配置Cisco VPN 3000集中器和Network Associates PGP客戶端

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[配置Network Associates PGP客戶端以連線到Cisco VPN 3000集中器](#)
[配置Cisco VPN 3000集中器以接受來自Network Associates PGP客戶端的連線](#)
[相關資訊](#)

簡介

本文描述如何配置運行6.5.1版的Cisco VPN 3000集中器和Network Associates Pretty Good Privacy(PGP)客戶端，以接受彼此的連線。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco VPN 3000集中器版本4.7
- Networks Associates PGP客戶端6.5.1版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

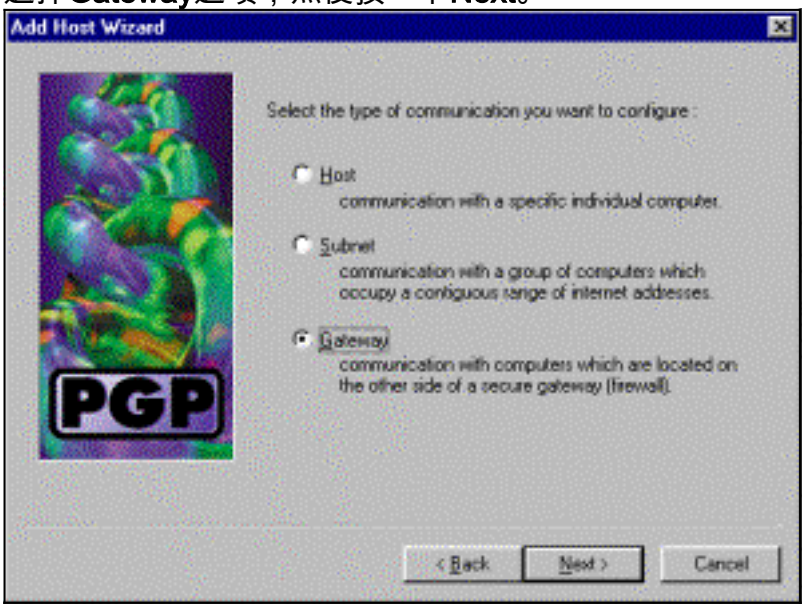
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

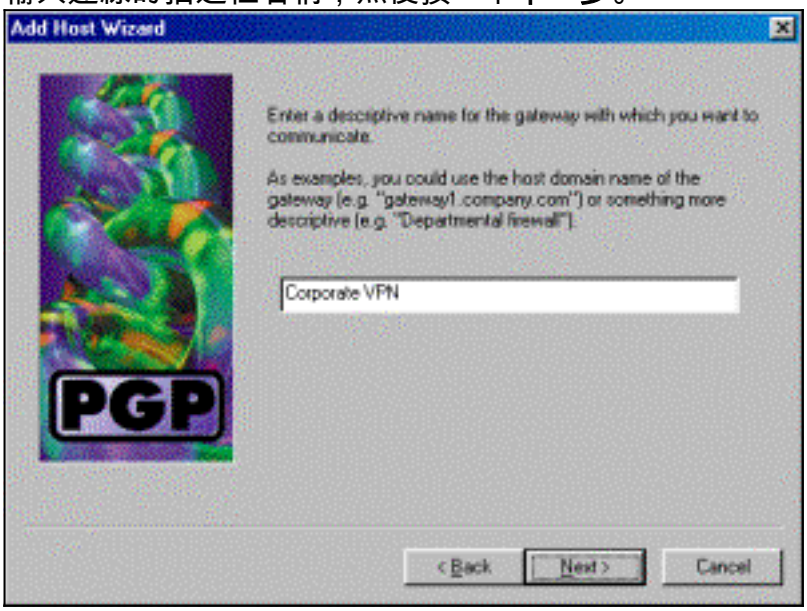
配置Network Associates PGP客戶端以連線到Cisco VPN 3000集中器

使用此過程配置Network Associates PGP客戶端以連線到VPN 3000集中器。

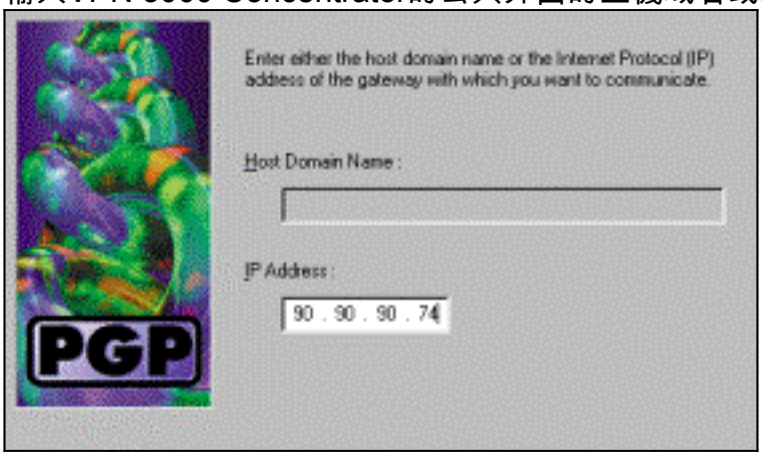
1. 啟動**PGPNet >主機**。
2. 按一下「**Add**」，然後按一下「**Next**」。
3. 選擇**Gateway**選項，然後按一下**Next**。



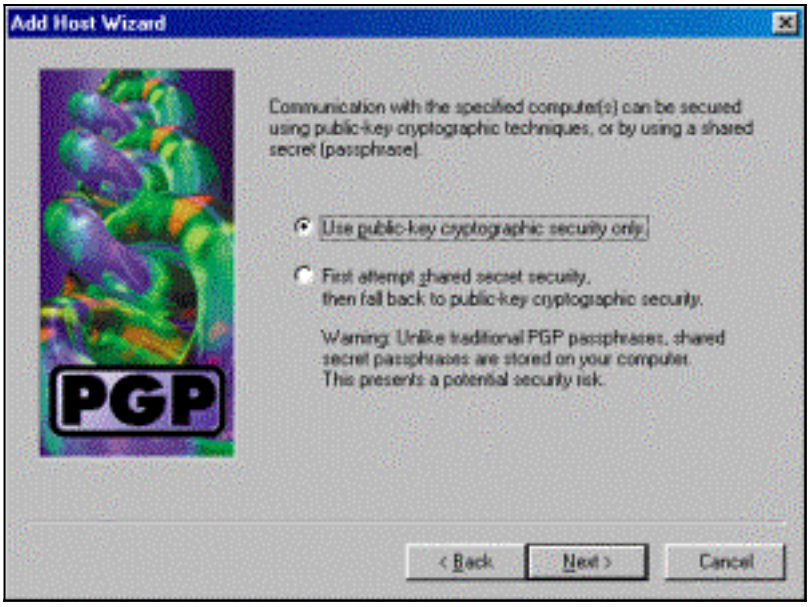
4. 輸入連線的描述性名稱，然後按一下**下一步**。

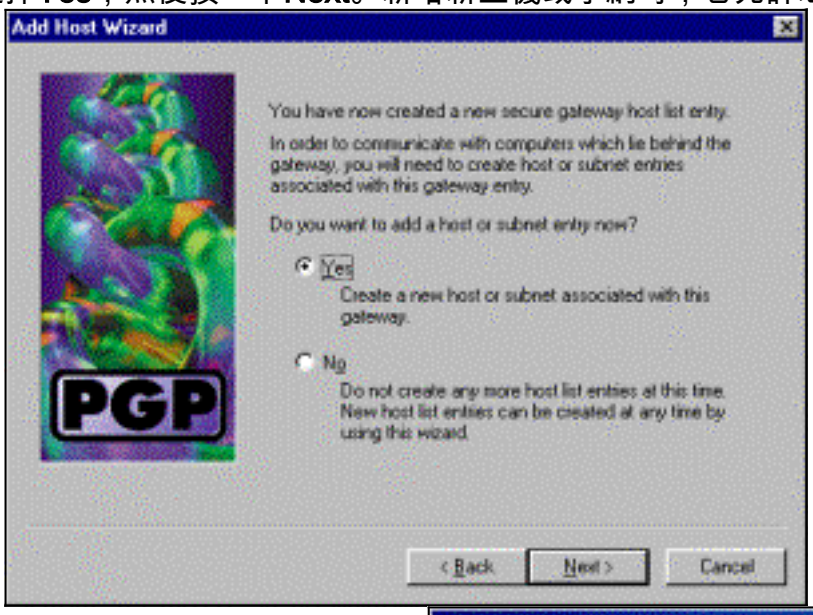


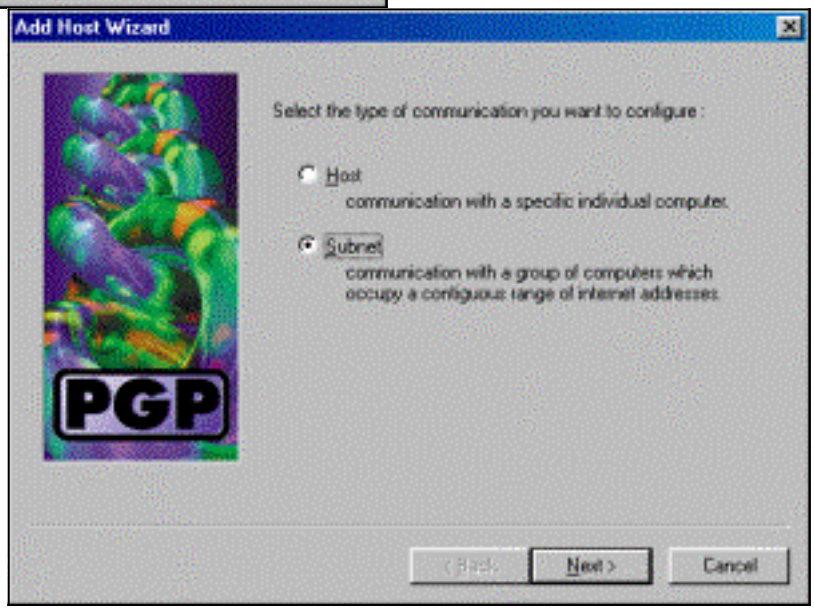
5. 輸入VPN 3000 Concentrator的公共介面的主機域名或IP地址，然後按一下**Next**。



6. 選擇**Use public-key cryptographic security only**，然後按一下**Next**。



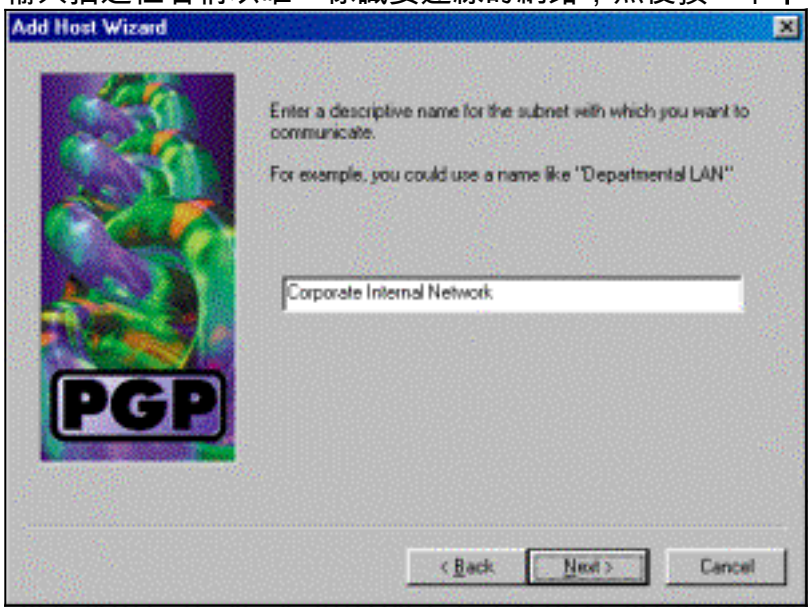
7. 選擇**Yes**，然後按一下**Next**。新增新主機或子網時，它允許您在連線受到保護後訪問專用網路


。


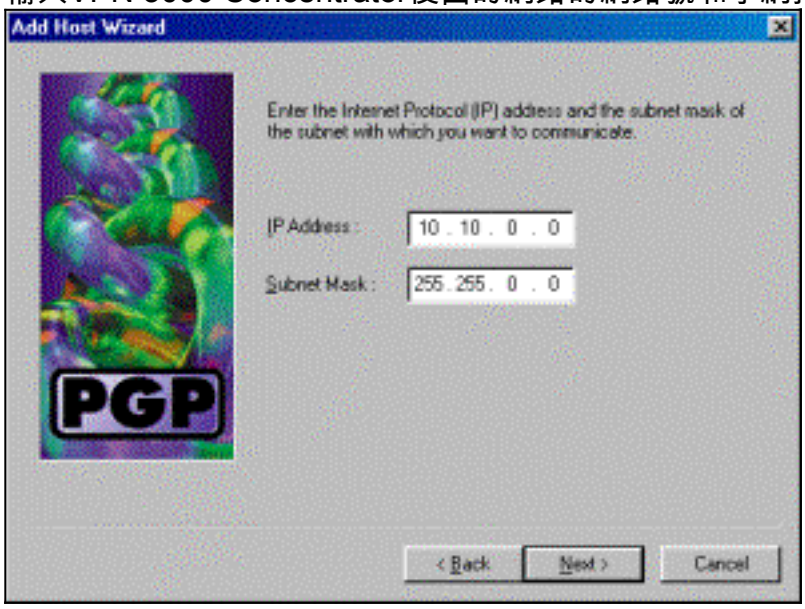
8. 選擇**Subnet**，然後按一下**Next**。
9. 選擇**Allow insecure communications**，然後按一下**Next**。VPN 3000集中器處理連線的安全

，而不是PGP客戶端軟體。

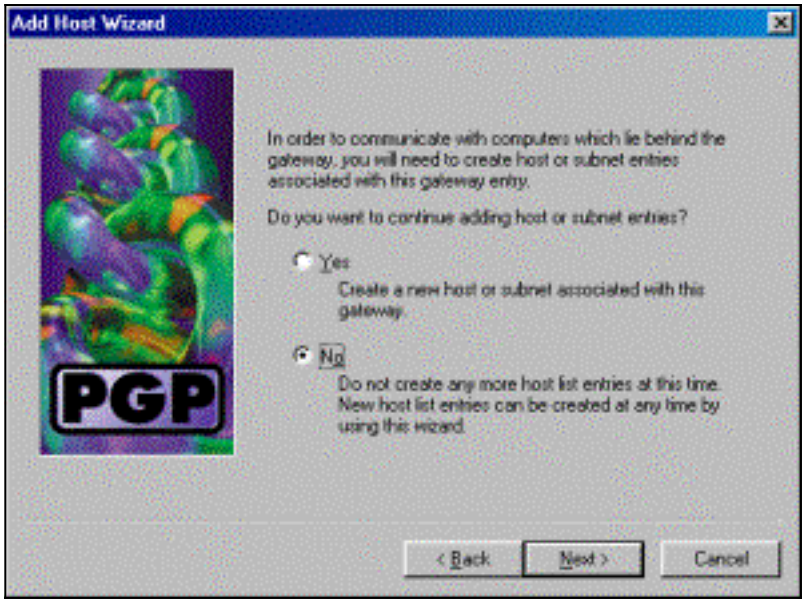
10. 輸入描述性名稱以唯一標識要連線的網路，然後按一下**下一步**。



11. 輸入VPN 3000 Concentrator後面的網路的網路號和子網掩碼，然後按一下**Next**。



12. 如果有更多內部網路，請選擇**Yes**。否則，選擇**No**，然後按一下**Next**。



配置Cisco VPN 3000集中器以接受來自Network Associates PGP客戶端的連線

使用以下過程配置Cisco VPN 3000集中器以接受來自Network Associates PGP客戶端的連線：

1. 選擇**Configuration > Tunneling and Security > IPSec > IKE Proposals**。
2. 在Inactive Proposals（非活動建議）列中選擇**IKE-3DES-SHA-DSA**建議，即可啟用該建議。接下來，按一下**Activate**按鈕，然後按一下**Save Needed**按鈕。
3. 選擇**Configuration > Policy Management > Traffic Management > SAs**。
4. 按一下「**Add**」。
5. 將除以下欄位以外的所有欄位保留為預設設定：**SA名稱**：建立唯一名稱以標識此名稱。**數位證書**：選擇安裝的伺服器標識證書。**IKE建議**：選擇**IKE-3DES-SHA-DSA**。
6. 按一下「**Add**」。
7. 選擇**Configuration > User Management > Groups**，按一下**Add Group**，然後配置以下欄位：**注意**：如果所有使用者都是PGP客戶端，則可以使用基本組(**Configuration > User Management > Base Group**)，而不是建立新組。如果是，請跳過Identity頁籤的步驟，並僅完成IPSec頁籤的步驟1和2。在Identity頁籤下，輸入以下資訊：**組名**：輸入唯一名稱。（此組名稱必須等於PGP客戶端數位證書中的OU欄位。）**密碼**：輸入組的密碼。在IPSec頁籤下，輸入以下資訊：**驗證**:將此項設定為**None**。**模式配置**：取消選中此項。
8. 按一下「**Add**」。
9. 始終根據需要進行儲存。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- IPSec支援頁面
- VPN軟體下載(僅限註冊客戶)
- 技術支援 - Cisco Systems