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

Contenido

Introducción

Este documento describe cómo configurar el Cisco VPN 3000 Concentrator y a los Network Associate versión client running 6.5.1 del Pretty Good Privacy (PGP) para validar las conexiones de uno a.

prerrequisitos

Requisitos

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.

- Versión 4.7 del Cisco VPN 3000 Concentrator
- Versión 6.5.1 del cliente PGP de los socios de las redes

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

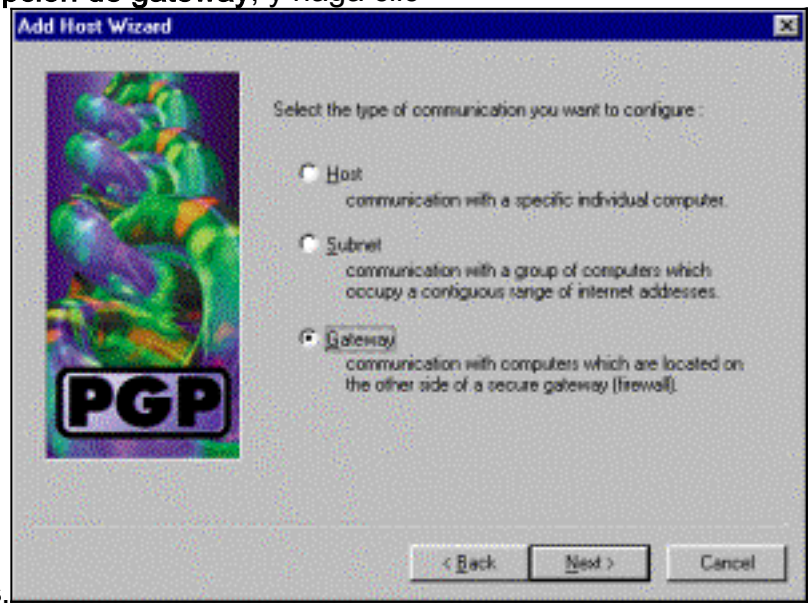
Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

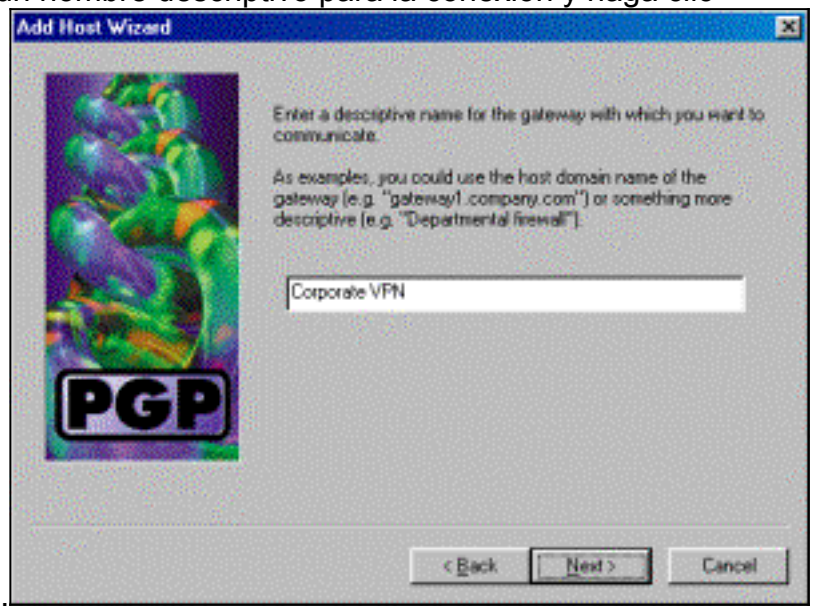
Configure a los Network Associate cliente PGP para conectar con el Cisco VPN 3000 Concentrator

Utilice este procedimiento para configurar a los Network Associate cliente PGP para conectar con el concentrador VPN 3000.

1. Ponga en marcha **PGPNet > los host**.
2. El tecleo **agrega** y después hace clic **después**.
3. Elija la **opción de gateway**, y haga clic **después**.

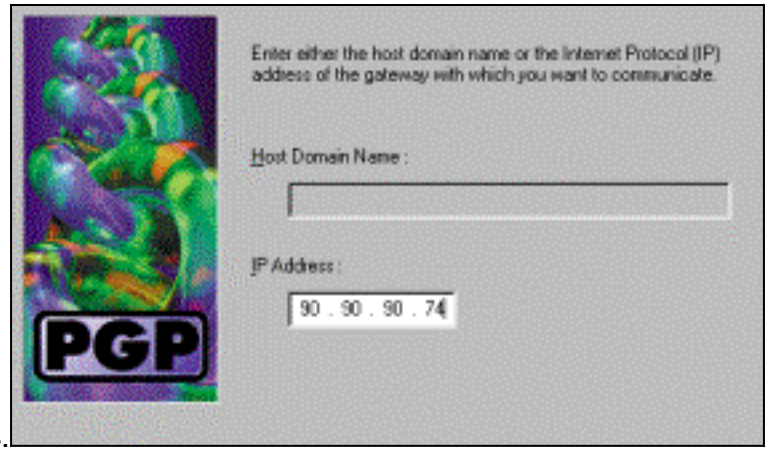


4. Ingrese un nombre descriptivo para la conexión y haga clic **después**.

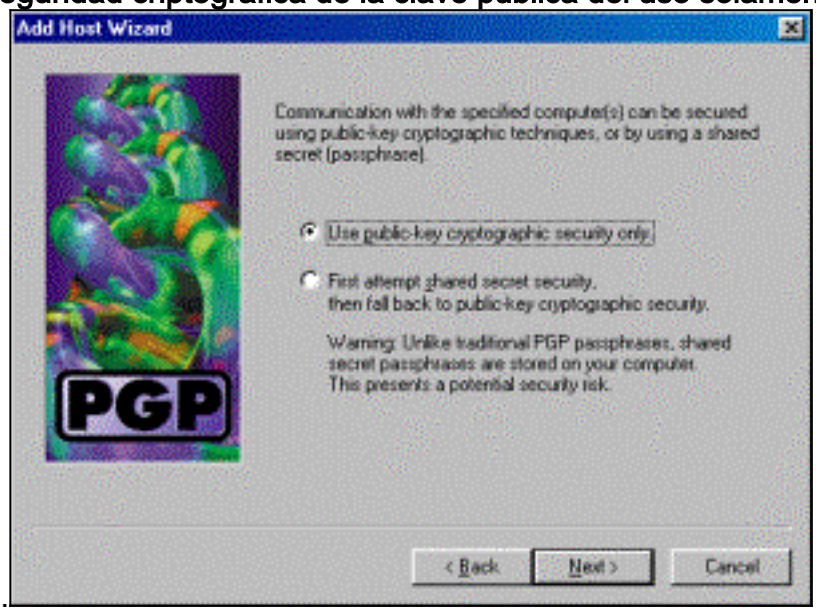


5. Ingrese el Domain Name del host o el IP Address de la interfaz pública del concentrador

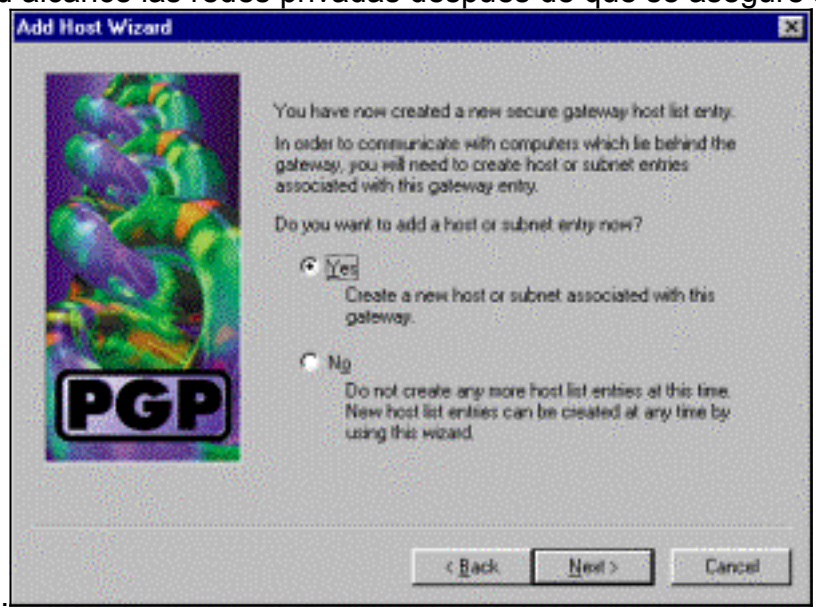
VPN 3000 y haga clic **después**.



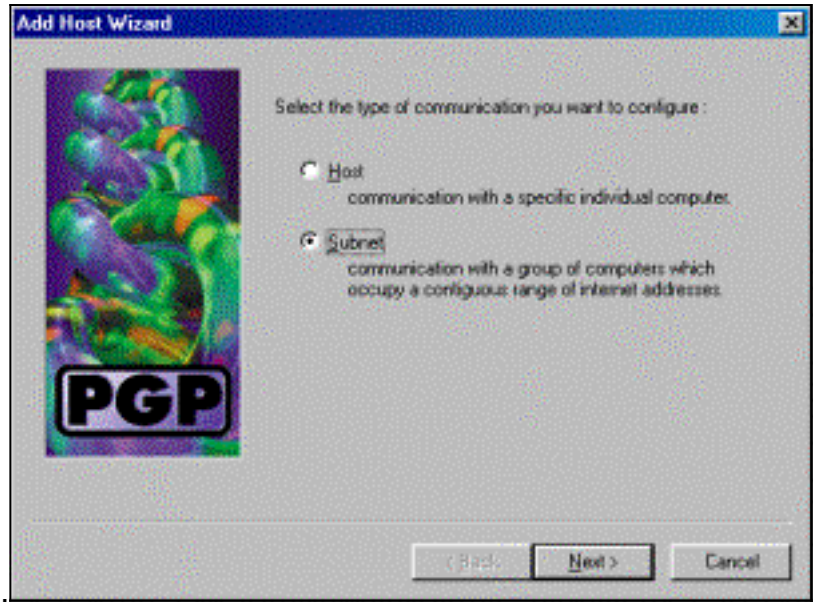
6. Elija la **seguridad criptográfica de la clave pública del uso solamente** y haga clic **después**.



7. Seleccione **sí**, y haga clic **después**. Cuando usted agrega un nuevo host o subred, permite que usted alcance las redes privadas después de que se asegure su conexión.

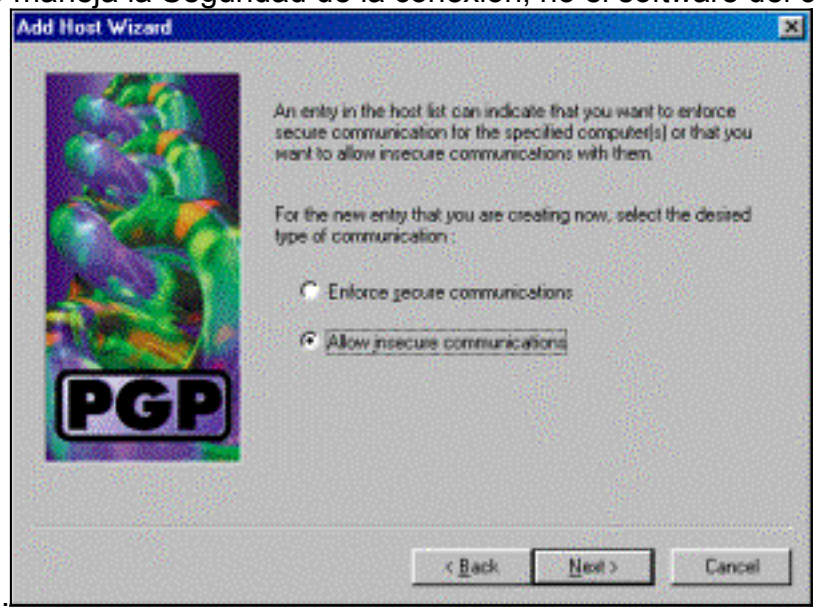


8. Seleccione la **subred** y haga clic



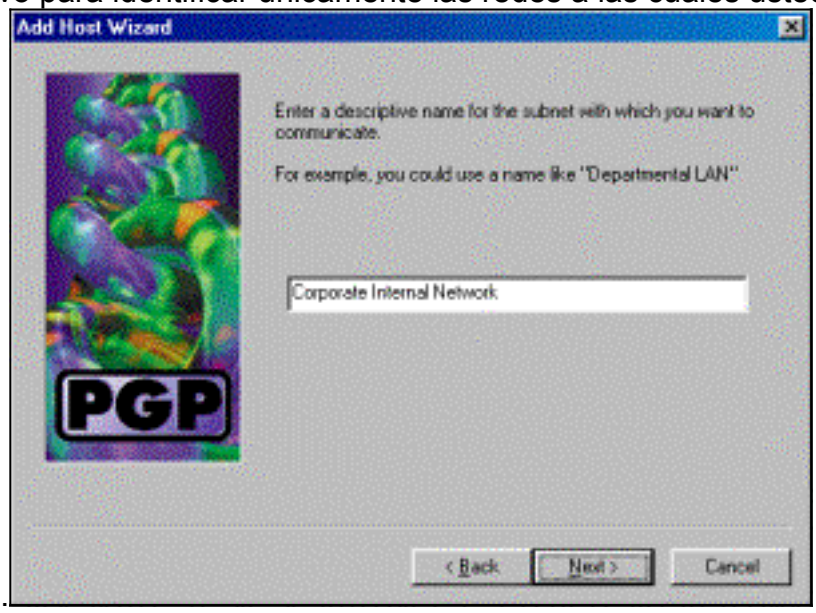
después.

9. Elija **permiten las comunicaciones inseguras** y hacen clic **después**.El concentrador VPN 3000 maneja la Seguridad de la conexión, no el software del cliente



PGP.

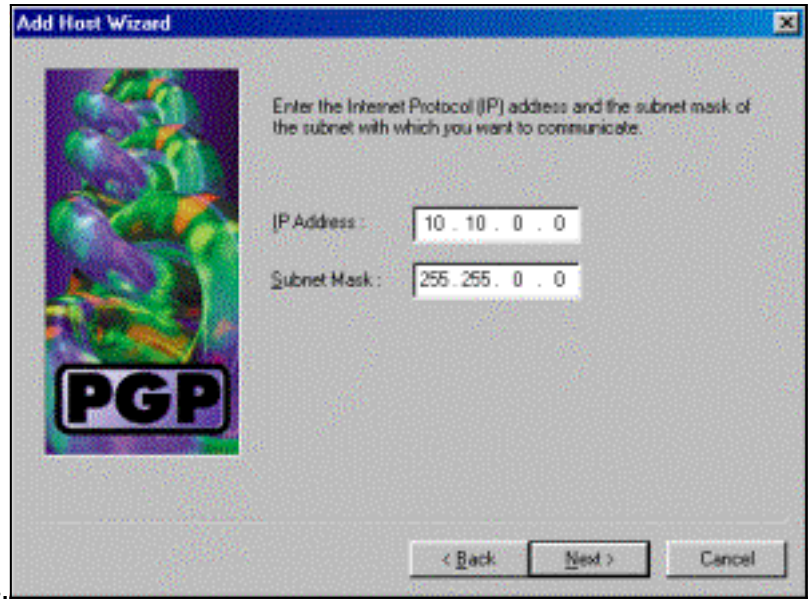
10. Ingrese un nombre descriptivo para identificar únicamente las redes a las cuales usted



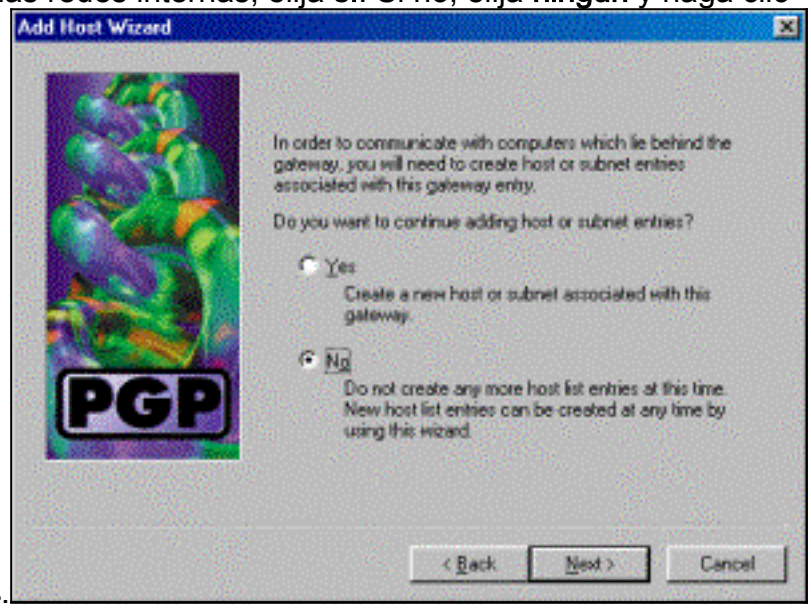
conecta y hace clic **después**.

11. Ingrese el network number y a la máscara de subred para la red detrás del concentrador

VPN 3000 y haga clic **después**.



12. Si hay más redes internas, elija **sí**. Si no, elija **ningún** y haga clic **después**.



Configure el Cisco VPN 3000 Concentrator para validar las conexiones de los Network Associate cliente PGP

Utilice este procedimiento para configurar el Cisco VPN 3000 Concentrator para validar las conexiones del los Network Associate cliente PGP:

1. Seleccione el **> IKE Proposals de la configuración > del Tunelización y de la Seguridad > del IPSec**.
2. Active la oferta **IKE-3DES-SHA-DSA** seleccionándola en columna Inactive Proposals (Propuestas inactivas). Después, haga clic el botón del **activar** y después haga clic el botón **necesario salvaguardia**.
3. Seleccione el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > los SA**.
4. Haga clic en Add (Agregar).
5. Deje todos excepto estos campos en sus configuraciones predeterminadas:**Nombre SA:** Cree un nombre único para identificar esto.**Certificado digital:** Elija el servidor instalado identifican el certificado.**Propuesta IKE:** Seleccione el **IKE-3DES-SHA-DSA**.

6. Haga clic en Add (Agregar).
7. **El Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)** selecto, tecleo **agrega al grupo**, y configura estos campos:**Note**: Si todos sus usuarios son clientes PGP, usted puede utilizar el grupo base (**Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)**) en vez de crear a los nuevos grupos. Si es así salte los pasos para la lengueta de la identidad y los pasos completos 1 y 2 para la lengueta del IPSec solamente.Bajo lengueta de la identidad, ingrese esta información:**Nombre del grupo:** Ingrese un nombre único. (Este nombre del grupo debe ser igual al campo OU en el certificado digital del cliente PGP.)**Contraseña** Ingrese la contraseña para el grupo.Bajo lengueta del IPSec, ingrese esta información:**Autenticación:** Fije esto a **ningunos**.**Configuración de modo:** Desmarque esto.
8. Haga clic en Add (Agregar).
9. Salve según las necesidades en todas partes.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte de IPSec
- Descarga de software VPN (clientes registrados solamente)
- Soporte Técnico - Cisco Systems