Utilizando servidores RADIUS com produtos VPN 3000

Contents

Introduction

Este documento descreve certas advertências encontradas ao usar alguns servidores RADIUS com o VPN 3000 Concentrator e VPN Clients.

- O servidor RADIUS do Windows 2000 requer o PAP (Password Authentication Protocol) para autenticar um Cisco VPN Client. (clientes IPSec)
- Usar um servidor RADIUS que não suporta o Microsoft Challenge Handshake Authentication Protocol (MSCHAP) exige que as opções MSCHAP sejam desativadas no VPN 3000 Concentrator. (Clientes Point-to-Point Tunneling Protocol [PPTP])
- O uso da criptografia com PPTP requer o atributo return MSCHAP-MPPE-Keys do RADIUS. (clientes PPTP)
- Com o Windows 2003, o MS-CHAP v2 pode ser usado, mas o método de autenticação deve ser definido como "RADIUS com vencimento".

Algumas dessas notas apareceram nas notas de versão do produto.

Antes de Começar

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco VPN 3000 Concentrator
- Cisco VPN Client

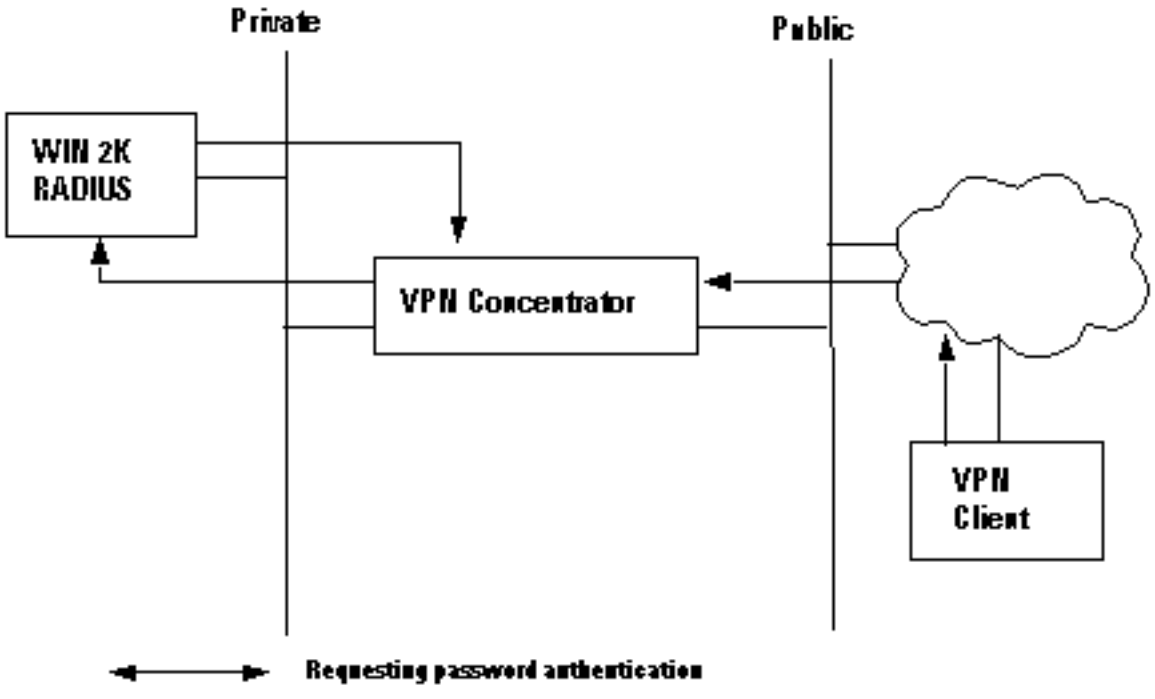
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Usando um servidor Windows 2000 RADIUS para autenticar um Cisco VPN Client

Você pode usar um servidor RADIUS do Windows 2000 para autenticar um usuário do VPN Client. No cenário a seguir (o VPN Client está solicitando autenticação), o VPN 3000 Concentrator recebe uma solicitação do VPN Client contendo o nome de usuário e a senha do cliente. Antes de enviar o nome de usuário/senha para um servidor RADIUS do Windows 2000 na rede privada para verificação, o VPN Concentrator o tem, usando o algoritmo HMAC/MD5.

O servidor RADIUS do Windows 2000 requer PAP para autenticar uma sessão de cliente VPN. Para permitir que o servidor RADIUS autentique um usuário do VPN Client, verifique o parâmetro **Autenticação não criptografada (PAP, SPAP)** na janela **Editar perfil de discagem** (por padrão, esse parâmetro não está marcado). Para definir esse parâmetro, selecione a **Diretiva de acesso remoto** que está usando, selecione **Propriedades** e selecione a guia **Autenticação**.

Note que a palavra *Não Criptografado* no nome deste parâmetro é enganosa. O uso desse parâmetro *não* causa uma violação de segurança, pois quando o VPN Concentrator envia o pacote de autenticação para o servidor RADIUS, ele não envia a senha em branco . O VPN Concentrator recebe o nome de usuário/senha e os pacotes criptografados do VPN Client e executa um hash HMAC/MD5 na senha antes de enviar o pacote de autenticação ao servidor.



Usando um servidor RADIUS que não suporte MSCHAP

Alguns servidores RADIUS não suportam autenticação de usuário MSCHAPv1 ou MSCHAPv2. Se estiver usando um servidor RADIUS que não suporta MSCHAP (v1 ou v2), você deve configurar o protocolo de autenticação PPTP do Grupo Base para usar PAP e/ou CHAP e também desativar as opções MSCHAP. Exemplos de servidores RADIUS que não suportam MSCHAP são o servidor RADIUS Livingston v1.61 ou qualquer servidor RADIUS baseado no código Livingston.

Observação: sem o MSCHAP, os pacotes de e para clientes PPTP *não* serão criptografados.

Utilizando criptografia com PPTP

Para usar a criptografia com PPTP, um servidor RADIUS deve suportar a autenticação MSCHAP e deve enviar o atributo return MSCHAP-MPPE-Keys para cada autenticação de usuário. Exemplos de servidores RADIUS que suportam esse atributo são mostrados abaixo.

- Cisco Secure ACS para Windows - versão 2.6 ou posterior
- Funk Software Steel-Belted RADIUS
- Pacote de opções do Microsoft Internet Authentication Server no NT 4.0 Server
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server — Internet Authentication Server

Informações Relacionadas

- Página de suporte RADIUS
- Cisco Secure ACS para página de suporte do Windows
- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Página de suporte do PPTP
- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems