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

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。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

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。

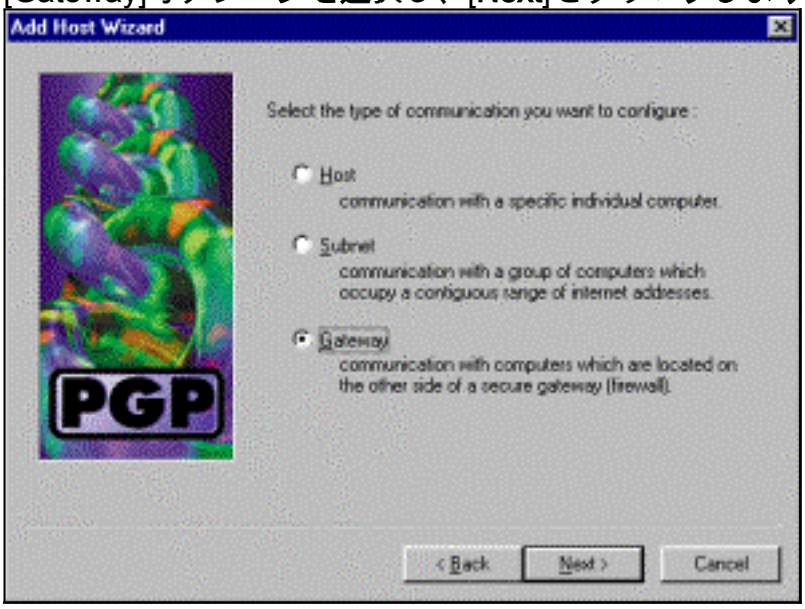
表記法

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

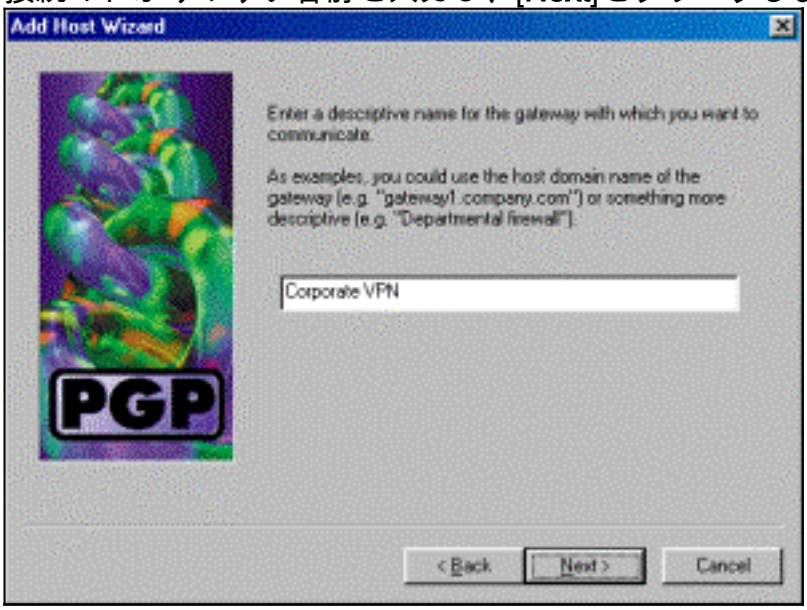
Cisco VPN 3000コンセントレータに接続するためのネットワーク関連PGPクライアントの設定

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。

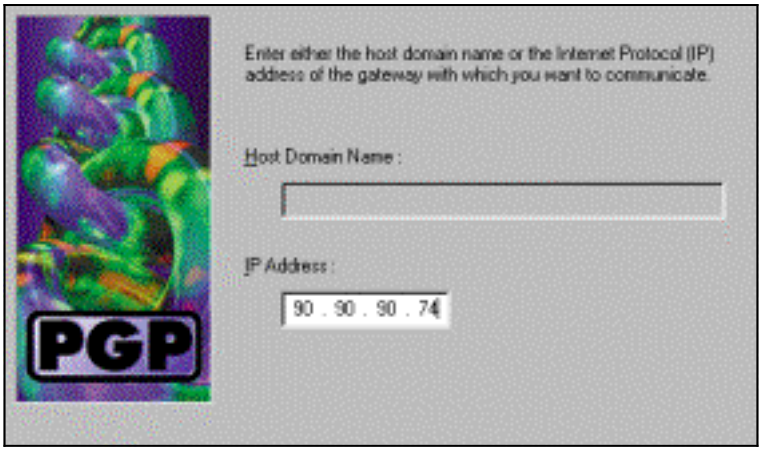
1. [PGPNet] > [Hosts]を起動します。
2. [Add]をクリックし、[Next]をクリックします。
3. [Gateway]オプションを選択し、[Next]をクリックします。



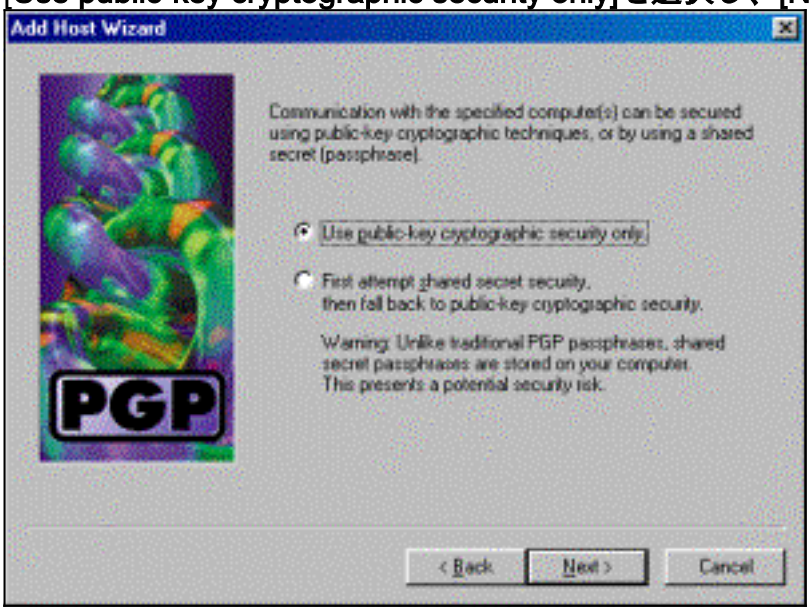
4. 接続のわかりやすい名前を入力し、[Next]をクリックします。



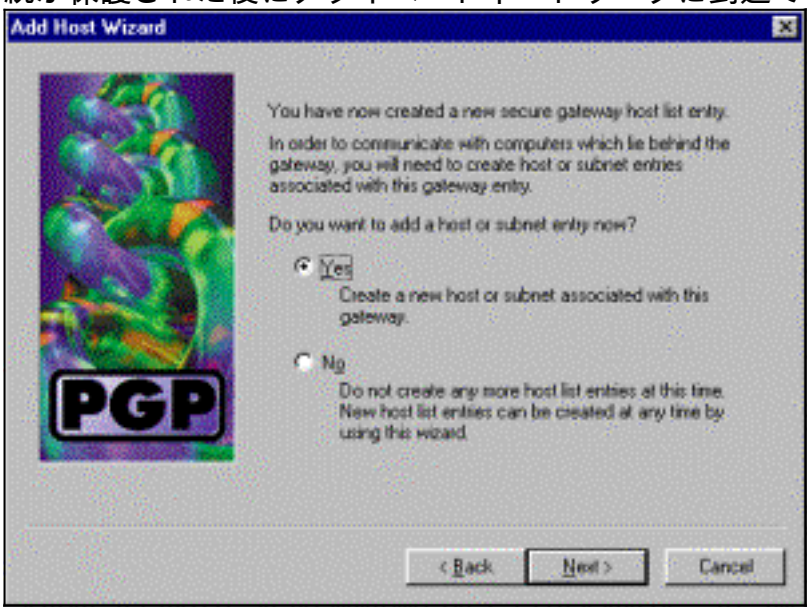
5. VPN 3000コンセントレータのパブリックインターフェイスのホストドメイン名またはIPアドレスを入力し、[Next]をクリックします。



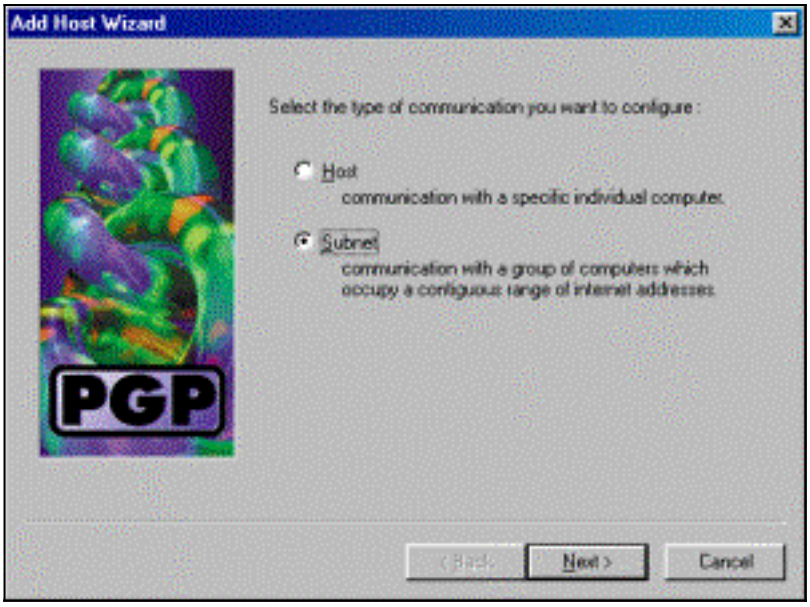
6. [Use public-key cryptographic security only]を選択し、[Next]をクリックします。



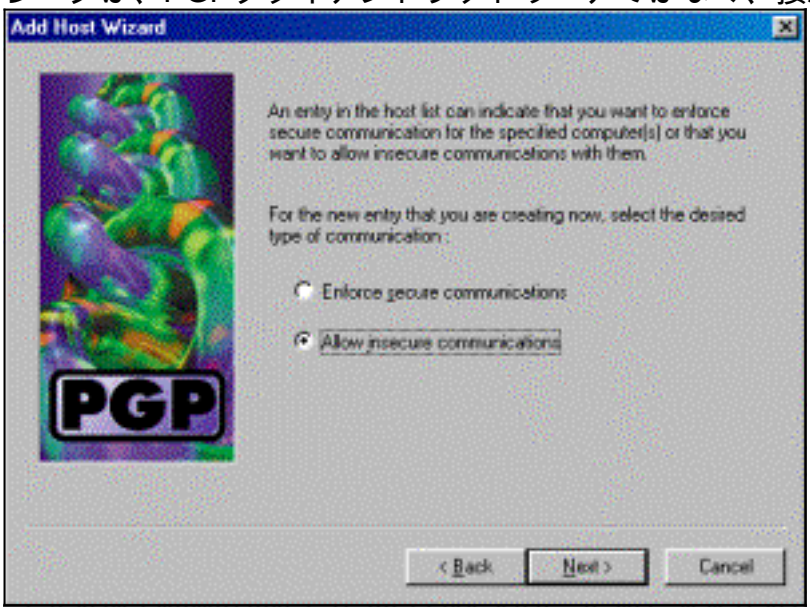
7. [Yes]を選択し、[Next]をクリックします。新しいホストまたはサブネットを追加すると、接続が保護された後にプライベートネットワークに到達できるようになります。



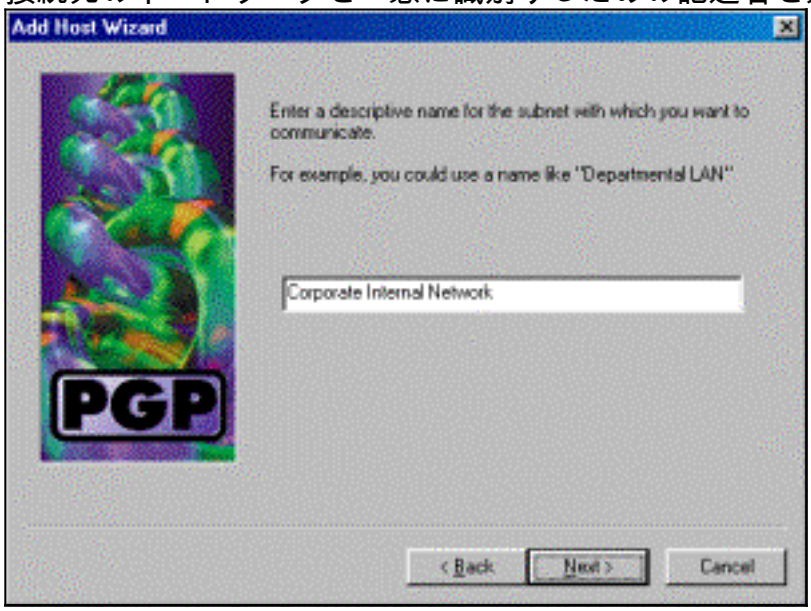
8. [サブネット]を選択し、[次へ]をクリックします。



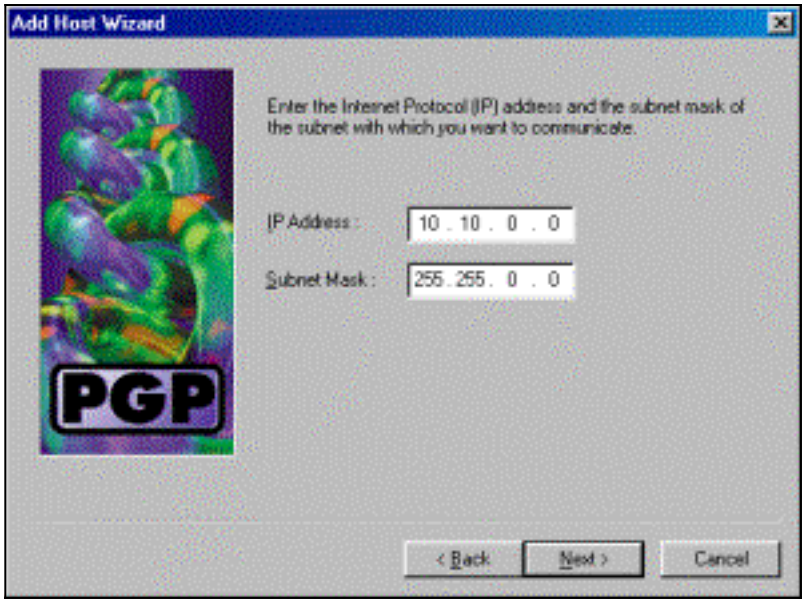
9. [Allow insecure communications]を選択し、[Next]をクリックします。VPN 3000コンセントレータは、PGPクライアントソフトウェアではなく、接続のセキュリティを処理します。



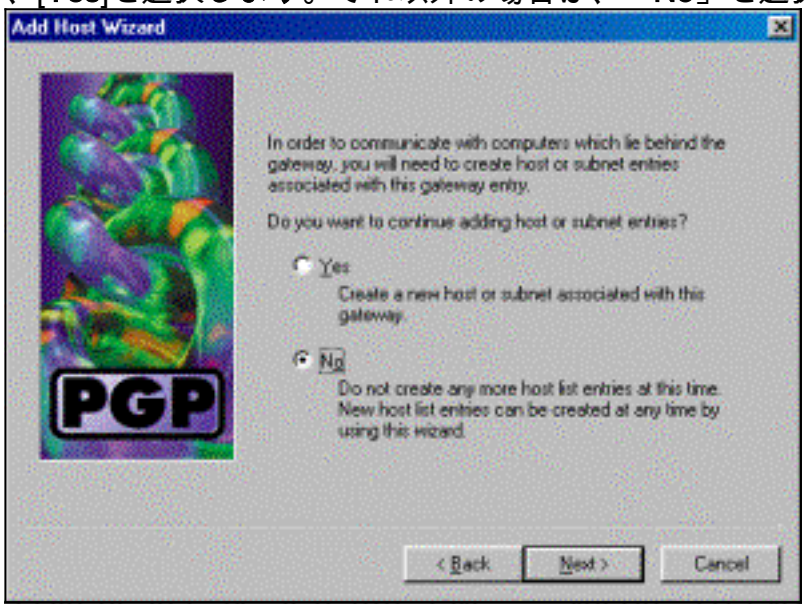
10. 接続先のネットワークを一意に識別するための記述名を入力し、[次へ]をクリックします。



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。



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。



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する

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。
2. [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。

関連情報

- 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
- VPN Software Download(登録ユーザ専用)
- テクニカルサポート - Cisco Systems