## De Cisco VPN 3000 Concentrator en de PGPclient voor Network Associates configureren

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureer de PGP-client voor Network Associates om deze aan te sluiten op Cisco VPN 3000 Concentrator Configureer de Cisco VPN 3000 Concentrator om verbindingen te aanvaarden van de PGP-client voor Network Associates Gerelateerde informatie

## **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.

## <u>Voorwaarden</u>

#### **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

# 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



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

Self The self of the	
532	Enter a descriptive name for the gateway with which you want to communicate.
	As examples, you could use the host domain name of the gateway (e.g. "gateway1 company.com") or something more descriptive (e.g. "Departmental firewall").
12	Corporate VPN
DGD	

Volgende.

Volgende

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

	Enter either the host domain name or the Internet Protocol (IP) address of the gateway with which you want to communicate.
PGP	Hox Domain Name : P Address : 90 . 90 . 90 . 74

Concentrator in en klik op Volgende.

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

dd Host Wizard	×
	Communication with the specified computer(s) can be secured using public-key cryptographic techniques, or by using a shared secret (passphrate).
	Use public-key cyptographic security only.     First attempt shared secret security.
	then fall back to public-key cryptographic security. Warning: Unlike traditional PGP parsphrases, shared secret passphrases are stored on your computer.
PGP	This presents a potential security tisk.
	< <u>B</u> ack. <u>N</u> ext> Cancel

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

Add Host Wizard		
	You have now created a new secure gateway host list entry.	
253	In order to communicate with computers which lie behind the gateway, you will need to create host or subnet entries associated with this gateway entry.	
	Do you want to add a host or subnet entry now?	
PGP	<ul> <li>Yes</li> <li>Create a new host or subnet associated with this gateway.</li> <li>Ng</li> <li>Do not create any more host list entries at this time. New host list entries can be created at any time by using this wizard.</li> </ul>	
	< <u>B</u> ack <u>N</u> ext> Cancel	

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-

Add Host Wizard	×
	An entry in the host list can indicate that you want to enforce secure communication for the specified computer(s) or that you want to allow insecure communications with them.
	For the new entry that you are creating now, select the desired type of communication :
	C Enforce geoure communications
	Alow insecure communications
PGP	
clientsoftware.	< <u>B</u> ack <u>N</u> ext> Cancel

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

d Host Wizard	
	Enter a descriptive name for the subnet with which you want to communicate. For example, you could use a name like "Departmental LAN"
	Corporate Internal Network
PGP	
	< Back Next> Cancel

op Volgende.

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

Add Host Wizard			×
	Enter the Internet the subnet with w	Protocol (IP) address and the subnet mask of high you want to communicate.	an a
Car.	[P Address :	10.10.0.0	
	≦ubnet Mask :	255.255.0.0	New York
PGP			14
		(Back Next) Cancel	

#### Volgende.

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



### 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)
- <u>Technische ondersteuning Cisco-systemen</u>