## 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

- Car	Select the type of communication you want to configure :
	<ul> <li>Host communication with a specific individual computer.</li> </ul>
	C Subret
<b>KC3A</b>	communication with a group of computers which occupy a contiguous range of internet addresses.
	(* Gateway)
	communication with computers which are located or the other side of a secure cateway (frewall).
PGP	
1997 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 - 1998 -	

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

		Enter a descriptive communicate. As examples, you o	name for the p ould use the h	pateway with which j	poureant to
	5	Corporate VPN	epartmental fi	enal"].	ig noie
P	GP				
1. 19 19 19 19 19 19 19 19 19 19 19 19 19			< Dash	[ <u></u> ]	Freed

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

	Enter either the host domain name or the Internet Protocol (IP) address of the gateway with which you want to communicate.
Car.	Host Domain Name :
	JP Address : 90 . 30 . 30 . 74
PGP	

Concentrator e fare clic su Avanti.

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

Add Host Wizard		×
	Communication with the specified computer(s) can be secured using public-key cryptographic techniques, or by using a shared secret (passphrase).	
CY AND	Use public-key cyptographic security only.	
AS A	<ul> <li>First attempt ghared secret security, then fall back to public-key cryptographic security.</li> </ul>	- 45
PGP	Warning: Unlike traditional PGP parsphrases, shared secret parsphrases are stored on your computer. This presents a potential security risk.	
	< Back Next > Cancel	

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

Avanti.

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

	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.
CONT A	For the new entry that you are creating now, select the desired type of communication :
Res M	C Enforce geoure communications
	Allow insecure communications
PGP	
	< <u>Back</u> Next> Cance

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

Pedo mose wizaro	
	Enter a descriptive name for the subnet with which you want to communicate. For example, you could use a name like "Departmental LAN"
	< <u>B</u> ack <u>Next&gt;</u> Cancel

fare clic su Avanti.

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

	Add Host Wizard			×
		Enter the Internet Protocol (IP) address and the subnet mask the subnet with which you want to communicate.		
		[P Address :	10.10.0.0	
		<u>S</u> ubnet Mask∶	255.255.0.0	
	PGP			
				1
fare clic su <b>Avanti</b>			< <u>B</u> ack <u>N</u> ext > Cancel	<u> </u>

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

	AND FORE WEEDED	-
Avanti.	< <u>Back Next&gt;</u> Cancel	

# 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

- <u>Cisco VPN serie 3000 Concentrator Support Page</u>
- Pagina di supporto per IPSec
- Download del software VPN (solo utenti registrati)
- <u>Supporto tecnico Cisco Systems</u>