VPN 3000 製品でRADIUSサーバを使用する方法

内容

概要

このドキュメントでは、VPN 3000 コンセントレータおよび VPN Client を使用している RADIUS サーバを使用した場合に表示される特定の警告について説明します。

- Windows 2000 RADIUSサーバでは、Cisco VPN Clientの認証にPassword Authentication Protocol(PAP)が必要です。（IPSecクライアント）
- Microsoft Challenge Handshake Authentication Protocol(MSCHAP)をサポートしていないRADIUSサーバを使用するには、VPN 3000コンセントレータでMSCHAPオプションを無効にする必要があります。(Point-to-Point Tunneling Protocol(PPTP)クライアント)
- PPTPで暗号化を使用するには、RADIUSからの戻り属性MSCHAP-MPPE-Keysが必要です（PPTPクライアント）。
- Windows 2003ではMS-CHAP v2を使用できますが、認証方式は「RADIUS with Expiry」に設定する必要があります。

これらのノートの一部は、製品のリリースノートに記載されています。

はじめに

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。

前提条件

このドキュメントに関しては個別の前提条件はありません。

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
- Cisco VPN Client

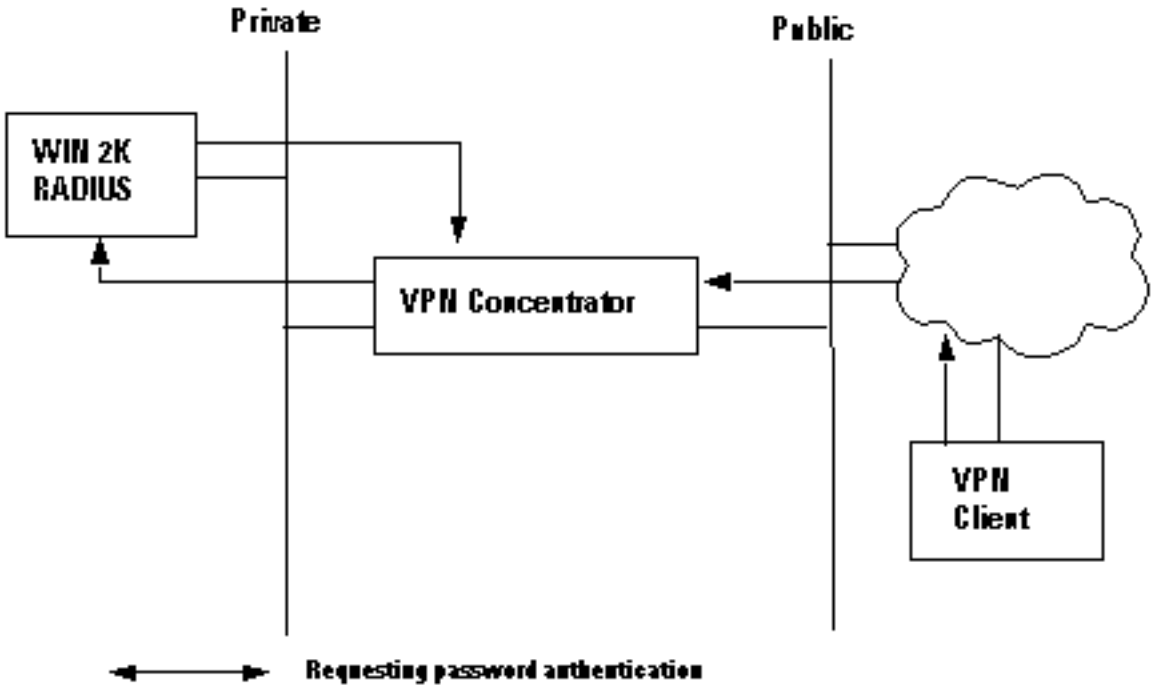
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

Windows 2000 RADIUSサーバを使用したCisco VPN Clientの認証

Windows 2000 RADIUSサーバを使用して、VPN Clientユーザを認証できます。次のシナリオ（VPN Clientが認証を要求している）では、VPN 3000コンセントレータは、クライアントユーザのユーザ名とパスワードを含む要求をVPN Clientから受信します。ユーザ名/パスワードをプライベートネットワークのWindows 2000 RADIUSサーバに送信して検証する前に、VPNコンセントレータはHMAC/MD5アルゴリズムを使用してハッシュします。

Windows 2000 RADIUSサーバでは、VPN Clientセッションの認証にPAPが必要です。RADIUSサーバでVPN Clientユーザの認証を有効にするには、[ダイヤルインプロファイルの**編集(Edit Dial-in Profile)]ウィンドウでUnencrypted Authentication (PAP, SPAP)パラメータにチェックマークを付け**ます（デフォルトでは、このパラメータはチェック外されません）。 このパラメータを設定するには、使用しているリモー**トアクセスポリシー**を選択し、[プロパティ]**を選択**し、[Authentication]タブを選択します。

このパラメータの名前に*関*するUnencryptedという単語は誤解を招きやすいことに注意してください。VPNコンセントレータが認証パケットをRADIUSサーバに送信する場合、パスワードがクリアテキスト(RADIUS)で送信されないため、このパラメータを使用してもセキュリティ違反は発生しません。VPNコンセントレータは、ユーザ名/パスワードと暗号化されたパケットをVPN Clientから受信し、認証パケットをサーバに送信する前に、パスワードでHMAC/MD5ハッシュを実行します。



MSCHAP をサポートしないRADIUSサーバの使用

一部のRADIUSサーバでは、MSCHAPv1またはMSCHAPv2ユーザ認証がサポートされていません。MSCHAP（v1またはv2）をサポートしていないRADIUSサーバを使用している場合は、PAPまたはCHAPを使用するようにベースグループのPPTP認証プロトコルを設定し、MSCHAPオプションも無効にする必要があります。MSCHAPをサポートしないRADIUSサーバの例としては、Livingston v1.61 RADIUSサーバや、Livingstonコードに基づくRADIUSサーバなどがあります。

注：MSCHAPを使用しない場合、PPTPクライアントとの間で送受信されるパケット*は暗号化*されません。

PPTP の暗号化の使用

PPTPで暗号化を使用するには、RADIUSサーバがMSCHAP認証をサポートし、すべてのユーザ認証に対して戻り属性MSCHAP-MPPE-Keysを送信する必要があります。この属性をサポートするRADIUSサーバの例を次に示します。

- Cisco Secure ACS for Windows：バージョン2.6以降
- Funk Software Steel-Belted RADIUS
- NT 4.0 Server Options PackのMicrosoft Internet Authentication Server
- Microsoft Commercial Internet System（MCIS 2.0）
- Microsoft Windows 2000 Server:Internet Authentication Server

関連情報

- RADIUS に関するサポート ページ
- Cisco Secure ACS for Windows に関するサポート ページ
- 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
- Cisco VPN 3000 シリーズ クライアントに関するサポート ページ
- IPSec に関するサポート ページ
- PPTP に関するサポート ページ
- RFC 2637:Point-to-Point Tunneling Protocol（PPTP）
- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems