

Konfigurieren des Cisco VPN 300 Concentrator und des Network Associates PGP Client

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren Sie den Network Associates PGP Client für die Verbindung mit dem Cisco VPN 3000 Concentrator.](#)

[Konfigurieren des Cisco VPN 3000 Concentrator zum Akzeptieren von Verbindungen vom PGP-Client der Netzwerkverknüpfungen](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird beschrieben, wie sowohl der Cisco VPN 3000 Concentrator als auch der Network Associates Pretty Good Privacy (PGP) Client mit Version 6.5.1 konfiguriert werden, um Verbindungen miteinander zu akzeptieren.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN 3000 Concentrator Version 4.7
- Networks Associates PGP Client Version 6.5.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

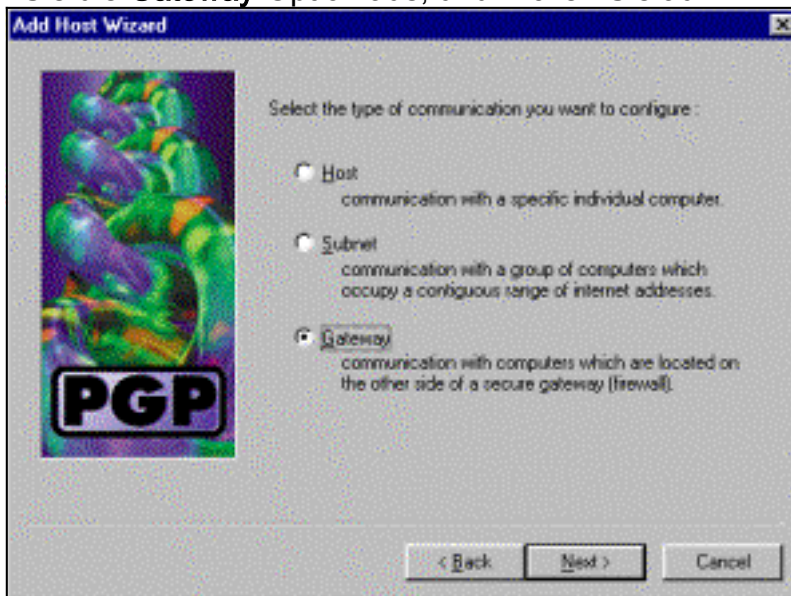
[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

Konfigurieren Sie den Network Associates PGP Client für die Verbindung mit dem Cisco VPN 3000 Concentrator.

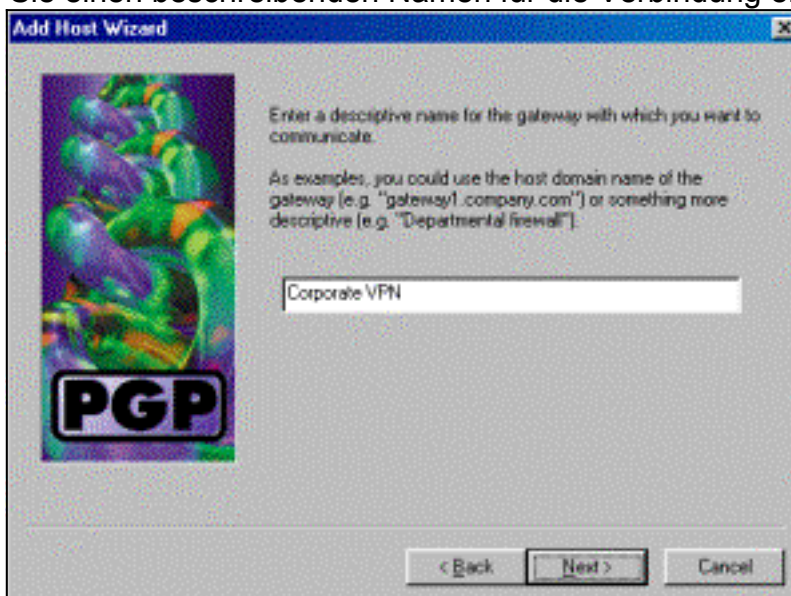
Mit diesem Verfahren konfigurieren Sie den Network Associates PGP Client für die Verbindung mit dem VPN 3000 Concentrator.

1. Starten Sie **PGPNet > Hosts**.
2. Klicken Sie auf **Hinzufügen** und dann auf **Weiter**.
3. Wählen Sie die **Gateway**-Option aus, und klicken Sie auf




Weiter.

4. Geben Sie einen beschreibenden Namen für die Verbindung ein, und klicken Sie auf



Weiter.

5. Geben Sie den Hostdomännennamen oder die IP-Adresse der öffentlichen Schnittstelle des VPN 3000 Concentrator ein, und klicken Sie auf



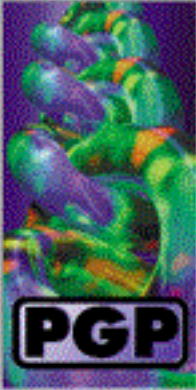
Enter either the host domain name or the Internet Protocol (IP) address of the gateway with which you want to communicate.

Host Domain Name :

IP Address :

Weiter.

6. Wählen Sie **Nur öffentliche kryptografische Sicherheit verwenden** aus, und klicken Sie auf



Communication with the specified computer(s) can be secured using public-key cryptographic techniques, or by using a shared secret (passphrase).

Use public-key cryptographic security only.


First attempt shared secret security, then fall back to public-key cryptographic security.

Warning: Unlike traditional PGP passphrases, shared secret passphrases are stored on your computer. This presents a potential security risk.

< Back Next > Cancel

Weiter.

7. Wählen Sie **Ja**, und klicken Sie auf **Weiter**. Wenn Sie einen neuen Host oder ein neues Subnetz hinzufügen, können Sie nach dem Sichern der Verbindung private Netzwerke



You have now created a new secure gateway host list entry. 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?

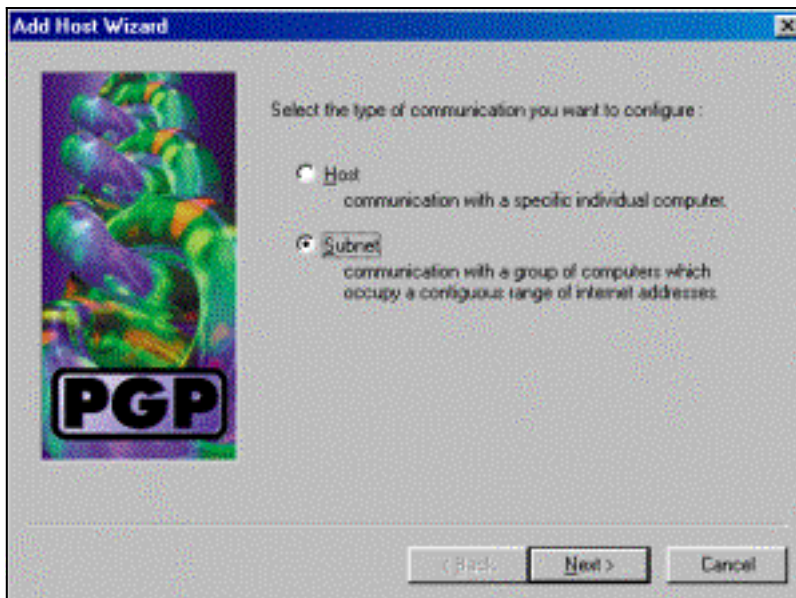
Yes
 Create a new host or subnet associated with this gateway.

No
 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.

< Back Next > Cancel

erreichen.

8. Wählen Sie **Subnet** aus, und klicken Sie auf



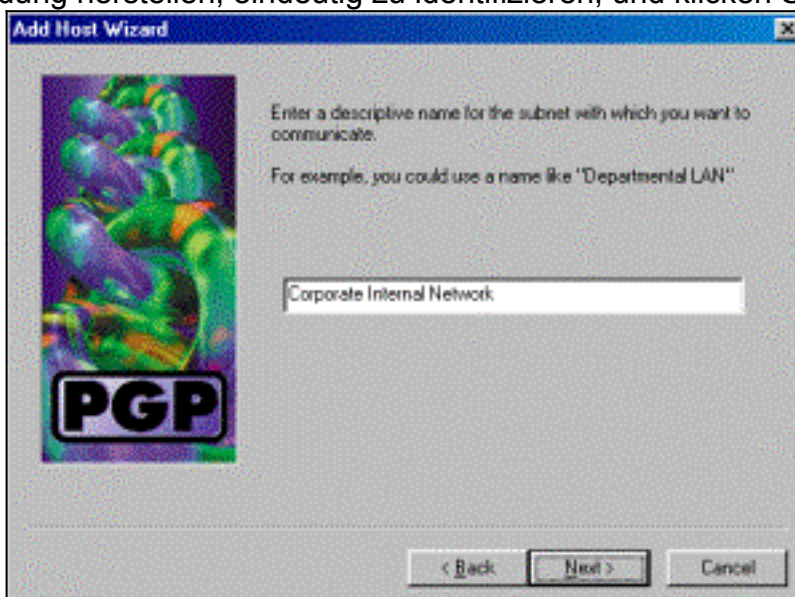
Weiter.

9. Wählen Sie **Unsichere Kommunikation zulassen aus**, und klicken Sie auf **Weiter**. Der VPN 3000 Concentrator übernimmt die Sicherheit der Verbindung, nicht die PGP-Client-



Software.

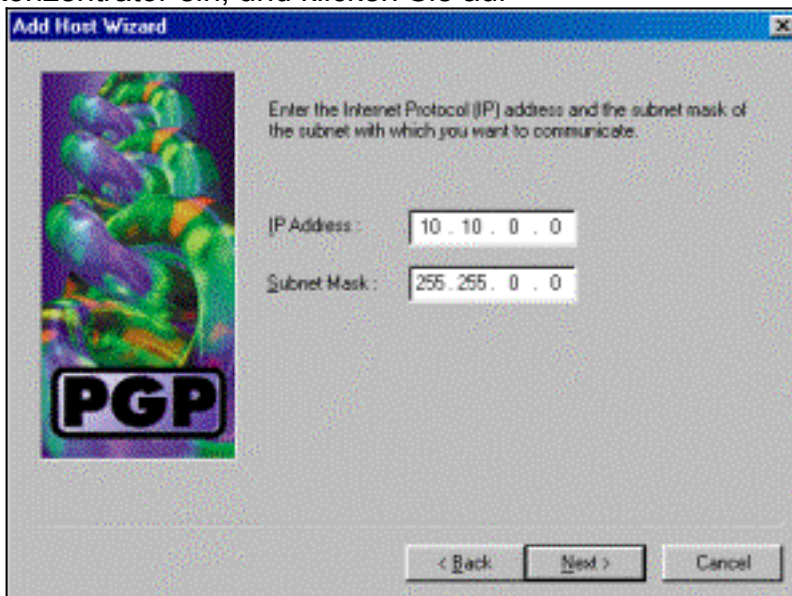
10. Geben Sie einen beschreibenden Namen ein, um die Netzwerke, mit denen Sie eine Verbindung herstellen, eindeutig zu identifizieren, und klicken Sie auf



Weiter.

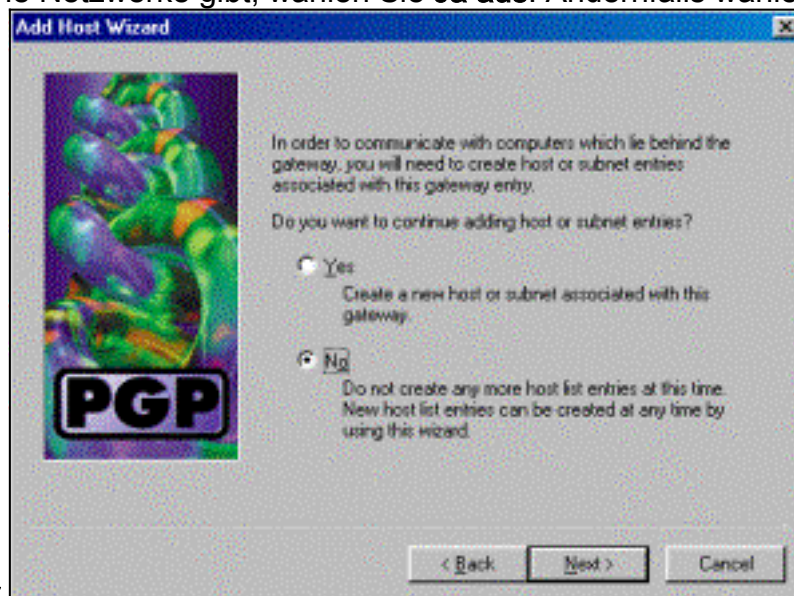
11. Geben Sie die Netzwerknummer und die Subnetzmaske für das Netzwerk hinter dem VPN

3000-Konzentrator ein, und klicken Sie auf



Weiter.

12. Wenn es weitere interne Netzwerke gibt, wählen Sie **Ja aus**. Andernfalls wählen Sie **Nein**



und klicken auf **Weiter**.

[Konfigurieren des Cisco VPN 3000 Concentrator zum Akzeptieren von Verbindungen vom PGP-Client der Netzwerkverknüpfungen](#)

Mit diesem Verfahren können Sie den Cisco VPN 300 Concentrator so konfigurieren, dass er Verbindungen von einem Network Associates PGP Client akzeptiert:

1. Wählen Sie **Konfiguration > Tunneling und Sicherheit > IPSec > IKE-Angebote** aus.
2. Aktivieren Sie das **IKE-3DES-SHA-DSA-Angebot**, indem Sie es in der Spalte **Inaktive Vorschläge** auswählen. Klicken Sie anschließend auf die Schaltfläche **Aktivieren** und anschließend auf die Schaltfläche **Erforderlich speichern**.
3. Wählen Sie **Configuration > Policy Management > Traffic Management > SAs** aus.
4. Klicken Sie auf **Hinzufügen**.
5. Lassen Sie alle Felder bis auf die Standardeinstellungen unverändert: **SA-Name**: Erstellen Sie einen eindeutigen Namen, um dies zu identifizieren. **Digitales Zertifikat**: Wählen Sie das

- installierte Serverkennungszertifikat aus. **IKE-Angebot:** Wählen Sie **IKE-3DES-SHA-DSA** aus.
6. Klicken Sie auf **Hinzufügen**.
 7. Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen** aus, klicken Sie auf **Gruppe hinzufügen**, und konfigurieren Sie diese Felder: **Hinweis:** Wenn alle Ihre Benutzer PGP-Clients sind, können Sie die Basisgruppe (**Konfiguration > Benutzerverwaltung > Basisgruppe**) verwenden, anstatt neue Gruppen zu erstellen. Wenn dies der Fall ist, überspringen Sie die Schritte für die Registerkarte "Identität", und führen Sie die Schritte 1 und 2 nur für die Registerkarte "IPSec" aus. Geben Sie auf der Registerkarte Identität die folgenden Informationen ein: **Gruppenname:** Geben Sie einen eindeutigen Namen ein. (Dieser Gruppenname muss mit dem OU-Feld im digitalen Zertifikat des PGP-Clients übereinstimmen.) **Kennwort:** Geben Sie das Kennwort für die Gruppe ein. Geben Sie auf der Registerkarte IPSec die folgenden Informationen ein: **Authentifizierung:** Legen Sie **None** fest. **Moduskonfiguration:** Deaktivieren Sie diese Option.
 8. Klicken Sie auf **Hinzufügen**.
 9. Speichern Sie alles nach Bedarf.

[Zugehörige Informationen](#)

- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [IPSec-Support-Seite](#)
- [VPN-Software-Download](#) (nur registrierte Kunden)
- [Technischer Support - Cisco Systems](#)