# Uso de servidores RADIUS con productos VPN 3000

## Contenido



## Introducción

Este documento describe ciertas advertencias encontradas al utilizar algunos servidores RADIUS con el concentrador VPN 3000 y los clientes VPN.

- El servidor RADIUS de Windows 2000 requiere el protocolo de autenticación de contraseña (PAP) para autenticar un cliente VPN de Cisco. (clientes IPSec)
- El uso de un servidor RADIUS que no admite el protocolo de autenticación por desafío mutuo de Microsoft (MSCHAP) requiere que las opciones de MSCHAP se desactiven en el concentrador VPN 3000. (Clientes PPTP)
- El uso del cifrado con PPTP requiere el atributo de devolución MSCHAP-MPPE-Keys de RADIUS. (clientes PPTP)
- Con Windows 2003, se puede utilizar MS-CHAP v2, pero el método de autenticación debe configurarse como "RADIUS con vencimiento".

Algunas de estas notas aparecen en las notas de la versión del producto.

## Antes de comenzar

### Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

### Prerequisites

No hay requisitos previos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Concentrador Cisco VPN 3000
- Cliente de Cisco VPN

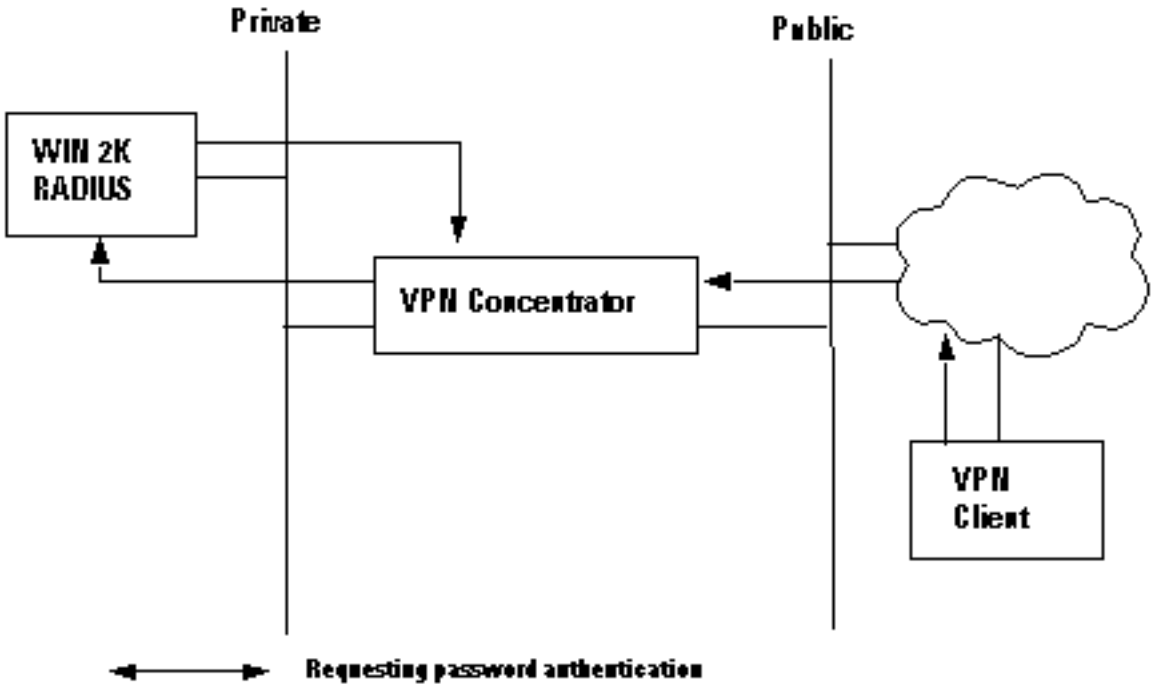
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Uso de un servidor RADIUS de Windows 2000 para autenticar un cliente VPN de Cisco

Puede utilizar un servidor RADIUS de Windows 2000 para autenticar un usuario de VPN Client. En el siguiente escenario (el VPN Client solicita autenticación), el VPN 3000 Concentrator recibe una solicitud del VPN Client que contiene el nombre de usuario y la contraseña del cliente. Antes de enviar el nombre de usuario/contraseña a un servidor RADIUS de Windows 2000 en la red privada para su verificación, el concentrador VPN lo bloquea, usando el algoritmo HMAC/MD5.

El servidor RADIUS de Windows 2000 requiere PAP para autenticar una sesión de VPN Client. Para habilitar el servidor RADIUS para autenticar a un usuario de VPN Client, verifique el parámetro **Autenticación no cifrada (PAP, SPAP)** en la ventana **Edit Dial-in Profile** (de forma predeterminada, este parámetro no está activado). Para establecer este parámetro, seleccione la **Política de acceso remoto** que está utilizando, seleccione **Propiedades** y seleccione la pestaña **Autenticación**.

Tenga en cuenta que la palabra *Unencryption* en el nombre de este parámetro es engañosa. El uso de este parámetro *no* causa una violación de la seguridad, porque cuando el VPN Concentrator envía el paquete de autenticación al servidor RADIUS, no envía la contraseña en el clear . El concentrador VPN recibe el nombre de usuario/la contraseña y los paquetes cifrados del cliente VPN, y realiza un hash HMAC/MD5 en la contraseña antes de enviar el paquete de autenticación al servidor.




## Uso de un servidor RADIUS que no admite MSCHAP

Algunos servidores RADIUS no admiten autenticación de usuario MSCHAPv1 o MSCHAPv2. Si utiliza un servidor RADIUS que no admite MSCHAP (v1 o v2), debe configurar el protocolo de autenticación PPTP del grupo base para utilizar PAP y/o CHAP y también inhabilitar las opciones MSCHAP. Ejemplos de servidores RADIUS que no soportan MSCHAP son el servidor Livingston v1.61 RADIUS o cualquier servidor RADIUS basado en el código Livingston.

**Nota:** Sin MSCHAP, los paquetes hacia y desde los clientes PPTP *no* se *cifrarán*.

## Uso de encripción con PPTP

Para utilizar el cifrado con PPTP, un servidor RADIUS debe admitir la autenticación MSCHAP y debe enviar el atributo de devolución MSCHAP-MPPE-Keys para cada autenticación de usuario. A continuación se muestran ejemplos de servidores RADIUS que admiten este atributo.

- Cisco Secure ACS para Windows: versión 2.6 o posterior
- Steel-Belted RADIUS de Funk Software
- Paquete de opciones de servidor de Microsoft Internet Authentication Server en NT 4.0
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server — Servidor de autenticación de Internet

## Información Relacionada

- Página de soporte de RADIUS
- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec

- Página de soporte de PPTP
- RFC 2637: Protocolo de Tunelización punto a Punto (PPTP)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems