# Configuración del concentrador Cisco VPN 3000 y de la red asociada al cliente PGP

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configure el Network Associates PGP Client para Conectarse al Cisco VPN 3000 Concentrator Configure el Cisco VPN 3000 Concentrator para Aceptar Conexiones del Cliente PGP de Network Associates Información Relacionada

### **Introducción**

Este documento describe cómo configurar tanto el Cisco VPN 3000 Concentrator como el Network Associates Pretty Good Privacy Client (PGP) Client que ejecuta la versión 6.5.1 para aceptar conexiones entre sí.

### **Prerequisites**

#### **Requirements**

No hay requisitos específicos para este documento.

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Concentrador VPN 3000 de Cisco versión 4.7
- Network Associates PGP Client versión 6.5.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### **Convenciones**

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

### Configure el Network Associates PGP Client para Conectarse al Cisco VPN 3000 Concentrator

Utilice este procedimiento para configurar Network Associates PGP Client para conectarse al concentrador VPN 3000.

- 1. Inicie **PGPNet > Hosts**.
- 2. Haga clic en Agregar y después haga clic en Siguiente.
- 3. Elija la opción Gateway y haga clic en



4. Introduzca un nombre descriptivo para la conexión y haga clic en

Add Host Wizard		×
PGP	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. "gateway! company.com") or something more descriptive (e.g. "Departmental firewall").	
	<back next=""> Cancel</back>	4

Siguiente

Next

5. Ingrese el nombre de dominio de host o la dirección IP de la interfaz pública del VPN 3000

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

Concentrator y haga clic en Next

6. Elija Usar seguridad criptográfica de clave pública solamente y haga clic en

Add Host Wizard		×
	Communication with the specified computer(s) can be secured using public-key cryptographic techniques, or by using a shared secret (passphraze).	
Carlos Carlos	Use public-key cryptographic security only.	
AND I	<ul> <li>First attempt ghared secret security, then fall back to public key cryptographic security.</li> </ul>	
PGP	Warning: Unlike traditional PGP passphrases, shared secret passphrases are stored on your computer. This presents a potential security tisk.	
19 19		
4.02	< <u>B</u> ack <u>N</u> ext > Cancel	

Siguiente.

7. Seleccione **Yes** y haga clic en **Next**. Cuando agrega un nuevo host o subred, le permite alcanzar redes privadas después de que la conexión esté

Add Host Wizard		X
PGP	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? Composition of the second state of the subnet entry now? Composition of the second state of the subnet associated with this gateway. Composition of the second state of the second state of the second second state of the second	
protegida.	< <u>B</u> ack <u>N</u> ext> Cancel	

8. Seleccione Subnet y haga clic en



Next

PGP

9. Elija Allow insecure communications y haga clic en Next.El concentrador VPN 3000 maneja la seguridad de la conexión, no el software cliente

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 C Allow insecure communications
PGP	< <u>₽</u> ack <u>N</u> ext > Cancel

10. Introduzca un nombre descriptivo para identificar de forma única las redes a las que se

emple, you could use a name like "Departmental LAN"
orate Internal Network

conecta y haga clic en Siguiente.

11. Ingrese el número de red y la máscara de subred para la red detrás del concentrador VPN

Add Host Wizard		×
PGP	Enter the Internet Piotocol (IP) address and the subnet mask of the subnet with which you want to communicate. IP Address: 10.10.0.0 Subnet Mask: 255.255.0.0	
aller.	<back next=""> Cancel</back>	1

3000 y haga clic en Siguiente.

12. Si hay más redes internas, elija Yes. De lo contrario, elija No y haga clic en

	Add Host Wizard	×
Ciaulianto	Image: Section of the section of th	
Siguiente.		

### Configure el Cisco VPN 3000 Concentrator para Aceptar Conexiones del Cliente PGP de Network Associates

Utilice este procedimiento para configurar el Cisco VPN 3000 Concentrator para aceptar conexiones de un Network Associates PGP Client:

- 1. Seleccione Configuración > Tunelización y Seguridad > IPSec > Propuestas IKE.
- 2. Active la propuesta **IKE-3DES-SHA-DSA** seleccionándola en la columna Propuestas inactivas. A continuación, haga clic en el botón **Activate** y, a continuación, haga clic en el botón **Save Needed**.
- 3. Seleccione Configuration > Policy Management > Traffic Management > SAs.
- 4. Haga clic en Add (Agregar).
- 5. Deje todos excepto estos campos en su configuración predeterminada: Nombre de SA: Cree un nombre único para identificarlo. Certificado digital: Elija el certificado de identificación del servidor instalado. Propuesta IKE: Seleccione IKE-3DES-SHA-DSA.
- 6. Haga clic en Add (Agregar).
- 7. Seleccione Configuration > User Management > Groups, haga clic en Add Group y configure

estos campos:**Nota:** Si todos los usuarios son clientes PGP, puede utilizar el grupo base (**Configuración > Administración de usuarios > Grupo base**) en lugar de crear nuevos grupos. Si es así, omita los pasos de la ficha Identidad y complete los pasos 1 y 2 sólo para la ficha IPSec.En la ficha Identidad, introduzca esta información:**Nombre del grupo:** Introduzca un nombre único. (Este nombre de grupo debe ser igual al campo OU del certificado digital del cliente PGP.)**Contraseña** Introduzca la contraseña del grupo.En la ficha IPSec, introduzca esta información:**Autenticación:** Establezca esto en **Ninguno.Configuración del modo:** Desactive esta opción.

- 8. Haga clic en Add (Agregar).
- 9. Ahorre lo que necesite.

## Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte de IPSec
- Descarga de Software VPN (sólo clientes registrados)
- <u>Soporte Técnico Cisco Systems</u>