek http://youtu.be/hHu2z6A78N8 voor een video met installatietips voor Quick VPN

Doel

Cisco QuickVPN is een gratis software die is ontworpen voor externe toegang tot een netwerk. Het is eenvoudig te installeren op een PC en eenvoudig te beheren. QuickVPN is compatibel met Windows-besturingssysteem (zowel de 32-bits als de 64-bits edities). Om QuickVPN goed te laten werken, moet er een aantal vereisten worden afgevinkt om de VPN-verbinding met het netwerk te kunnen garanderen.

In dit artikel worden de vereisten en tips voor het correct uitvoeren van QuickVPN toegelicht, evenals een uitleg van hoe QuickVPN toegang krijgt tot uw netwerk.

Toepasselijke apparaten

â€¢RV215W
â€¢RV110W
· RV180/RV180W
RV120W
RV220W
· RV016
· RV042/RV042G
· RV082
· RVS4000
SA520/SA520W
SA540
· WRV200
· WRV210
· WRVS4400N
· Windows XP, Windows Vista, Windows 7

QuickVPN-proces

Het volgende is een uitleg van hoe QuickVPN werkt in uw computer en waarom het belangrijk is om aan de vereisten te voldoen voordat u QuickVPN probeert uit te voeren.

1. De client maakt verbinding met de router met behulp van SSL (Secure Socket Layer). De verbinding gebruikt poortnummer 443 of 60443 (afhankelijk van uw VPN-configuratie op de router) en zoekt naar een certificaat. Raadpleeg voor meer informatie de sectie *Routervereisten*.

Opmerking: als u een certificaat gebruikt, zorg er dan voor dat dit in de computer is opgeslagen. Anders klikt u op **Nee** om een certificaat niet te gebruiken wanneer het waarschuwingsbericht voor het certificaat verschijnt.

2. De gebruikersnaam en het wachtwoord voor de client worden door de router geverifieerd. Zodra de gebruiker wordt geverifieerd, wordt de IPSec-tunnel vervolgens geopend.

Opmerking: als u niet kunt inloggen op VPN, ontvangt u een foutmelding.

3. De client verzendt een ICMP Echo-verzoekpakket naar het interne IP-adres van de router. De router antwoordt terug met een pakket van het Antwoord van ICMP Echo. Het doel is om verbinding te maken tussen beide doelen. Dit is waarom u ervoor moet zorgen (afhankelijk van uw besturingssysteem) om de juiste vereisten voor ICMP in te stellen. Raadpleeg voor meer informatie de sectie *Windows Vista / Windows 7 Operating System Requirements*.

Opmerking: Als de verbinding mislukt, krijgt u een foutbericht van een externe gateway die niet reageert.

Routervereisten

Hieronder is een lijst van vereisten uw kleine bedrijfsrouter moet voldoen.

· Beheer op afstand moet zijn ingeschakeld voor poorten 443 en 60443.

· Gebruikers moeten de VPN-tunnel maken en inschakelen.

· Gebruikersnaam en wachtwoord zijn beide hoofdlettergevoelig en moeten aan beide uiteinden van de verbinding overeenkomen.

· Er is slechts één verbinding per gebruikersaccount toegestaan.

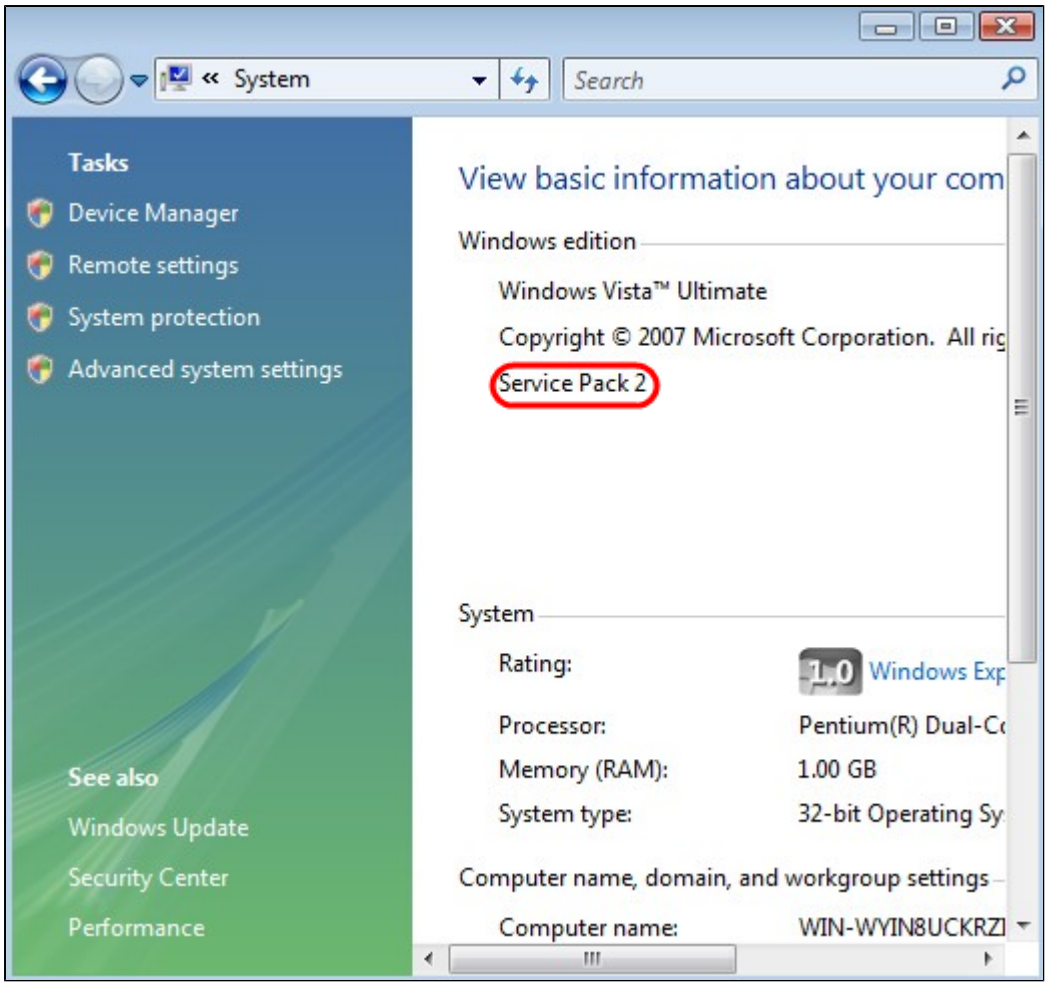
· Lokale netwerksubnetwerkknooppunt moet verschillen van het externe netwerksubnetwerkknooppunt.

· Als u een certificaat gebruikt, moet het certificaatbestand op uw computer worden opgeslagen in de map QuickVPN Client.

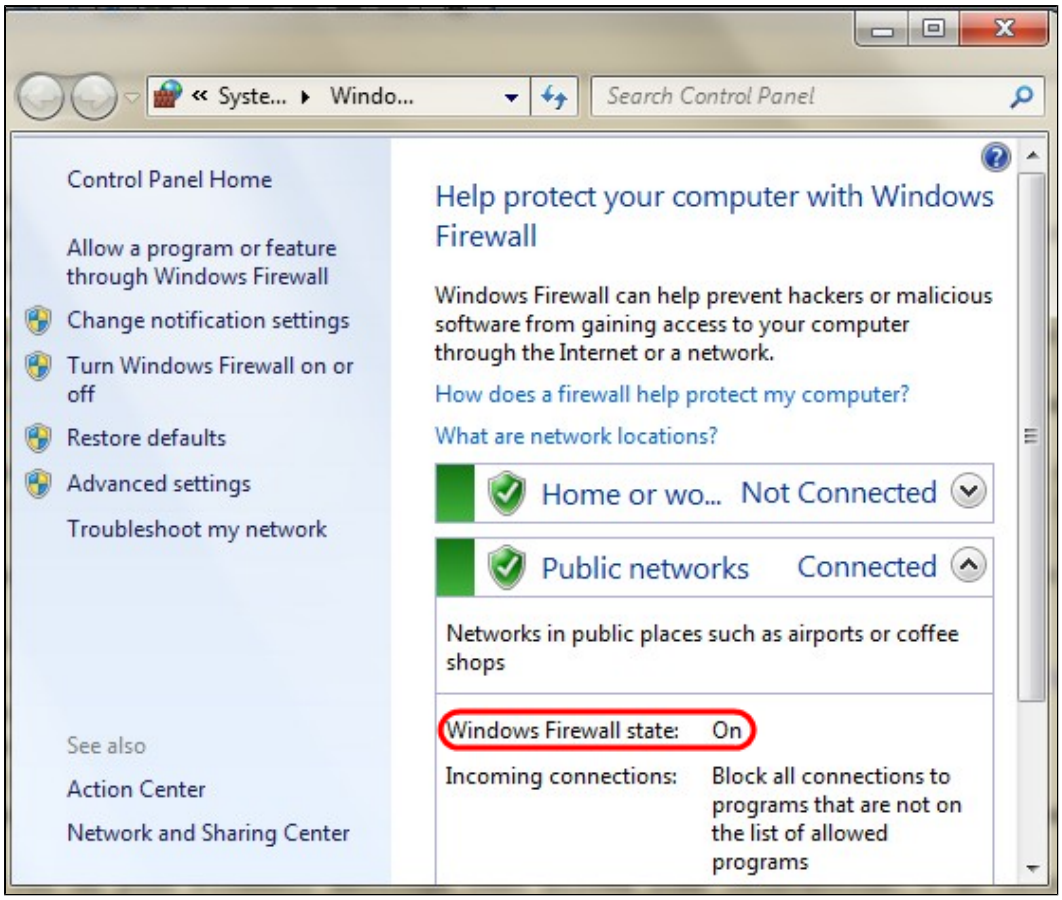
Vereisten voor Windows Vista/Windows 7-besturingssysteem

Stap 1. Als uw computer Windows Vista heeft, moet u Service Pack 2 of Vista Service Pack 2 compatibiliteit voor Windows 7 hebben geïnstalleerd. Om dit te controleren, kiest u **Start > Systeemeigenschappen computer**. Als uw computer Windows 7 heeft, sla deze stap dan over.

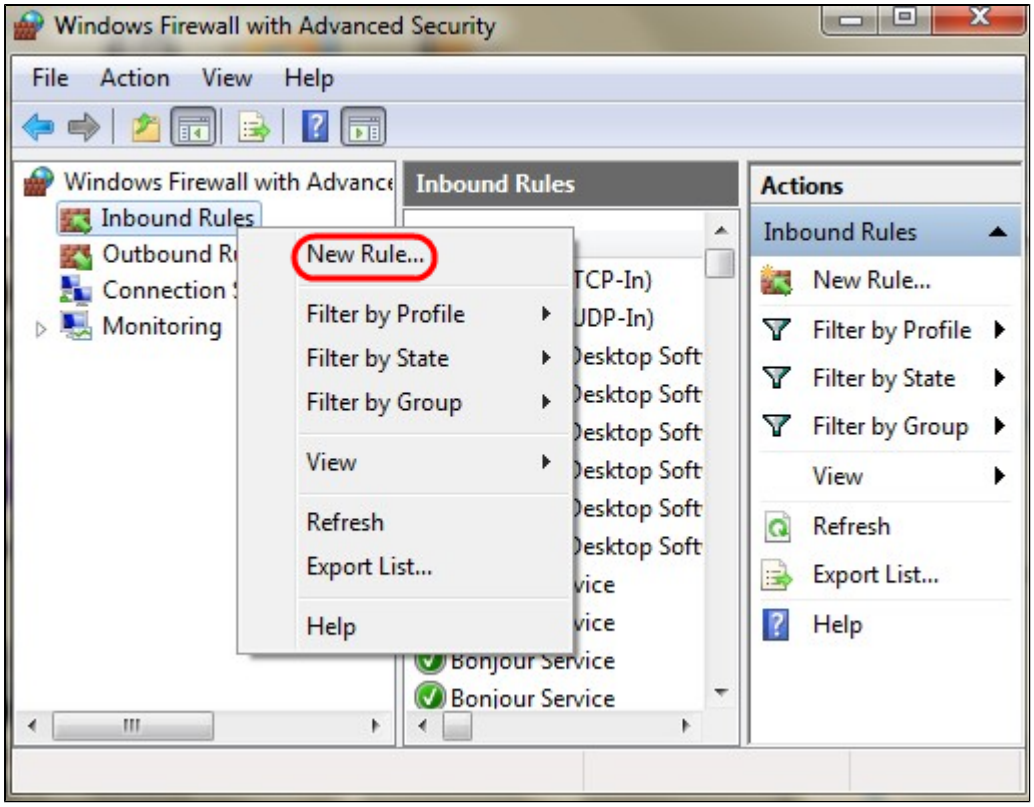
Opmerking: Als u voor Windows Vista het Service Pack niet hebt geïnstalleerd, kiest u **Start > Alle programma's > Windows Update** om uw systeem bij te werken.



Stap 2. De Windows Firewall moet zijn ingeschakeld. Om dit te controleren, kiest u **Start > Configuratiescherm > Systeem en beveiliging > Windows Firewall**.

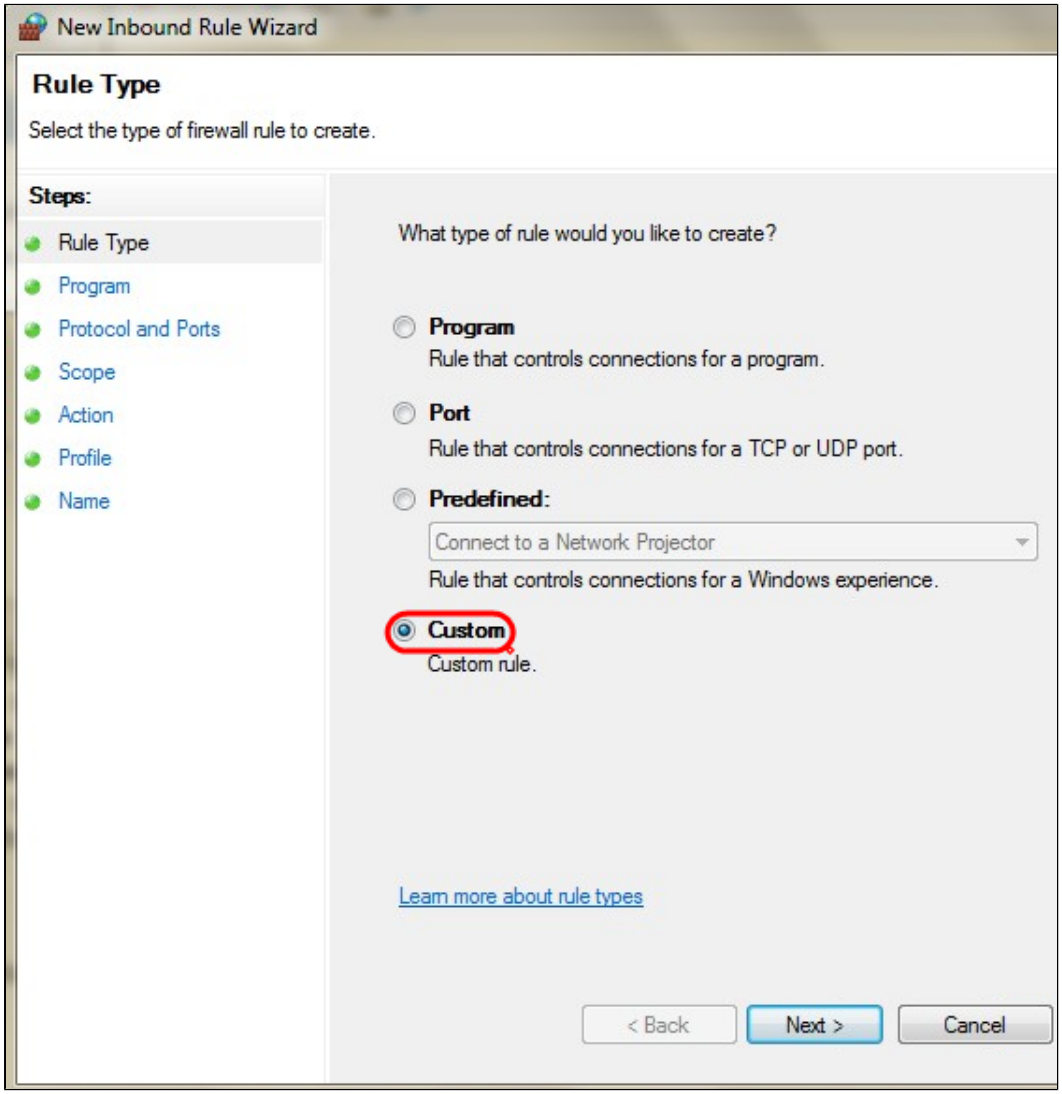


Stap 3. Er moet een regel worden gemaakt om ICMP-pakkettransmissies (Internet Control Message Protocol) toe te staan. Kies hiervoor **Start > Configuratiescherm > Systeem en beveiliging > Windows Firewall > Geavanceerde instellingen**. Het venster *Windows Firewall met geavanceerde beveiliging* wordt geopend:

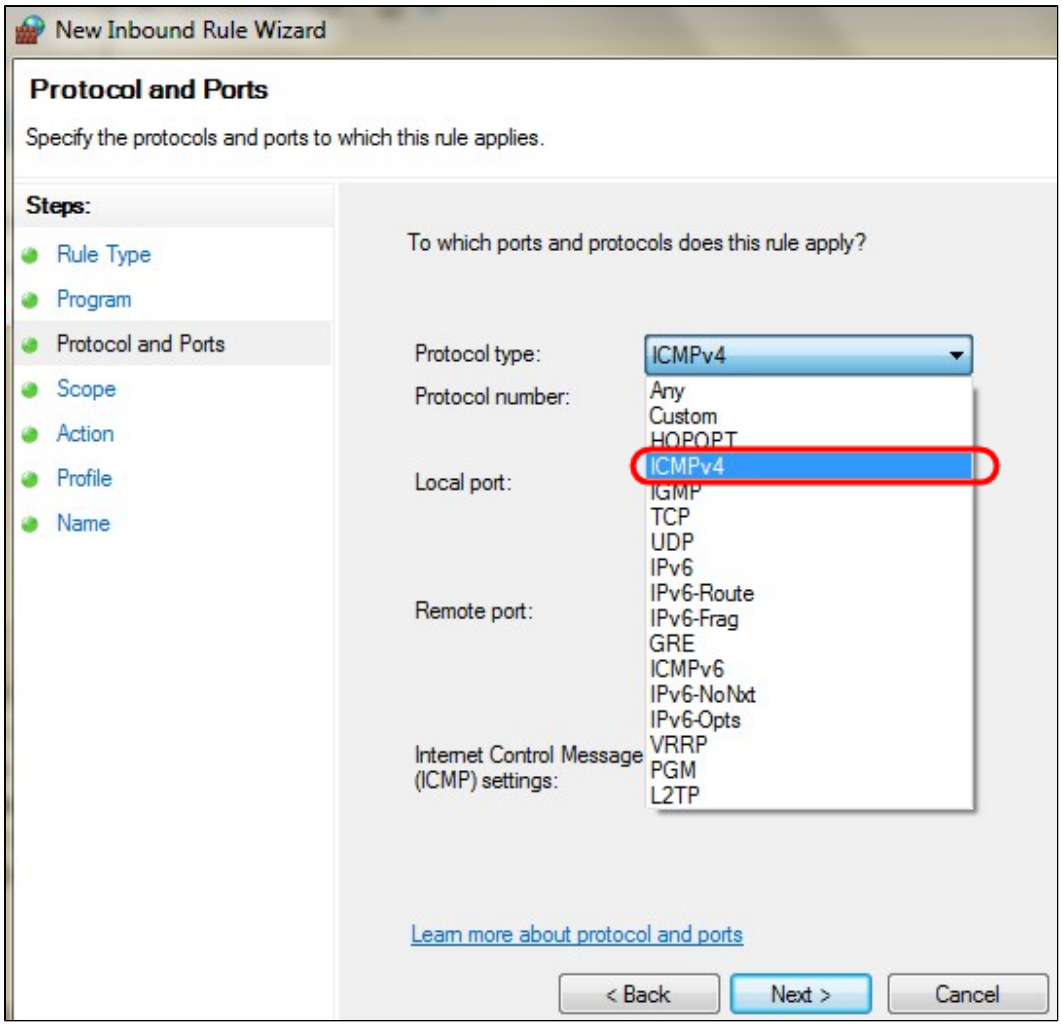


Stap 4. Klik met de rechtermuisknop op **Inkomende regels** en kies **Nieuwe regel**. De *nieuwe* pagina

van de wizard Inkomende regel wordt geopend:

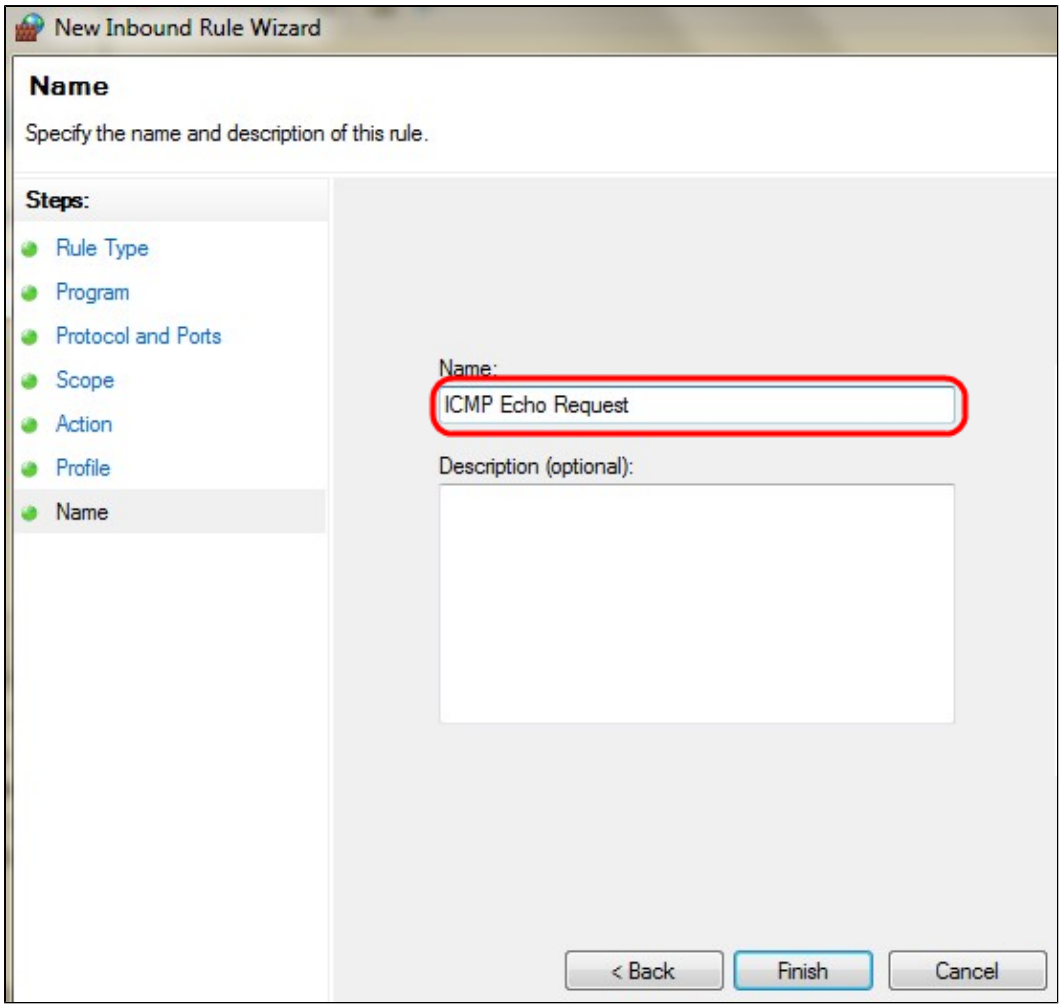


Stap 5. Klik op **Aangepast** om een aangepaste regel te maken.



Stap 6. Kies **ICMPv4 in** de vervolgkeuzelijst Protocoltype.

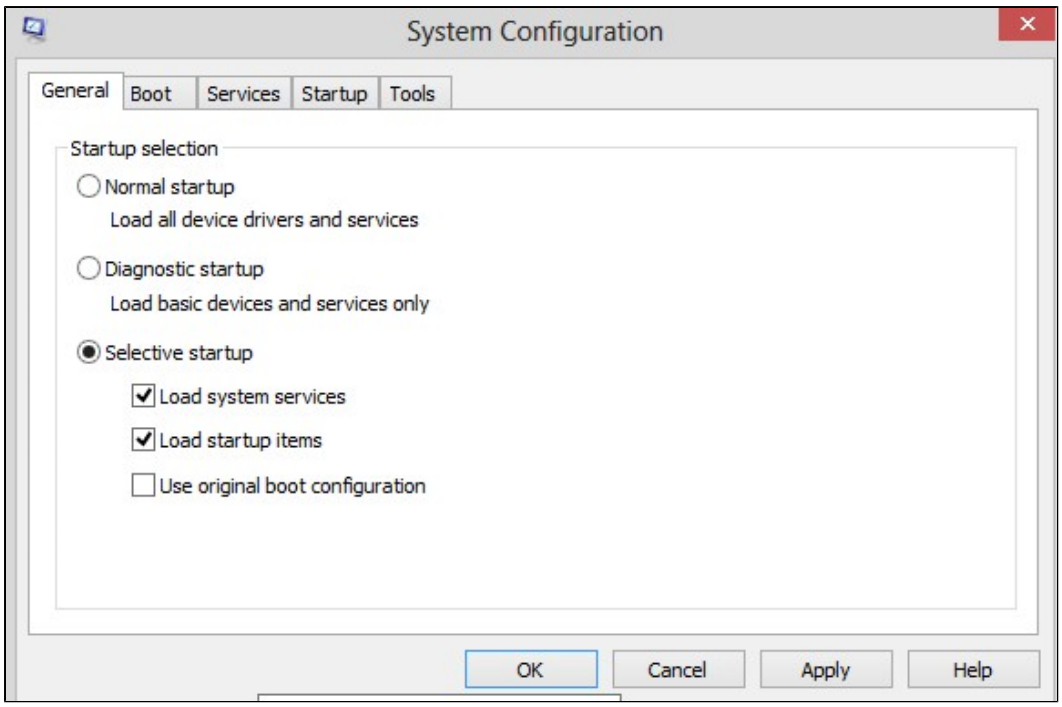
Opmerking: de andere velden kunnen als standaardconfiguratie blijven.



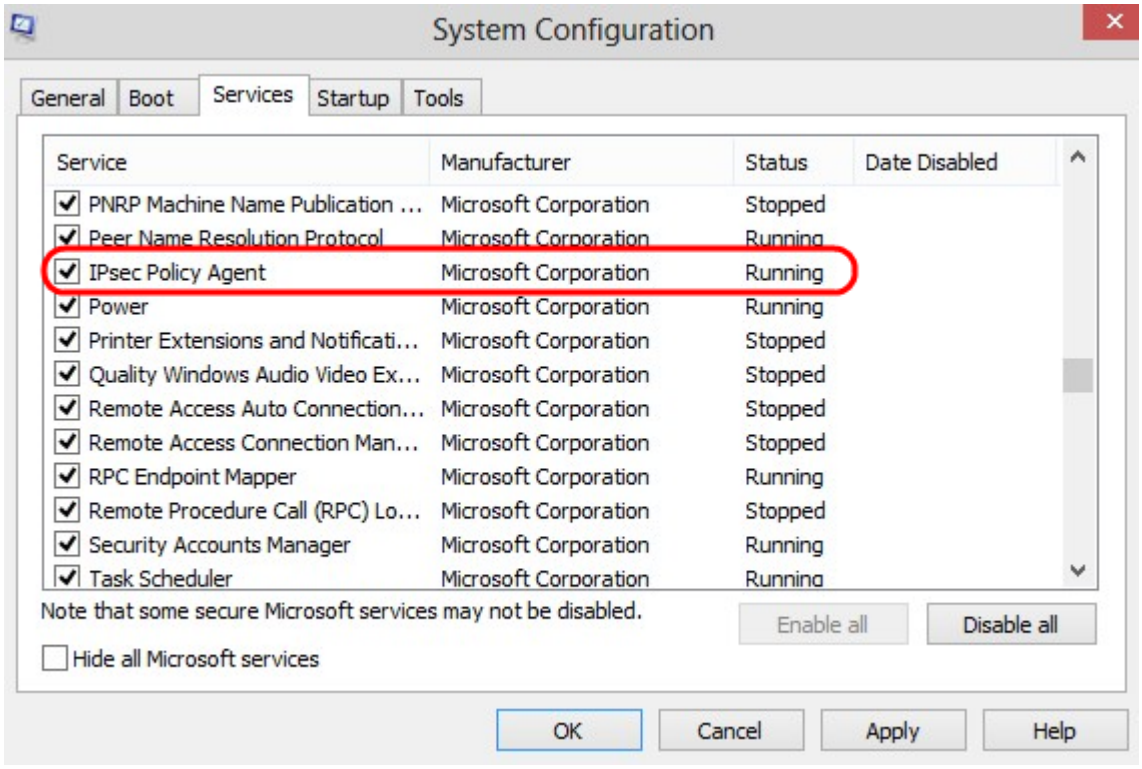
Stap 7. Typ in het veld Naam een naam die deze regel beschrijft.

Stap 8. Klik op **Finish** (Voltooien).

Stap 9. U moet IPSec-service actief hebben. Om dit te controleren, klik op **Start** en voer in het veld Zoekprogramma's en bestanden **msconfig** in. Het venster *Systeemconfiguratie* wordt geopend:



Stap 10. Klik op **het** tabblad **Services** om er zeker van te zijn dat de IPSec Policy Agent is ingeschakeld. Als deze niet is ingeschakeld, schakelt u het aankruisvakje **IPSec Policy Agent in** om IPSec-service toe te staan.



Stap 11. Klik op **Toepassen** om de instellingen op te slaan.

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.