

Using VPN with the Cisco Aironet Base Station

Document ID: 21502

Introduction

Prerequisites

Requirements

Components Used

Conventions

Set Up VPN

IP Security

Adjust the MTU

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

Cisco Aironet Base Stations (BSM and BSE models) provide home users and small offices with wireless connectivity to an intranet or the Internet. The Base Station Ethernet (BSE) model, with an Ethernet RJ-45 port, can be connected to the Internet by digital subscriber line (DSL) or cable modem. The Base Station Modem (BSM) model is equipped with an integrated 56k v.90 dialup modem that enables multiple computers to access the Internet through the legacy phone system.

A typical use of the Base Station unit is to access the Internet over either cable or DSL connection in conjunction with Virtual Private Networking (VPN) technology to provide quick and secure access to the company network.

It is easy to set up the Base Station unit with the Base Station Client Utility (BSCU). This document shows how to set up the unit for use with VPN.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- VPN network operation
- Base Station configuration

Components Used

The information in this document is based on the Cisco Aironet Base Station (BSM and BSE models).

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.

Conventions

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

Set Up VPN

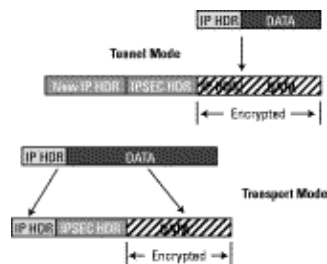
IP Security

The first step in VPN setup is to accommodate for the use of the IP Security (IPSec) technology, which is incorporated within the VPN technology. IPSec uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network.

IPSec defines a new set of headers that are added to IP datagrams. These headers are placed after the IP header and before the Layer 4 protocol (typically Transmission Control Protocol [TCP] or User Datagram Protocol [UDP]). The result is that the packets go from the local network where the PC is installed through to the internet. These packets are a larger size than non-encrypted packets. The increased size can cause problems to devices that expect normal size packets, because the receiving devices see them as oversized packets.

Figure 1 shows how the IPSec header fits within a normal packet.

Figure 1 IPSec Header



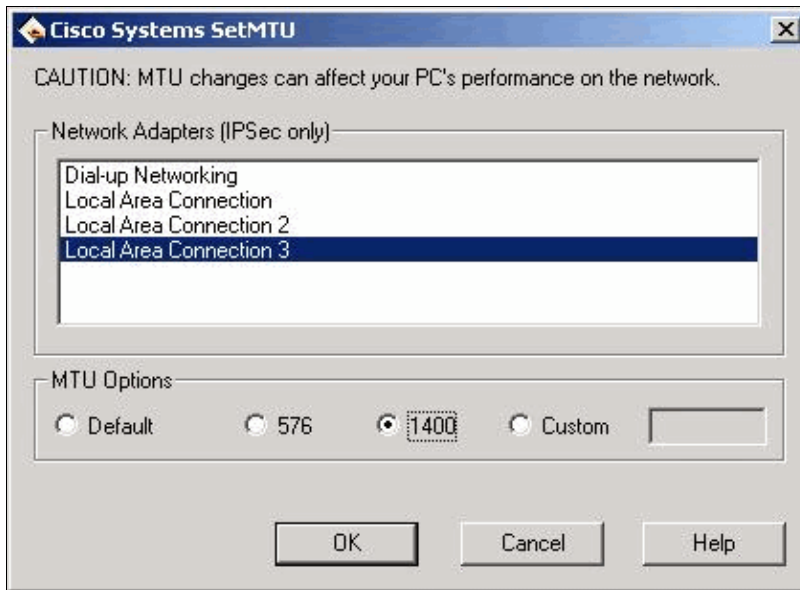
Adjust the MTU

In order to ensure that receiving devices do not perceive the packets as oversized, you must adjust the size of the Maximum Transmission Unit (MTU) on the PC/host side. Adjust the total maximum size that the packet can take so that it does not exceed the normal size of a non encrypted Ethernet packet. VPN applications typically provides the option to customize the MTU size.

Complete these steps to adjust the MTU in a Cisco Systems VPN client within Microsoft Windows:

1. Choose **Start > Programs > Cisco Systems VPN Client > Set MTU**. This window opens:

Figure 2



2. Select the wireless client adapter that you use to connect to your Base Station unit (in the example shown in Figure 2, Local Area Connection 3).
3. Under **MTU Options**, click the **1400** radio button, and then click **OK**. This causes your PC to transmit packets with 1400 bytes as the maximum. Therefore, the additional IPSec header is accommodated, but the 1518 byte normal maximum size of an Ethernet packet is not exceeded.

Note: The statement that "MTU changes can affect your PC's performance on the network" refers to the fact that because of the smaller MTU size, two packets are required to send the data previously contained in a single non-encrypted frame.

For details on how to configure your Base Station unit for PPP over Ethernet (PPPoE) and Cable/DSL, refer to Configuring the BSE342 and BSM342 Base Stations.

Note: Point-to-Point Tunneling Protocol (PPTP) is not supported

Note: Install the wireless card *before* the VPN client is installed. If necessary remove both, then reinstall the card followed by the VPN. Although this was an issue in the Cisco 2.x release of the VPN client, it was fixed in the later revisions.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless
Wireless – Mobility: WLAN Radio Standards
Wireless – Mobility: Security and Network Management
Wireless – Mobility: Getting Started with Wireless
Wireless – Mobility: General

Related Information

- [Configuring the BSE342 and BSM342 Base Stations](#)
 - [Cisco Aironet 340 Series Tech Notes](#)
 - [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 31, 2006

Document ID: 21502
