

Utilizando o VPN com a estação base Cisco Aironet

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar VPN](#)

[Segurança de IP](#)

[Ajuste a MTU](#)

[Informações Relacionadas](#)

Introduction

As Cisco Aironet Base Stations (modelos BSM e BSE) fornecem aos usuários domésticos e aos pequenos escritórios conectividade sem fio a uma intranet ou à Internet. O modelo Ethernet de estação base (BSE), com uma porta Ethernet RJ-45, pode ser conectado à Internet por linha de assinante digital (DSL - Digital Subscriber Line) ou modem a cabo. O modelo BSM (Base Station Modem) é equipado com um modem de discagem 56k v.90 integrado que permite que vários computadores acessem a Internet através do sistema telefônico herdado.

Um uso típico da unidade da estação base é acessar a Internet por conexão via cabo ou DSL em conjunto com a tecnologia VPN (Virtual Private Networking) para fornecer acesso rápido e seguro à rede da empresa.

É fácil configurar a unidade de estação base com o BSCU (Base Station Client Utility, utilitário cliente de estação base). Este documento mostra como configurar a unidade para uso com VPN.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- operação de rede VPN
- Configuração da estação base

Componentes Utilizados

As informações neste documento são baseadas nos modelos Cisco Aironet Base Station (BSM e BSE).

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](#).

Configurar VPN

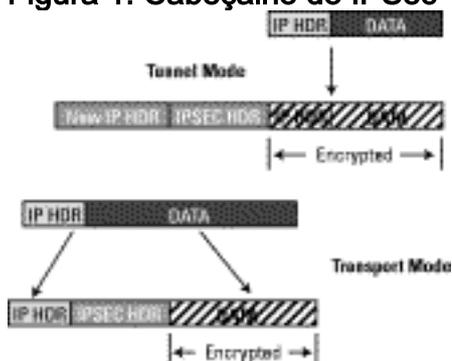
Segurança de IP

A primeira etapa na configuração da VPN é acomodar o uso da tecnologia IPsec (IP Security), incorporada na tecnologia VPN. O IPsec usa tecnologia de criptografia para fornecer confidencialidade, integridade e autenticidade de dados entre os colegas participantes em uma rede privada.

O IPsec define um novo conjunto de cabeçalhos que são adicionados aos datagramas IP. Esses cabeçalhos são colocados após o cabeçalho IP e antes do protocolo de Camada 4 (geralmente Transmission Control Protocol [TCP] ou User Datagram Protocol [UDP]). O resultado é que os pacotes vão da rede local onde o PC está instalado para a Internet. Esses pacotes são de tamanho maior do que os pacotes não criptografados. O tamanho aumentado pode causar problemas aos dispositivos que esperam pacotes de tamanho normal, porque os dispositivos receptores os veem como pacotes de tamanho excessivo.

A Figura 1 mostra como o cabeçalho IPsec se encaixa em um pacote normal.

Figura 1: Cabeçalho do IPsec



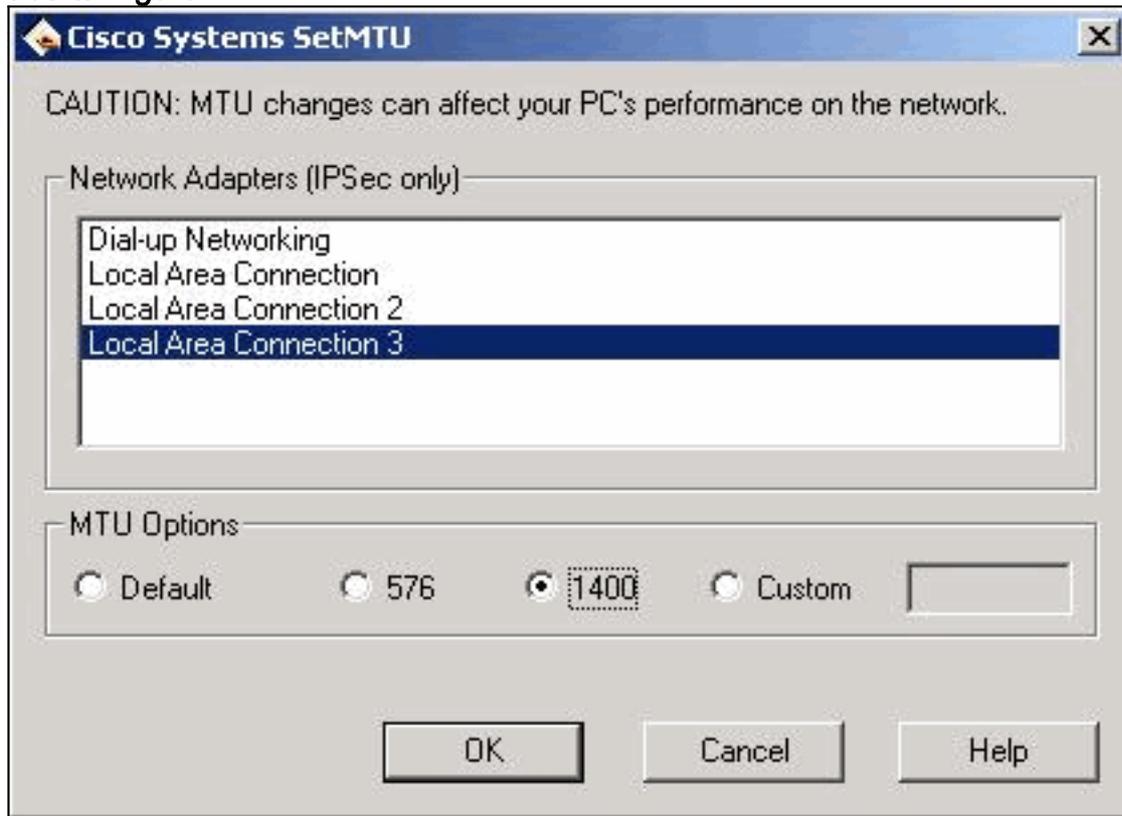
Ajuste a MTU

Para garantir que os dispositivos de recebimento não percebam os pacotes como superdimensionados, você deve ajustar o tamanho da MTU (Maximum Transmission Unit, Unidade Máxima de Transmissão) no lado PC/host. Ajuste o tamanho máximo total que o pacote pode tomar para que não exceda o tamanho normal de um pacote Ethernet não criptografado. Os aplicativos VPN normalmente oferecem a opção de personalizar o tamanho da MTU.

Conclua estes passos para ajustar a MTU em um cliente VPN da Cisco Systems no Microsoft

Windows:

1. Escolha **Iniciar > Programas > Cisco Systems VPN Client > Definir MTU**. Esta janela é aberta: **Figure 2**



2. Selecione o adaptador cliente sem fio que você usa para se conectar à sua unidade de estação base (no exemplo mostrado na Figura 2, Conexão de área local 3).
3. Em **MTU Options**, clique no botão de opção **1400** e clique em **OK**. Isso faz com que o PC transmita pacotes com 1400 bytes no máximo. Portanto, o cabeçalho IPSec adicional é acomodado, mas o tamanho máximo normal de 1518 bytes de um pacote Ethernet não é excedido.

Observação: a declaração de que "alterações de MTU podem afetar o desempenho do PC na rede" refere-se ao fato de que, devido ao tamanho de MTU menor, dois pacotes são necessários para enviar os dados previamente contidos em um único quadro não criptografado.

Para obter detalhes sobre como configurar sua unidade de estação base para PPP sobre Ethernet (PPPoE) e Cabo/DSL, consulte [Configuração das Estações de Base BSE342 e BSM342](#).

Observação: o PPTP (Point-to-Point Tunneling Protocol) não é suportado

Observação: instale a placa sem fio *antes* de instalar o cliente VPN. Se necessário, remova ambos e reinstale a placa seguida pela VPN. Embora esse tenha sido um problema na versão Cisco 2.x do cliente VPN, ele foi corrigido nas revisões posteriores.

[Informações Relacionadas](#)

- [Configurando as estações de base BSE342 e BSM342](#)
- [Notas técnicas do Cisco Aironet 340 Series](#)
- [Suporte Técnico - Cisco Systems](#)