Usando los servidores de RADIUS con los Productos VPN 3000

Contenido

Introducción

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

- El servidor de RADIUS del Windows 2000 requiere el protocolo password authentication (PAP) para autenticar a un Cliente Cisco VPN. (Clientes IPSec)
- Usando un servidor de RADIUS que no soporte el protocolo microsoft challenge handshake authentication (MSCHAP) requiere las opciones MSCHAP de ser inhabilitado en el concentrador VPN 3000. (Del protocolo de túnel punto a punto clientes [PPTP])
- Usando el cifrado con el PPTP requiere las Claves del MSCHAP MPPE de vuelta del atributo del RADIUS. (Clientes PPTP)
- Con Windows 2003, el v2 MS-CHAP puede ser utilizado, pero el método de autentificación se debe fijar como “RADIUS con el vencimiento”.

Algunas de estas notas han aparecido en los Release Note del producto.

Antes de comenzar

Convenciones

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

prerrequisitos

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

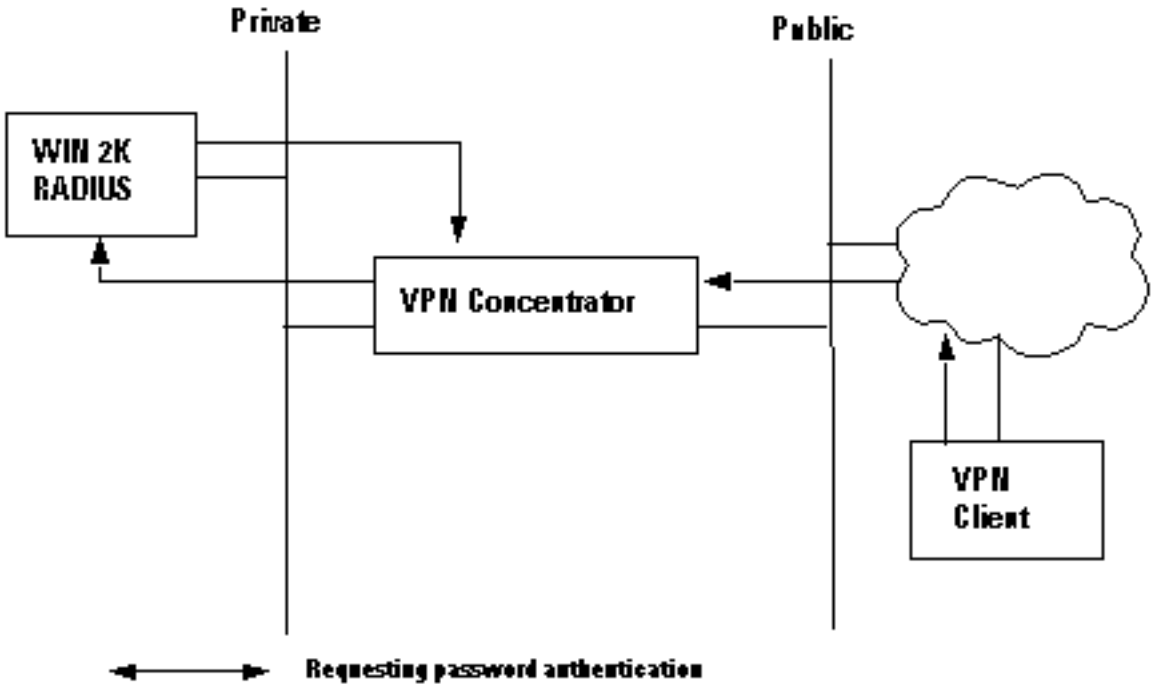
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Usando un servidor de RADIUS del Windows 2000 para autenticar a un Cliente Cisco VPN

Usted puede utilizar a un servidor de RADIUS del Windows 2000 para autenticar a un usuario de cliente VPN. En el escenario siguiente (el cliente VPN está pidiendo la autenticación), el concentrador VPN 3000 recibe una petición del cliente VPN que contiene el nombre de usuario y contraseña del usuario de cliente. Antes de enviar el nombre de usuario/la contraseña a un servidor de RADIUS del Windows 2000 en la red privada para la verificación, el concentrador VPN la desmenuza, usando el algoritmo HMAC/MD5.

El servidor de RADIUS del Windows 2000 requiere el PAP para autenticar una sesión de cliente VPN. Para permitir al servidor de RADIUS para autenticar a un usuario de cliente VPN, marque el parámetro **Unencrypted de la autenticación (PAP, SPAP)** en la ventana del **perfil del dial-in del editar** (por abandono, este parámetro no se marca). Para fijar este parámetro, seleccionar la **política de acceso remoto que** usted está utilizando, las **propiedades** selectas, y selecciona la lengueta de la **autenticación**.

Observe que la palabra *Unencrypted* en el este nombre de parámetro es engañosa. Usando este parámetro no causa a una falla de seguridad, porque cuando el concentrador VPN envía el paquete de autenticación al servidor de RADIUS, no envía la contraseña en el claro. El concentrador VPN recibe el nombre de usuario/la contraseña y los paquetes encriptados 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 de RADIUS no soportan la autenticación de usuario del MSCHAPv1 o del MSCHAPv2. Si usted está utilizando a un servidor de RADIUS que no soporte el MSCHAP (v1 o v2), usted debe configurar el protocolo de la autenticación PPTP del grupo base para utilizar el PAP y/o PARA AGRIETAR y también para inhabilitar las opciones MSCHAP. Los ejemplos de los servidores de RADIUS que no soportan el MSCHAP son el servidor de RADIUS de Livingston v1.61 o cualquier servidor de RADIUS basado en el código de Livingston.

Nota: Sin el MSCHAP, los paquetes a y desde los clientes PPTP no serán cifrados.

Uso de encripción con PPTP

Para utilizar el cifrado con el PPTP, un servidor de RADIUS debe soportar la autenticación de MSCHAP y debe enviar las Claves del MSCHAP MPPE de vuelta del atributo para cada autenticación de usuario. Los ejemplos de los servidores de RADIUS que soportan este atributo se muestran abajo.

- Cisco Secure ACS for Windows - versión 2.6 o posterior
- Steel-Belted RADIUS de Funk Software
- Servidor de autenticación de Internet de Microsoft en el paquete de las opciones del servidor NT4.0
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server -- Internet Authentication Server

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