

在VPN 3000產品中使用RADIUS伺服器

目錄

[簡介](#)

[開始之前](#)

[慣例](#)

[必要條件](#)

[採用元件](#)

[使用Windows 2000 RADIUS伺服器驗證Cisco VPN客戶端](#)

[使用不支援MSCHAP的RADIUS伺服器](#)

[對PPTP使用加密](#)

[相關資訊](#)

簡介

本檔案介紹將某些RADIUS伺服器與VPN 3000集中器和VPN使用者端一起使用時發現的一些警告。

- Windows 2000 RADIUS伺服器需要密碼身份驗證協定(PAP)來驗證Cisco VPN客戶端。
(IPsec客戶端)
- 使用不支援Microsoft質詢握手身份驗證協定(MSCHAP)的RADIUS伺服器要求在VPN 3000集中器上禁用MSCHAP選項。(點對點通道通訊協定[PPTP]使用者端)
- 在PPTP中使用加密需要從RADIUS返回屬性MSCHAP-MPPE-Keys。(PPTP客戶端)
- 在Windows 2003中，可以使用MS-CHAP v2，但身份驗證方法應設定為「RADIUS with Expiry」。

其中一些註釋出現在產品發行說明中。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

必要條件

本文件沒有特定先決條件。

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 Concentrator

- Cisco VPN使用者端

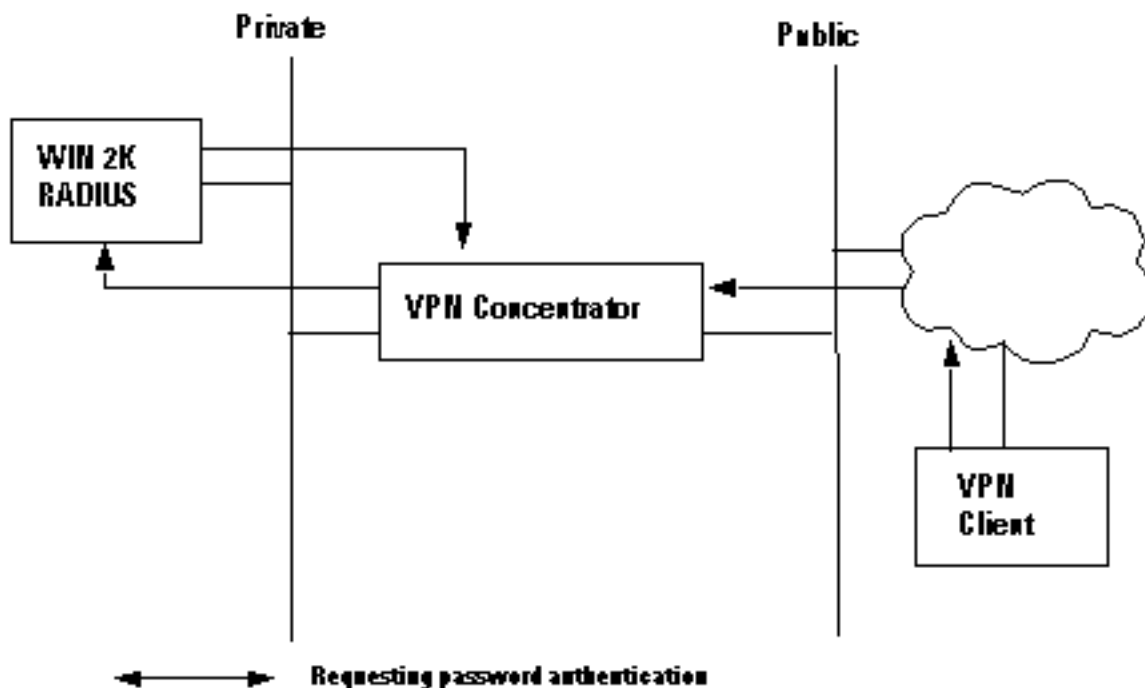
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

使用Windows 2000 RADIUS伺服器驗證Cisco VPN客戶端

您可以使用Windows 2000 RADIUS伺服器驗證VPN客戶端使用者。在以下場景中（VPN客戶端請求身份驗證），VPN 3000集中器從VPN客戶端接收包含客戶端使用者的使用者名稱和密碼的請求。在將使用者名稱/密碼傳送到專用網路中的Windows 2000 RADIUS伺服器進行驗證之前，VPN集中器使用HMAC/MD5演算法對其進行雜湊。

Windows 2000 RADIUS伺服器需要PAP來驗證VPN客戶端會話。要啟用RADIUS伺服器對VPN客戶端使用者進行身份驗證，請檢查編輯撥入配置檔案視窗上的未加密身份驗證(PAP, SPAP)引數（預設情況下，不檢查此引數）。要設定此引數，請選擇正在使用的遠端訪問策略，選擇屬性，然後選擇身份驗證頁籤。

請注意，此引數名稱上的Unencrypted字詞具有誤導性。使用此引數不會引起安全漏洞，因為VPN集中器向RADIUS伺服器傳送身份驗證資料包時，不會以明文形式傳送密碼（如果使用VPN集中器，則不會以明文形式傳送密碼）。VPN集中器從VPN客戶端接收使用者名稱/密碼和加密資料包，並在向伺服器傳送身份驗證資料包之前對密碼執行HMAC/MD5雜湊。



使用不支援MSCHAP的RADIUS伺服器

某些RADIUS伺服器不支援MSCHAPv1或MSCHAPv2使用者驗證。如果使用不支援MSCHAP（v1或v2）的RADIUS伺服器，則必須將基本組的PPTP身份驗證協定配置為使用PAP和/或CHAP，同時禁用MSCHAP選項。不支援MSCHAP的RADIUS伺服器的示例包括Livingston v1.61 RADIUS伺服器或基於Livingston代碼的任何RADIUS伺服器。

注意：如果沒有MSCHAP，PPTP客戶端之間的資料包將不會被加密。

對PPTP使用加密

要對PPTP使用加密，RADIUS伺服器必須支援MSCHAP身份驗證，並且必須為每個使用者身份驗證傳送返回屬性MSCHAP-MPPE-Keys。支援此屬性的RADIUS伺服器示例如下所示。

- Cisco Secure ACS for Windows - 2.6版或更高版本
- Funk軟體鋼帶式RADIUS
- Microsoft Internet Authentication Server on NT 4.0伺服器選項包
- Microsoft商業網際網路系統(MCIS 2.0)
- Microsoft Windows 2000 Server — Internet身份驗證伺服器

相關資訊

- [RADIUS 支援頁面](#)
- [Cisco Secure ACS for Windows支援頁](#)
- [Cisco VPN 3000系列集中器支援頁面](#)
- [Cisco VPN 3000系列使用者端支援頁面](#)
- [IPSec支援頁面](#)
- [PPTP支援頁面](#)
- [RFC 2637:點對點通道通訊協定\(PPTP\)](#)
- [要求建議 \(RFC\)](#)
- [技術支援 - Cisco Systems](#)