De Cisco VPN 3000 Concentrator en de PGP-client voor Network Associates configureren

Inhoud

Inleiding

Dit document beschrijft hoe u zowel de Cisco VPN 3000 Concentrator als de Network Associates Best Good Privacy (PGP) Client moet configureren en versie 6.5.1 kunt gebruiken om verbindingen van elkaar te accepteren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VPN 3000 Concentrator versie 4.7
- Networks Associated PGP-clientversie 6.5.1

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

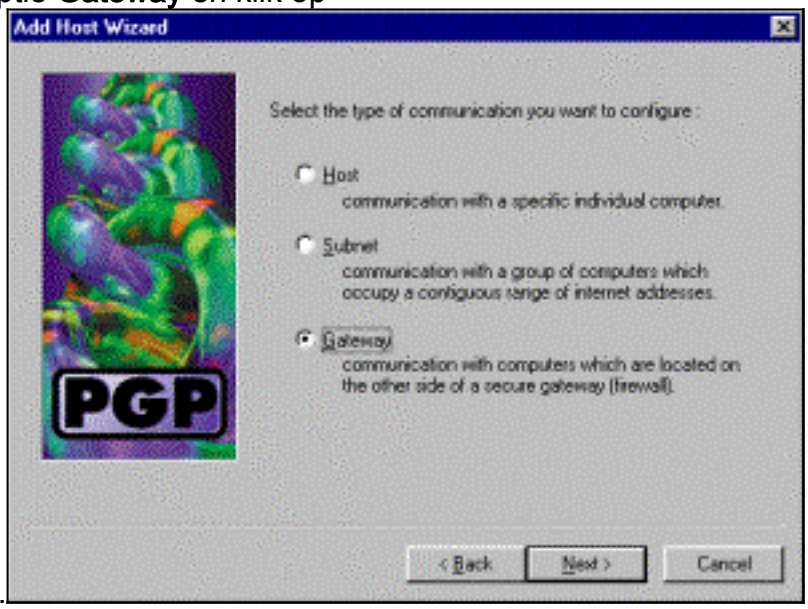
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor

meer informatie over documentconventies.

Configureer de PGP-client voor Network Associates om deze aan te sluiten op Cisco VPN 3000 Concentrator

Gebruik deze procedure om de PGP-client voor Network Associates te configureren voor aansluiting op de VPN 3000 Concentrator.

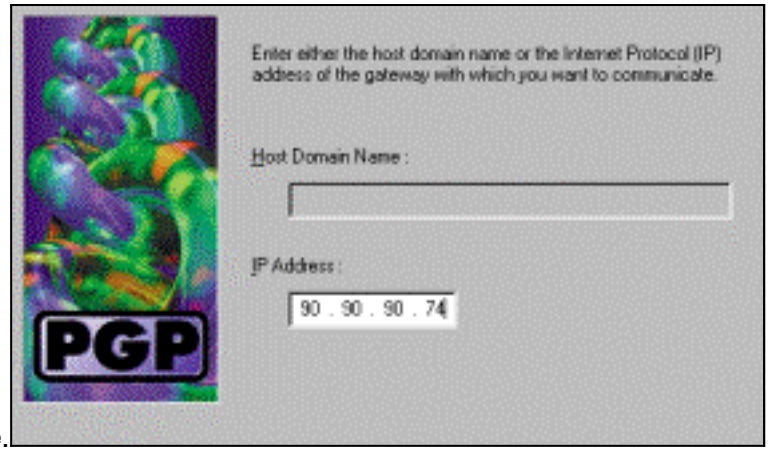
1. Start **PGPet > hosts**.
2. Klik op **Toevoegen** en vervolgens op **Volgende**.
3. Kies de optie **Gateway** en klik op **Volgende**.



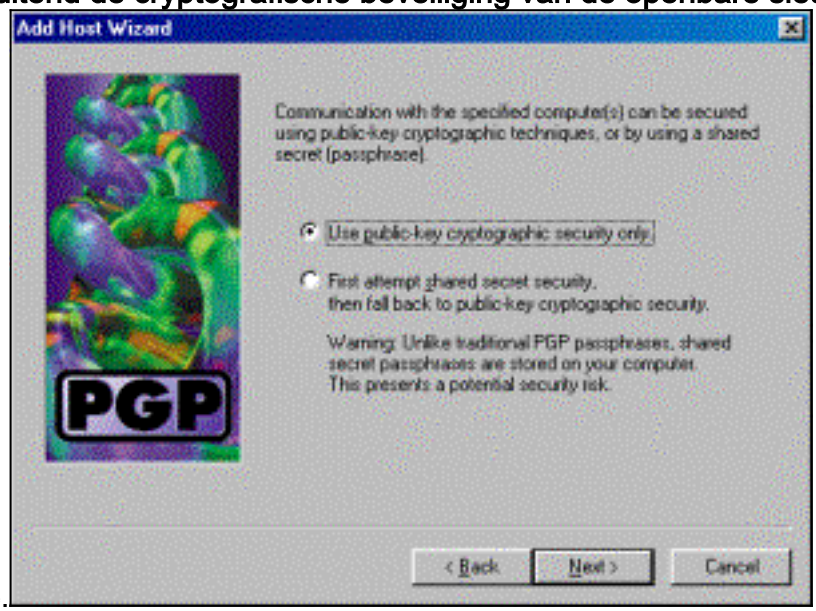
4. Typ een beschrijvende naam voor de verbinding en klik op **Volgende**.

5. Voer de host-domeinnaam of het IP-adres van de openbare interface van VPN 3000

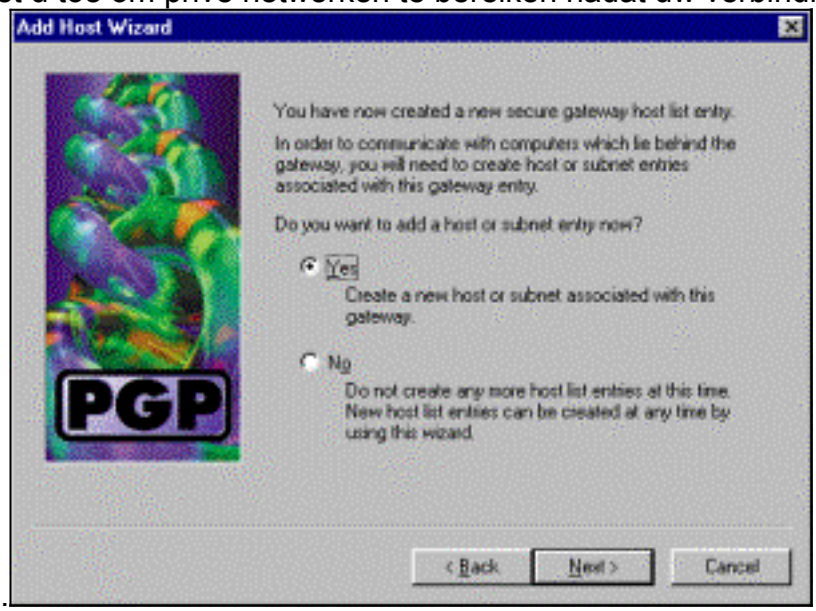
Concentrator in en klik op **Volgende**.



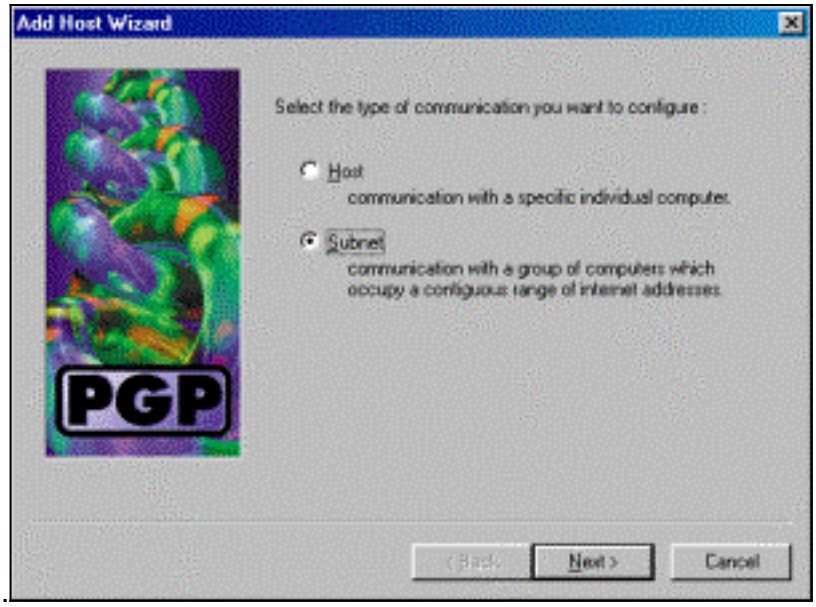
6. Kies **uitsluitend de cryptografische beveiliging van de openbare sleutel gebruiken** en klik op **Volgende**.



7. Selecteer **Ja** en klik op **Volgende**. Wanneer u een nieuwe host of SUBNET toevoegt, staat het u toe om privé netwerken te bereiken nadat uw verbinding veilig is.

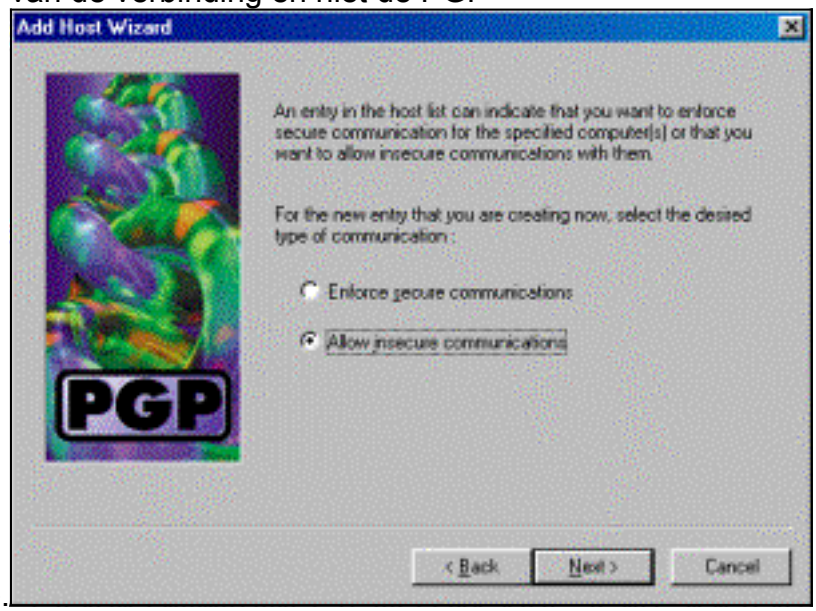


8. Selecteer **Subnet** en klik op



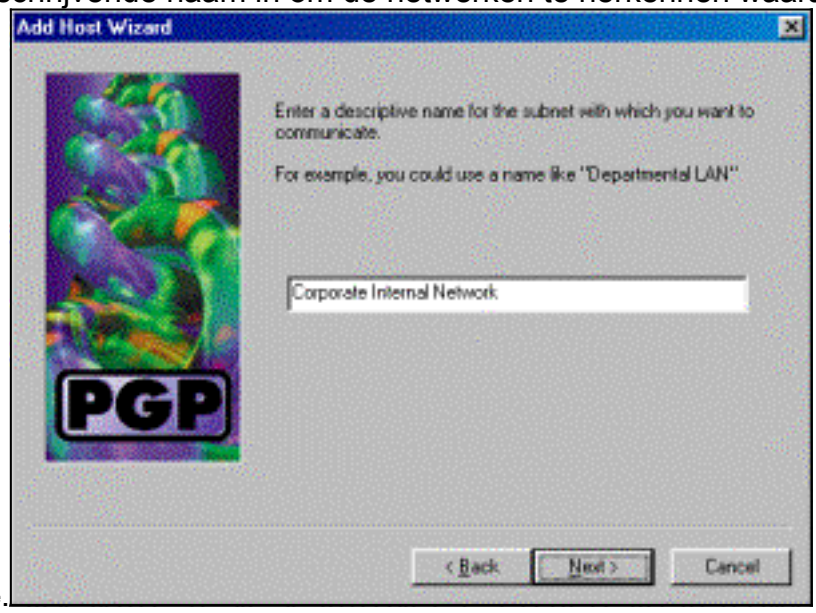
Volgende.

9. Kies **Onveilige communicatie toestaan** en klik op **Volgende**.VPN 3000 Concentrator verwerkt de beveiliging van de verbinding en niet de PGP-



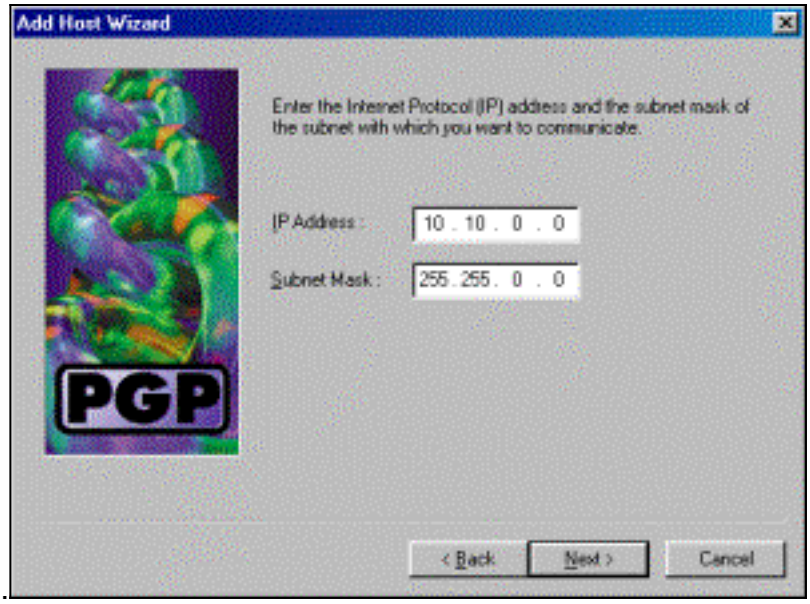
clientsoftware.

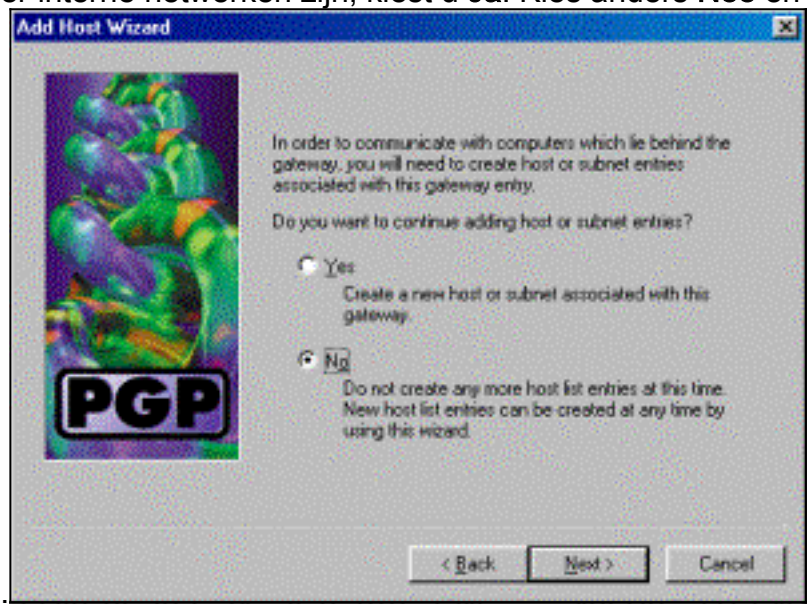
10. Voer een beschrijvende naam in om de netwerken te herkennen waaraan u koppelt en klik



op **Volgende**.

11. Voer het netwerknummer en het subnetmasker voor het netwerk achter de VPN 3000 Concentrator in en klik op

Volgende. 

12. Als er meer interne netwerken zijn, kiest u **Ja**. Kies anders **Nee** en klik op Volgende. 

Configureer de Cisco VPN 3000 Concentrator om verbindingen te aanvaarden van de PGP-client voor Network Associates

Gebruik deze procedure om Cisco VPN 3000 Concentrator te configureren om verbindingen te aanvaarden van een PGP-client voor Network Associates:

1. Selecteer **Configuration > Tunneling en Security > IPSec > IKE-voorstellen**.
2. Activeer het **IKE-3DES-SHA-DSA**-voorstel door het in de kolom Inactieve voorstellen te selecteren. Klik vervolgens op de knop **Activeren** en vervolgens op de knop **Opslaan nodig**.
3. Selecteer **Configuration > Policy Management > Traffic Management > SA's**.
4. Klik op **Add** (Toevoegen).
5. Laat alle behalve deze velden bij hun standaardinstellingen:**Naam SA:** Maak een unieke naam om dit te identificeren.**Digitaal certificaat:** Kies het geïnstalleerde server identificatiecertificaat.**IKE-voorstel:** Selecteer **IKE-3DES-SHA-DSA**.
6. Klik op **Add** (Toevoegen).
7. Selecteer **Configuration > User Management > Groepen**, klik op **Add Group** en stel deze velden in:**N.B.:** Als al uw gebruikers PGP-clients zijn, kunt u de Base Group (**Configuration >**

User Management > Base Group) gebruiken in plaats van nieuwe groepen te maken. Als dit zo is, sla de stappen voor het tabblad Identity over en voltooi stap 1 en 2 alleen voor het tabblad IPSec.Typ deze informatie onder het tabblad Identity:**Naam groep:** Voer een unieke naam in. (Deze groepsnaam moet gelijk zijn aan het OU-veld in het digitale certificaat van de PGP-client.)**Wachtwoord:** Voer het wachtwoord in voor de groep.Voer onder het tabblad IPSec deze informatie in:**Verificatie:** Stel dit in op **niemand**.**Configuratie modus:** Schakel deze optie uit.

8. Klik op **Add** (Toevoegen).
9. Bespaar waar nodig door.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- IPsec-ondersteuningspagina
- VPN-softwaredownloads (alleen geregistreerde klanten)
- Technische ondersteuning - Cisco-systemen