

Configuring the Cisco VPN 3000 Concentrator for Microsoft Windows 2000 Support

Document ID: 5757

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

How to Configure the VPN 3000 for Windows 2000 Support

Related Information

Introduction

This document demonstrates how to configure the VPN 3000 Concentrator for Windows 2000 support.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

- This document assumes that you are using digital certificates for authentication and that you are adding Windows 2000 support to a working configuration.
- Before you begin this procedure, you should review the documentation on configuring digital certificates. Refer to **Administration > Certificate Management** in the VPN 3000 Concentrator Series User Guide and select VPN Concentrator User Guides.

Components Used

The information in this document is based on the Cisco VPN 3000 Concentrator series.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

How to Configure the VPN 3000 for Windows 2000 Support

Follow the instructions provided below to configure the VPN 3000 Concentrator.

1. Go to **Configuration > User Management > Groups** and click **Add Group**.
 - a. Enter a Group Name and a Password. The Group Name must be the same as the Organizational Unit (OU) field in the Windows 2000 Client's digital certificate. The Password is not used so you can set it to anything you choose.
 - b. On the General tab, select Tunneling Protocols = **L2TP over IPSec**.

- c. On the IPsec tab, select IPsec SA = **ESP-L2TP-TRANSPORT**, Authentication = **None**, and Mode Configuration = **None** (unchecked).
 2. Go to **Configuration > System > Tunneling Protocols > IPsec > IKE Proposals** and activate the IKE-3DES-MD5-RSA or IKE-3DES-SHA-DSA proposal depending on the client certificate type (RSA or DSA). Move the proposal to the top of the list.
 3. Go to **Configuration > Policy Management > Traffic Management > Security Associations**. Select **ESP-L2TP-TRANSPORT** and click **Modify**. Under Digital Certificate, click the drop-down menu and select the certificate you created for the VPN Concentrator.
-

Related Information

- [VPN 3000 Product Documentation](#)
 - [Cisco VPN 3000 Concentrator Support Page](#)
 - [Cisco VPN 3000 Client Support Page](#)
 - [IP Security \(IPsec\) Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 5757
