# Cisco VPN 3000 コンセントレータおよびネット ワーク関連 PGP クライアントの設定

### 内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント <u>表記法</u> <u>Cisco VPN 3000コンセントレータに接続するためのネットワーク関連PGPクライアントの設定</u> <u>Network Associates PGP Clientからの接続を受け入れるようにCisco VPN 3000コンセントレータ</u> <u>を設定する</u> 関連情報

### 概要

このドキュメントでは、バージョン6.5.1を実行するCisco VPN 3000コンセントレータとNetwork Associates Pretty Good Privacy(PGP)クライアントの両方で、相互の接続を受け入れるように設 定する方法について説明します。

# <u>前提条件</u>

#### <u>要件</u>

このドキュメントに特有の要件はありません。

#### <u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco VPN 3000 コンセントレータ バージョン 4.7
- Networks Associates PGP Client version 6.5.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

#### <u>表記法</u>

ドキュメント表記の詳細は、「<u>シスコ テクニカル ティップスの表記法</u>」を参照してください。

## <u>Cisco VPN 3000コンセントレータに接続するためのネットワー</u> <u>ク関連PGPクライアントの設定</u>

VPN 3000コンセントレータに接続するようにNetwork Associates PGP Clientを設定するには、次の手順を使用します。

- 1. [PGPNet] > [Hosts]を起動します。
- 2. [Add]をクリックし、[Next]をクリックします。
- 3. [Gateway]オプションを選択し、[Next]をクリックします。



4. <u>接続のわかりやすい名前を入力し、[Next]をクリ**ックします**。</u>

dd Host Wizard		12
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 friendal").	
	<back next=""> Cancel</back>	

5. VPN 3000コンセントレータのパブリックインターフェイスのホストドメイン名またはIPア ドレスを入力し、[**Next**]をクリックします。

	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

6. [Use public-key cryptographic security only]を選択し、[Next]をクリックします。 Add Host Wized

	Communication with the specified computer(s) can be secured using public-key cryptographic techniques, or by using a shared secret (passphrare).
Carlo	Use public-key cyptographic security only.
PGP	<ul> <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 risk.</li> </ul>
	< <u>B</u> ack. <u>N</u> exit > Cancel

7. [Yes]を選択し、[Next]をクリ**ックします**。新しいホストまたはサブネットを追加すると、接 続が保護された後にプライベートネットワークに到達できるようになります。

Add Host Wizard		×
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 entry as associated with this gateway entry. Do you want to add a host or subnet entry now? I feed Create a new host or subnet associated with this gateway. I have no not create any more host list entries at this time. New host list entries can be created at any time by using this weakd.	
	< <u>₽</u> ack <u>N</u> ext > Cance	

8. [サブネット]を選択し、[次へ]をクリックします。



9. [Allow insecure communications]を選択し、[Next]をクリックします。VPN 3000コンセント レータは、PGPクライアントソフトウェアではなく、接続のセキュリティを処理します。

Add Host Wizard	J
	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.	For the new entry that you are creating now, select the desired type of communication :
	C Enforce geoure communications
	Alow insecure communications
Fer	
	< Back Next > Cancel

10. 接続先のネットワークを一意に識別するための記述名を入力し、[次へ]をクリックします。



11. VPN 3000コンセントレータの背後にあるネットワークのネットワーク番号とサブネットマ スクを入力し、[Next]をクリックします。

Add Host Wizard		×
	Enter the Internet Protocol (IP) address and the subnet mask of the subnet with which you want to communicate.	
1 Carto	IP Address : 10 . 10 . 0 . 0	
	Subnet Mask : 255.255.0.0	
		100
PGP		
		2
	< Back Next > Cance	

12. 内部ネットワークが多い場合は、[Yes]を選択します。それ以外の場合は、「No」を選択し



、「次へ」をクリ**ックします**。

### <u>Network Associates PGP Clientからの接続を受け入れるように</u> <u>Cisco VPN 3000コンセントレータを設定する</u>

次の手順を使用して、Network Associates PGP Clientからの接続を受け入れるようにCisco VPN 3000コンセントレータを設定します。

- 1. Configuration > Tunneling and Security > IPSec > IKE Proposalsの順に選択します。
- [Inactive Proposals]列でIKE-3DES-SHA-DSAプロポーザルを選択して、プロポーザルをアク ティブにします。次に、[アクティブ化]ボタンをクリックし、[必要な保存]ボタンをクリック します。
- 3. [Configuration] > [Policy Management] > [Traffic Management] > [SAs]を選択します。
- 4. [Add] をクリックします。
- 5. 次のフィールドを除くすべてのフィールドをデフォルト設定のままにします。SA名:これ を識別する一意の名前を作成します。**デジタル証明書:**インストールされているサーバID証 明書を選択します。IKE Proposal:IKE-3DES-SHA-DSAを選択します。
- 6. [Add] をクリックします。
- 7. [Configuration] > [User Management] > [Groups]を選択し、[Add Group]をクリックして、次

のフィールドを設定します。注:すべてのユーザーがPGPクライアントの場合は、新しいグ ループを作成する代わりに、ベースグループ([Configuration] > [User Management] > [Base Group])を使用できます。その場合は、[Identity]タブの手順をスキップし、[IPSec]タブの手 順1と2のみを実行します。[Identity]タブで、次の情報を入力します。グループ名:一意の名前 を入力します。(このグループ名は、PGPクライアントのデジタル証明書のOUフィールド と同じである必要があります)。パスワード:グループのパスワードを入力します。 [IPSec]タブで、次の情報を入力します。認証:これを[なし]に設定します。モード設定:こ れをオフにします。

- 8. [Add] をクリックします。
- 9. 必要に応じて全体を保存します。

### <u>関連情報</u>

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- IPSec に関するサポート ページ
- <u>VPN Software Download</u>(登録<u>ユーザ</u>専用)
- <u>テクニカルサポート Cisco Systems</u>