

Using RADIUS Servers With VPN 3000 Products

Document ID: 5616

Contents

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Using a Windows 2000 RADIUS Server to Authenticate a Cisco VPN Client

Using a RADIUS Server That Does Not Support MSCHAP

Using Encryption With PPTP

Related Information

Introduction

This document describes certain caveats found when using some RADIUS servers with the VPN 3000 Concentrator and VPN Clients.

- Windows 2000 RADIUS server requires Password Authentication Protocol (PAP) for authenticating a Cisco VPN Client. (IPSec clients)
- Using a RADIUS server that does not support Microsoft Challenge Handshake Authentication Protocol (MSCHAP) requires MSCHAP options to be disabled on the VPN 3000 Concentrator. (Point-to-Point Tunneling Protocol [PPTP] clients)
- Using encryption with PPTP requires the return attribute MSCHAP-MPPE-Keys from RADIUS. (PPTP clients)
- With Windows 2003, MS-CHAP v2 can be used, but the authentication method should be set as "RADIUS with Expiry".

Some of these notes have appeared in product release notes.

Before You Begin

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- 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

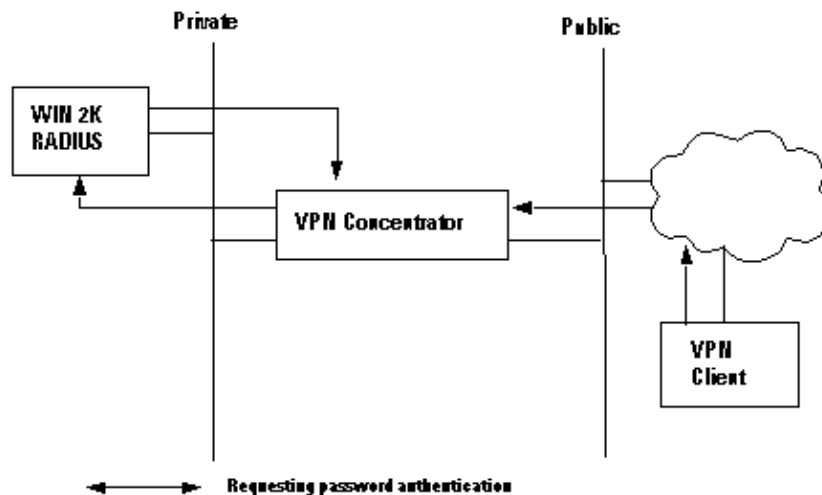
devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Using a Windows 2000 RADIUS Server to Authenticate a Cisco VPN Client

You can use a Windows 2000 RADIUS server to authenticate a VPN Client user. In the following scenario (the VPN Client is requesting authentication), the VPN 3000 Concentrator receives a request from the VPN Client containing the client user's username and password. Before sending the username/password to a Windows 2000 RADIUS server in the private network for verification, the VPN Concentrator hashes it, using the HMAC/MD5 algorithm.

The Windows 2000 RADIUS server requires PAP for authenticating a VPN Client session. To enable the RADIUS server to authenticate a VPN Client user, check the **Unencrypted Authentication (PAP, SPAP)** parameter on the **Edit Dial-in Profile** window (by default, this parameter is not checked). To set this parameter, select the **Remote Access Policy** you are using, select **Properties**, and select the **Authentication** tab.

Note that the word *Unencrypted* on this parameter's name is misleading. Using this parameter does *not* cause a breach of security, because when the VPN Concentrator sends the authentication packet to the RADIUS server, it does not send the password in the clear. The VPN Concentrator receives the username/password and encrypted packets from the VPN Client, and performs an HMAC/MD5 hash on the password before sending the authentication packet to the server.



Using a RADIUS Server That Does Not Support MSCHAP

Some RADIUS servers do not support MSCHAPv1 or MSCHAPv2 user authentication. If you are using a RADIUS server that does not support MSCHAP (v1 or v2), you must configure the Base Group's PPTP authentication protocol to use PAP and/or CHAP and also disable the MSCHAP options. Examples of RADIUS servers that do not support MSCHAP are the Livingston v1.61 RADIUS server or any RADIUS server based on Livingston code.



Note: Without MSCHAP, packets to and from PPTP Clients will *not* be encrypted.

Using Encryption With PPTP

To use encryption with PPTP, a RADIUS server must support MSCHAP authentication and must send the return attribute MSCHAP–MPPE–Keys for every user authentication. Examples of RADIUS servers that support this attribute are shown below.

- Cisco Secure ACS for Windows – version 2.6 or later
- Funk Software Steel–Belted RADIUS
- Microsoft Internet Authentication Server on NT 4.0 Server Options Pack
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server – Internet Authentication Server

Related Information

- [RADIUS Support Page](#)
- [RADIUS in IOS Documentation](#)
- [Documentation for Cisco Secure ACS for Windows](#)
- [Cisco Secure ACS for Windows Support Page](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [PPTP Support Page](#)
- [RFC 2637: Point–to–Point Tunneling Protocol \(PPTP\)](#) 
- [Requests for Comments \(RFCs\)](#) 
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 14, 2005

Document ID: 5616
