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

目次

概要

この資料に互いからの接続を許可するためにバージョン 6.5.1 を実行する Cisco VPN 3000 コンセントレータおよびネットワークアソシエイト PGP クライアントを両方設定する方法を記述されています。

前提条件

要件

このドキュメントに関する固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くものです。

- Cisco VPN 3000 コンセントレータ バージョン 4.7
- ネットワーク仲間 PGP クライアントバージョン 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

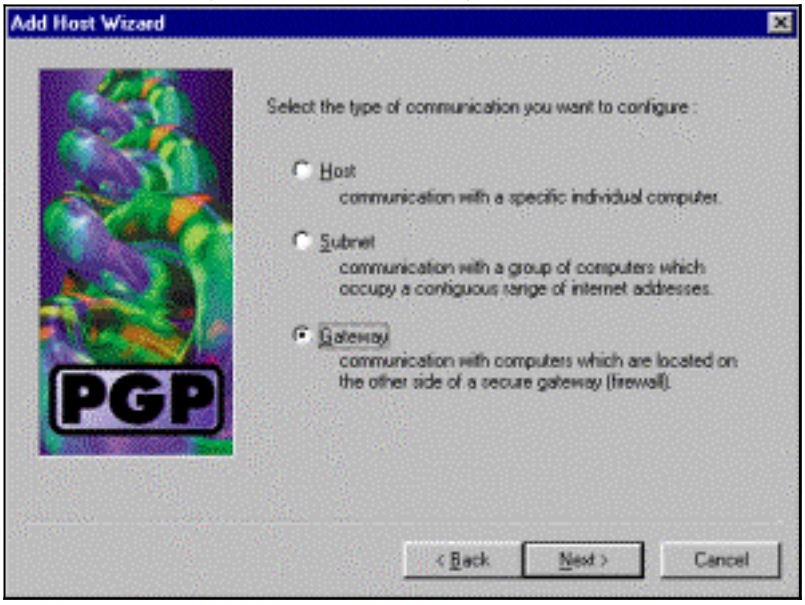
表記法

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。

ネットワークアソシエイト PGP クライアントを Cisco VPN 3000 コンセントレータに接続するために設定して下さい

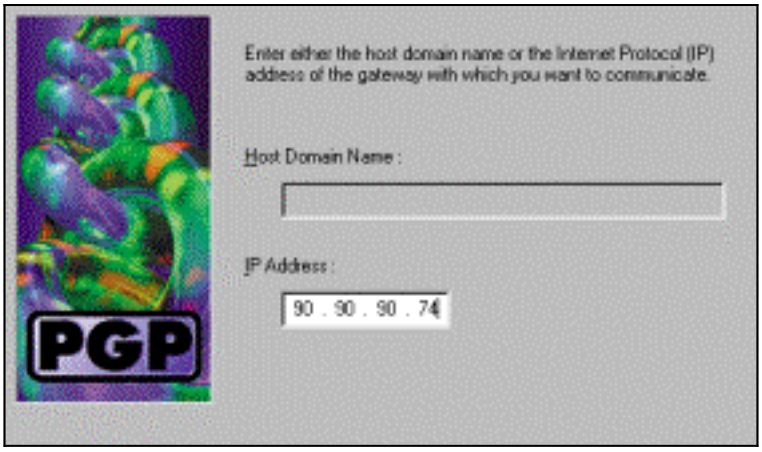
ネットワークアソシエイト PGP クライアントを VPN 3000 コンセントレータに接続するために設定するのにこのプロシージャを使用して下さい。

1. **PGPNet > ホストを**起動させて下さい。
2. 『Add』 をクリック し、次に『Next』 をクリック して下さい。
3. **GATEWAY オプションを**選択し、『Next』 をクリック して下さい。

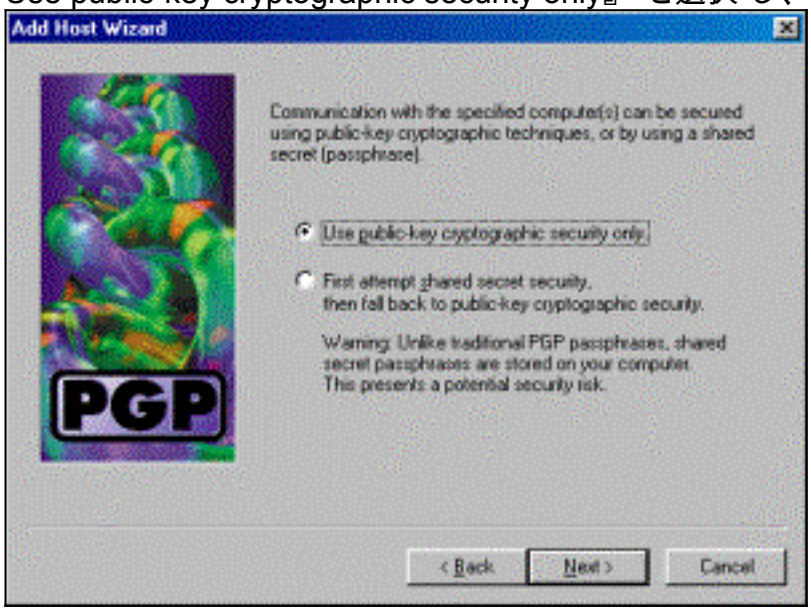


4. 接続のわかりやすい名前を入力し、『Next』 をクリック して下さい。

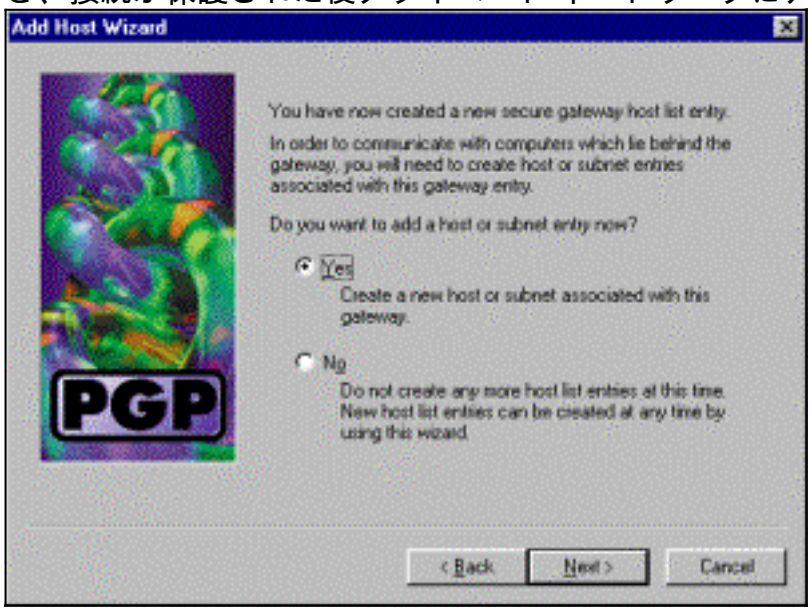
5. VPN 3000 コンセントレータのパブリックインターフェイスのホスト ドメイン名か IP アドレスを入力し、『Next』 をクリック して下さい。



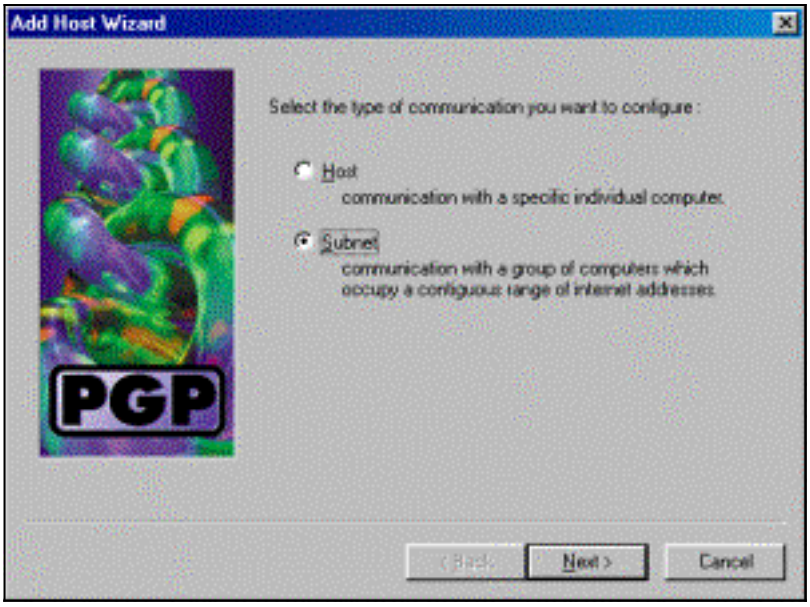
6. 『Use public-key cryptographic security only』 を選択 し、『Next』 をクリック して下さい。



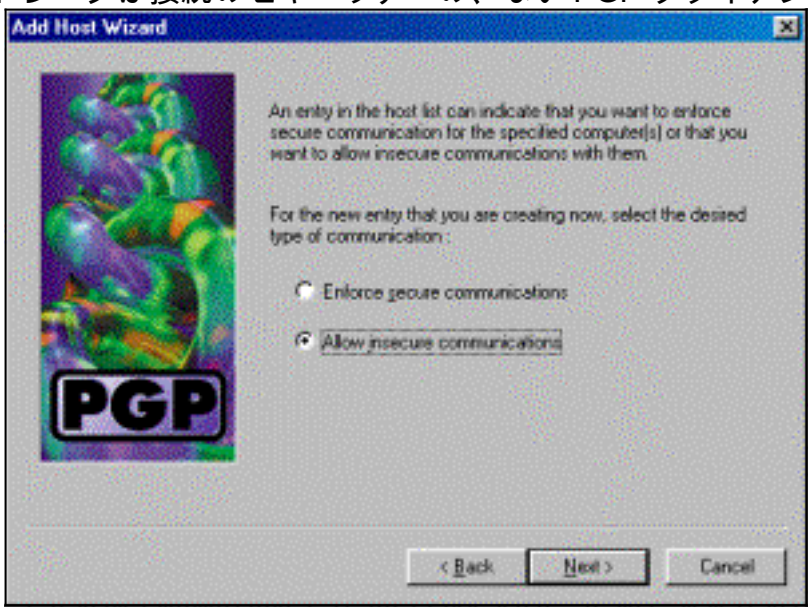
7. 『Yes』 を選択 し、『Next』 をクリック して下さい。 新しいホストかサブネットを追加するとき、接続が保護された後プライベート ネットワークにアクセスすることを可能にします。



8. 『Subnet』 を選択 し、『Next』 をクリック して下さい。

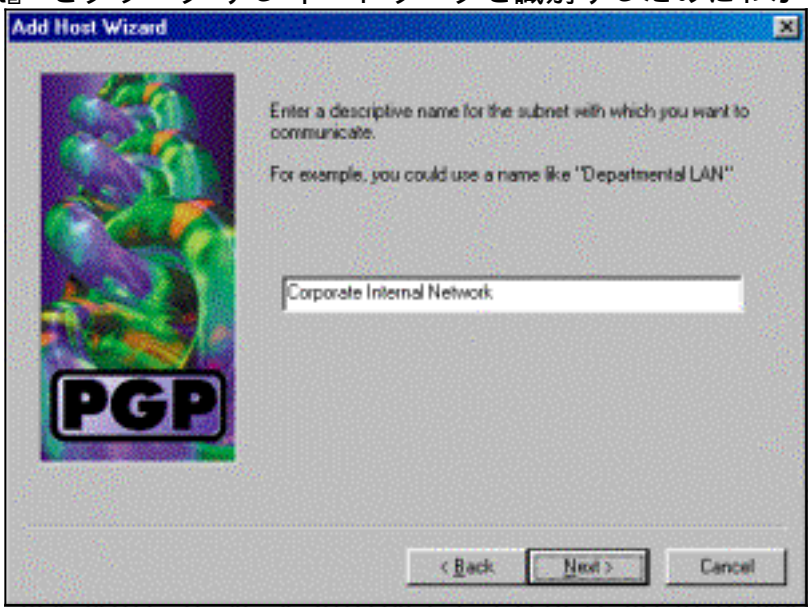


9. 『Allow insecure communications』 を選択 し、『Next』 をクリック して下さい。VPN 3000 コンセントレータは接続のセキュリティの、ない PGP クライアントソフトウェア問題



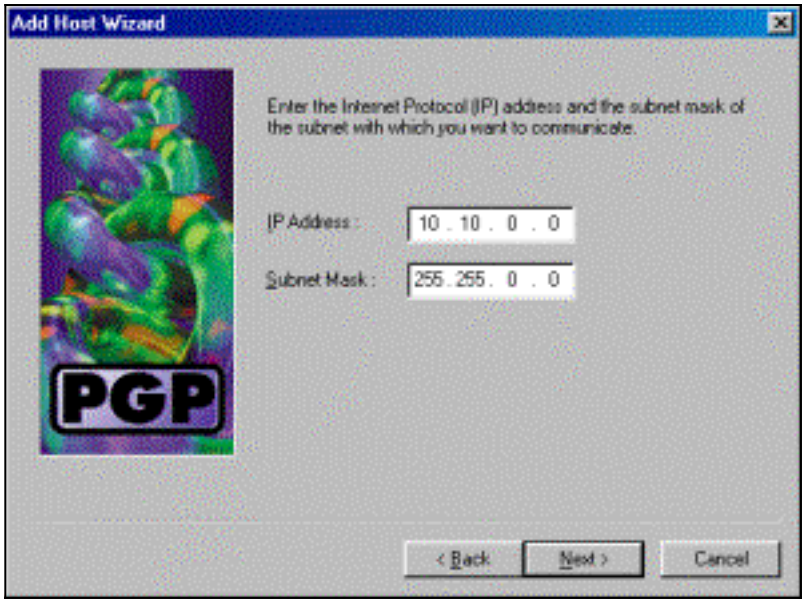
を解決します。

10. 接続し、『Next』 をクリック する ネットワークを識別するためにわかりやすい名前を入

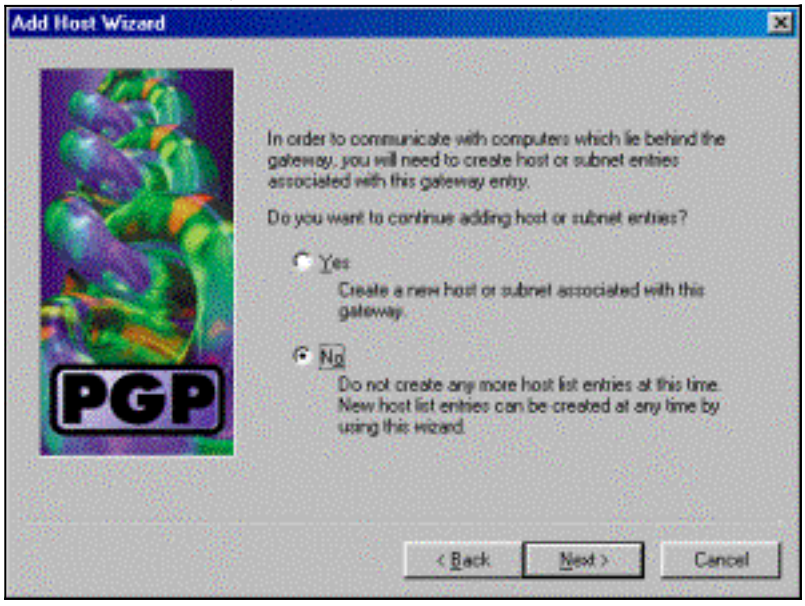


力して下さい。

11. VPN 3000 コンセントレータの背後にあるネットワークのためのネットワーク番号および サブネット マスクを入力し、『Next』 をクリック して下さい。



12. より多くの内部ネットワークがある場合、『Yes』 を選択 して下さい。 さもなければ、『No』 を選択 し、『Next』 をクリック して下さい。



ネットワークアソシエイト PGP クライアントからの接続を許可するために Cisco VPN 3000 コンセントレータを設定して下さい

Cisco VPN 3000 コンセントレータをネットワークアソシエイト PGP クライアントからの接続を許可するために設定するのにこのプロシージャを使用して下さい:

1. Configuration > Tunneling and Security > IPSec > IKE Proposals の順に選択 して下さい。
2. 非アクティブ提案カラムでそれを選択することによって **IKE-3DES-SHA-DSA** 提案をアクティブにして下さい。 次に、**Activate ボタンを**クリックし、次に **Save Needed ボタンを**クリックして下さい。
3. Configuration > Policy Management > Traffic Management > SAs の順に選択 して下さい。
4. [Add] をクリックします。
5. デフォルト設定でこれらのフィールドを除いてすべてを残して下さい:**SA 名前:** これを識別するために固有の名前を作成して下さい。**デジタル認証:** インストール済みサーバを識別します認証を選択して下さい。**IKE Proposal:** 『IKE-3DES-SHA-DSA』 を選択 して下さい。
6. [Add] をクリックします。

7. これらのフィールドを Configuration > User Management > Groups の順に選択 し、『Add Group』 をクリック し、設定して下さい:**注:** すべてのユーザが PGP クライアントである場合、新しいグループを作成するかわりに基礎群（**Configuration > User Management > Base Group**）を使用できます。 その場合、Identity タブのためのステップをスキップし、IPSec タブだけのためのステップ 1 および 2 を完了して下さい。Identity タブの下で、この情報を入力して下さい:**グループ名:** 固有の名前を入力して下さい。（このグループ名は PGP クライアントのデジタル認証の OU フィールドと等しい必要があります。）**[Password]：** グループのためのパスワードを入力して下さい。IPSec タブの下で、この情報を入力して下さい:**認証： どれも**にこれを設定 しない で下さい。**モードコンフィギュレーション:** これのチェックを外して下さい。
8. [Add] をクリックします。
9. すっかり必要に応じて保存。

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 ソフトウェアダウンロード（登録ユーザのみ）
- テクニカルサポート - Cisco Systems