

Configurazione di Cisco VPN 3000 Concentrator e Network Associates PGP Client

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurare il client PGP Network Associates per la connessione al concentratore Cisco VPN 3000](#)

[Configurare Cisco VPN 3000 Concentrator in modo che accetti le connessioni da Network Associates PGP Client](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare Cisco VPN 3000 Concentrator e Network Associates Pretty Good Privacy (PGP) Client con versione 6.5.1 in modo da accettare connessioni tra loro.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

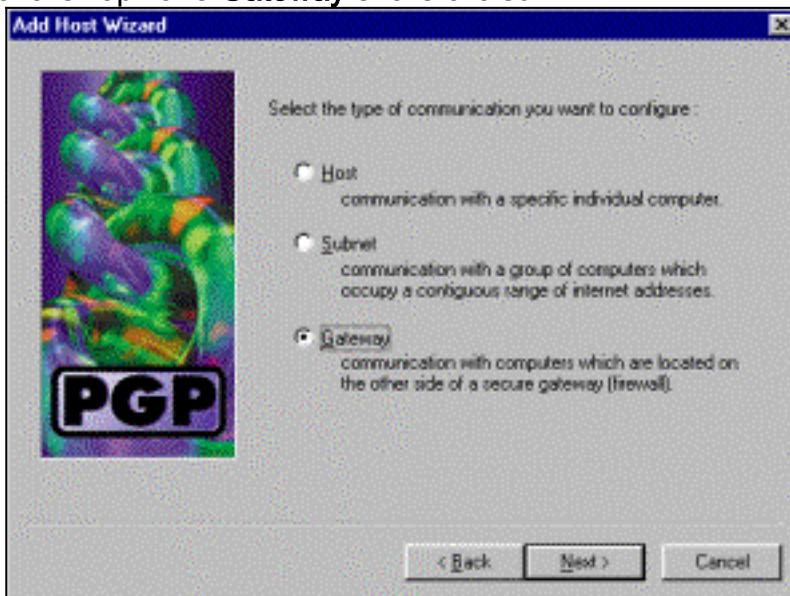
[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

[Configurare il client PGP Network Associates per la connessione al concentratore Cisco VPN 3000](#)

Utilizzare questa procedura per configurare il client PGP Network Associates per la connessione al concentratore VPN 3000.

1. Avviare **PGPNet > Host**.
2. Fare clic su **Add** (Aggiungi), quindi su **Next** (Avanti).
3. Selezionare l'opzione **Gateway** e fare clic su



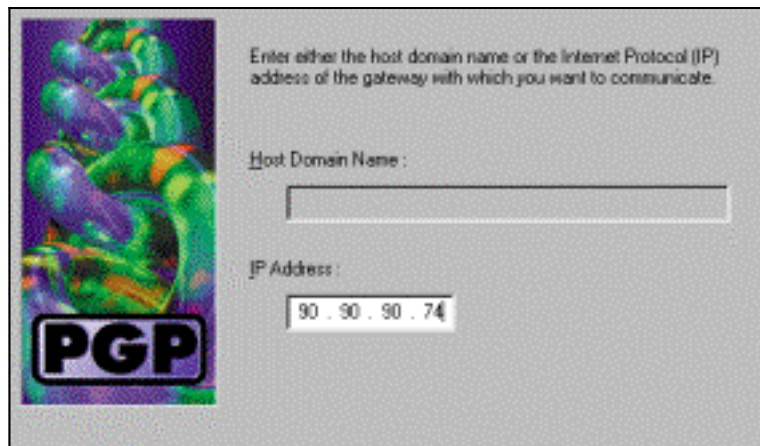
Avanti.

4. Immettere un nome descrittivo per la connessione e fare clic su



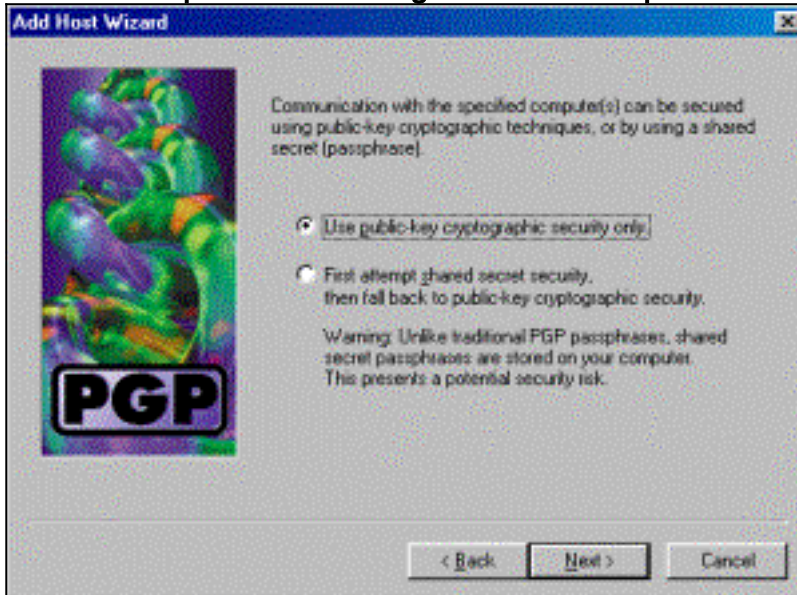
Avanti.

5. Immettere il nome di dominio host o l'indirizzo IP dell'interfaccia pubblica di VPN 3000



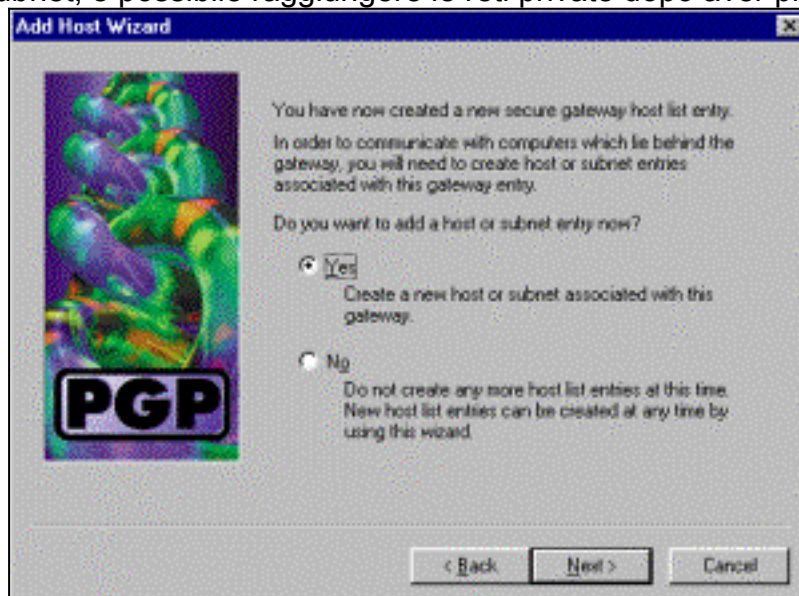
Concentrator e fare clic su **Avanti**.

6. Scegliere **Usa solo protezione crittografica a chiave pubblica** e fare clic su



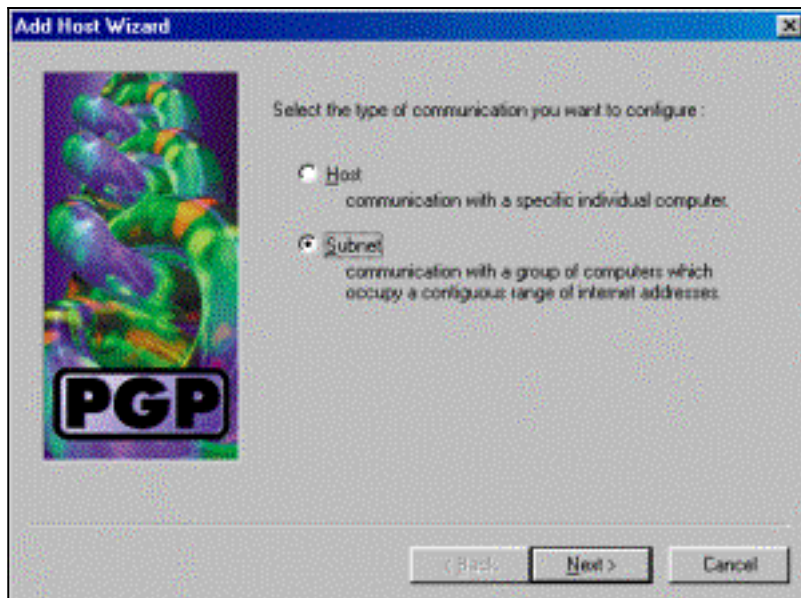
Avanti.

7. Selezionare **Yes (Sì)**, quindi fare clic su **Next (Avanti)**. Quando si aggiunge un nuovo host o una nuova subnet, è possibile raggiungere le reti private dopo aver protetto la



connessione.

8. Selezionare **Subnet**, quindi fare clic su



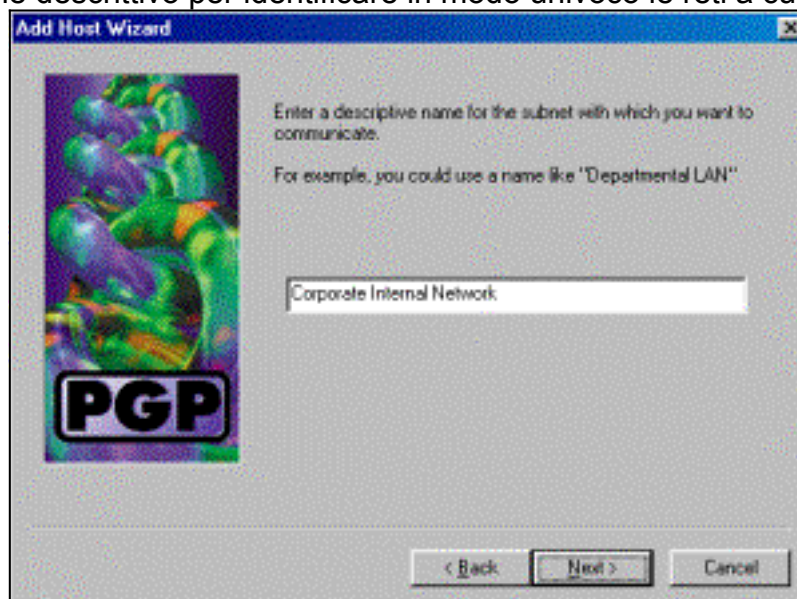
Avanti.

9. Scegliere **Consenti comunicazioni non sicure** e fare clic su **Avanti**. VPN 3000 Concentrator gestisce la sicurezza della connessione, non il software client



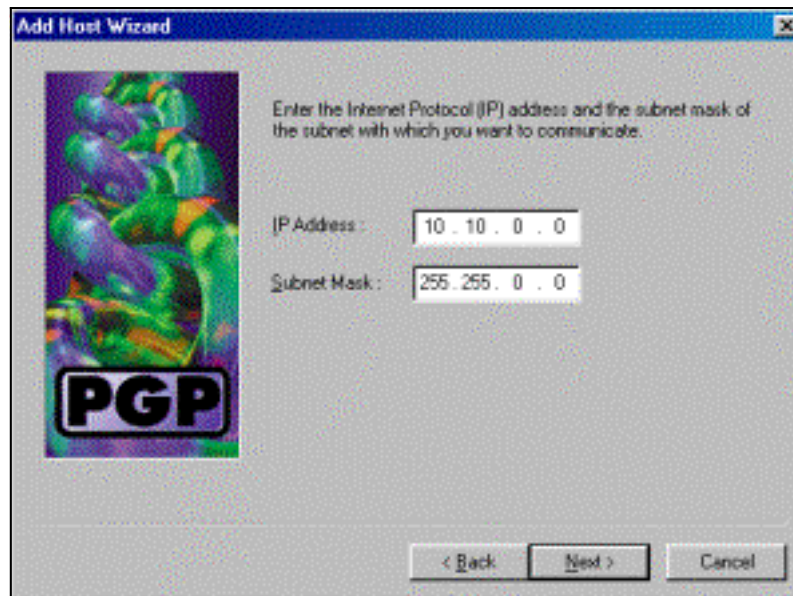
PGP.

10. Immettere un nome descrittivo per identificare in modo univoco le reti a cui ci si connette e



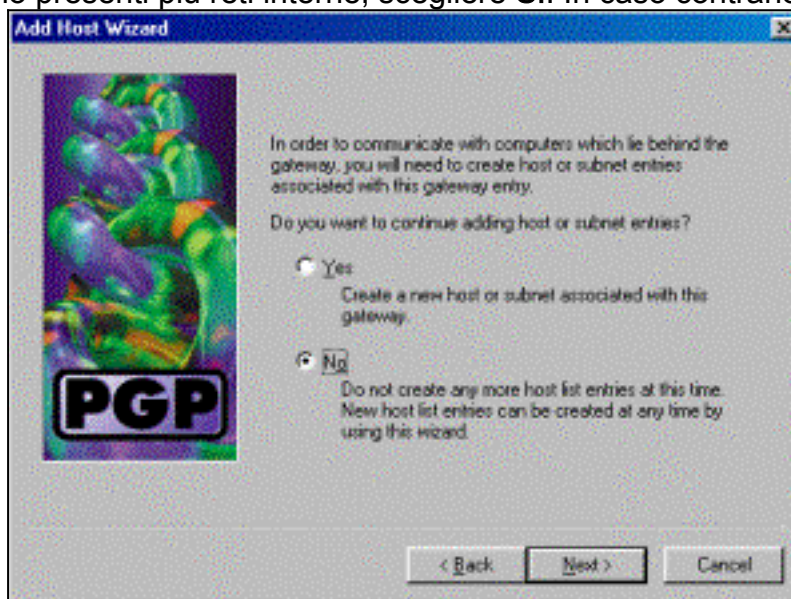
fare clic su **Avanti**.

11. Immettere il numero di rete e la subnet mask per la rete dietro a VPN 3000 Concentrator e



fare clic su **Avanti**.

12. Se sono presenti più reti interne, scegliere **Sì**. In caso contrario, scegliere **No** e fare clic su



Avanti.

[Configurare Cisco VPN 3000 Concentrator in modo che accetti le connessioni da Network Associates PGP Client](#)

Utilizzare questa procedura per configurare Cisco VPN 3000 Concentrator in modo che accetti connessioni da un client PGP Network Associates:

1. Selezionare **Configurazione > Tunneling e sicurezza > IPSec > Proposte IKE**.
2. Attivare la proposta **IKE-3DES-SHA-DSA** selezionandola nella colonna **Proposte inattive**. Quindi, fare clic sul pulsante **Attiva** e fare clic sul pulsante **Salva** necessario.
3. Selezionare **Configurazione > Gestione delle policy > Gestione del traffico > SA**.
4. Fare clic su **Add**.
5. Mantenere le impostazioni predefinite di tutti i campi tranne questi:**Nome SA**: Creare un nome univoco per identificarlo.**Certificato digitale**: Scegliere il certificato di identificazione del server installato.**Proposta IKE**: Selezionare **IKE-3DES-SHA-DSA**.
6. Fare clic su **Add**.
7. Selezionare **Configurazione > Gestione utente > Gruppi**, fare clic su **Aggiungi gruppo** e configurare i seguenti campi:**Nota**: se tutti gli utenti sono client PGP, è possibile utilizzare il

gruppo base (**Configurazione > Gestione utenti > Gruppo base**) anziché creare nuovi gruppi. In tal caso, ignorare i passaggi per la scheda Identità e completare i passaggi 1 e 2 solo per la scheda IPsec. Nella scheda Identità immettere le informazioni seguenti:**Nome gruppo:** Immettere un nome univoco. Il nome del gruppo deve essere uguale al campo OU nel certificato digitale del client PGP.**Password:** Immettere la password per il gruppo. Nella scheda IPsec immettere le informazioni seguenti:**Autenticazione:** Impostare su **Nessuno**.**Configurazione modalità:** Deselezionare.

8. Fare clic su **Add**.

9. Salvare in base alle esigenze.

[Informazioni correlate](#)

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Pagina di supporto per IPsec](#)
- [Download del software VPN](#) (solo utenti [registrati](#))
- [Supporto tecnico – Cisco Systems](#)