# Configurando o Concentrador Cisco VPN 3000 e o Cliente PGP da Network Associates

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Configurar o cliente PGP Network Associates para se conectar ao Cisco VPN 3000 Concentrator Configure o Cisco VPN 3000 Concentrator para aceitar conexões do Network Associates PGP Client Informações Relacionadas

# **Introduction**

Este documento descreve como configurar o Cisco VPN 3000 Concentrator e o Network Associates PGP (Pretty Good Privacy) Client executando a versão 6.5.1 para aceitar conexões entre si.

# **Prerequisites**

#### **Requirements**

Não existem requisitos específicos para este documento.

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco VPN 3000 Concentrator versão 4.7
- Networks Associates PGP Client versão 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.

#### **Conventions**

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

# Configurar o cliente PGP Network Associates para se conectar ao Cisco VPN 3000 Concentrator

Use este procedimento para configurar o Network Associates PGP Client para se conectar ao VPN 3000 Concentrator.

- 1. Inicie **PGPNet > Hosts**.
- 2. Clique em Adicionar e, em seguida, clique em Avançar.
- 3. Escolha a opção Gateway e clique em



Avançar.

4. Insira um nome descritivo para a conexão e clique em

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. "gateway1.company.com") or something more descriptive (e.g. "Departmental linewall").	
	<back next=""> Cancel</back>	4

Avançar.

5. Insira o nome de domínio do host ou o endereço IP da interface pública do VPN 3000 Concentrator e clique em **Next** 

	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 :
PGP	JP Address : 90 . 90 . 90 . 74

(Avançar).

6. Escolha Usar somente segurança criptográfica de chave pública e clique em

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

Avançar.

7. Selecione Sim e clique em Avançar. Quando você adiciona um novo host ou sub-rede, ele permite que você acesse redes privadas depois que sua conexão é

Add Host V	izard	×
	<ul> <li>You have now created a new secure gateway host list entry.</li> <li>To be now created a new secure gateway host list entry.</li> <li>To pow writh the data host or subnet entry now?</li> <li>Image: Secure and the secure gateway host list entry.</li> <li>The secure host or subnet associated with this gateway.</li> <li>The Secure and host or subnet associated with this gateway.</li> <li>The Secure and host or subnet associated with this gateway.</li> </ul>	
protegida.	< Back Next > Cancel	

8. Selecione Sub-rede e clique em



Avançar.

9. Escolha **Permitir comunicações inseguras** e clique em **Avançar**.O VPN 3000 Concentrator lida com a segurança da conexão, não com o 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
	Alow insecure communications
PGP	
	<back next=""> Cancel</back>

10. Insira um nome descritivo para identificar exclusivamente as redes às quais você se

	Enter a descriptive name for the subnet with which you want to communicate. For example, you could use a name like "Departmental LAN"
PGP	Corporate Internal Network
	< <u>B</u> ack Next> Cancel

conecta e clique em Avançar.

11. Digite o número da rede e a máscara de sub-rede da rede atrás do VPN 3000 Concentrator

Add Hast Wizard	Enter the interne the subnet with v	t Protocol (IP) address and the subnet mask of which you want to communicate.	×
PGP	(P Address : Subnet Mask :	10.10.0.0	
		< <u>B</u> ack <u>N</u> ext > Cancel	

e clique em Next.

12. Se houver mais redes internas, escolha Sim. Caso contrário, escolha Não e clique em

	Add Host Wizard	×
	<image/>	
Avancar.	< <u>Back</u> Next> Cancel	

### Configure o Cisco VPN 3000 Concentrator para aceitar conexões do Network Associates PGP Client

Use este procedimento para configurar o Cisco VPN 3000 Concentrator para aceitar conexões de um Network Associates PGP Client:

- 1. Selecione Configuration > Tunneling and Security > IPSec > IKE Proposal.
- 2. Ative a proposta **IKE-3DES-SHA-DSA** selecionando-a na coluna Propostas inativas. Em seguida, clique no botão **Ativar** e clique no botão **Salvar necessário**.
- 3. Selectione Configuration > Policy Management > Traffic Management > SAs.
- 4. Clique em Add.
- Deixe todos, exceto estes campos, em suas configurações padrão: Nome SA: Crie um nome exclusivo para identificar isso. Certificado digital: Escolha o certificado de identificação do servidor instalado. Proposta de IKE: Selecione IKE-3DES-SHA-DSA.
- 6. Clique em Add.
- 7. Selecione **Configuration > User Management > Groups**, clique em **Add Group** e configure estes campos:**Observação:** se todos os seus usuários forem clientes PGP, você poderá usar

o Grupo Base (**Configuração > Gerenciamento de Usuário > Grupo Base**) em vez de criar novos grupos. Em caso afirmativo, ignore as etapas para a guia Identidade e conclua as etapas 1 e 2 somente para a guia IPSec.Na guia Identidade, insira estas informações:**Nome do grupo:** Digite um nome exclusivo. (Esse nome de grupo deve ser igual ao campo OU no certificado digital do cliente PGP.)**Senha:** Digite a senha para o grupo.Na guia IPSec, insira estas informações:**Autenticação:** Defina como **Nenhum.Configuração do modo:** Desmarque isso.

- 8. Clique em Add.
- 9. Salve conforme necessário.

### Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte do IPSec
- Download do software VPN (apenas clientes registrados)
- <u>Suporte Técnico Cisco Systems</u>