

Utilizando o VPN com a estação base Cisco Aironet

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[VPN estabelecido](#)

[Segurança de IP](#)

[Ajuste o MTU](#)

[Informações Relacionadas](#)

Introdução

As estações base do Cisco Aironet (modelos BSM e BSE) fornecem utilizadores domésticos e escritórios pequenos a conectividade Wireless a um intranet ou ao Internet. O modelo do Base Station Ethernet (BSE), com uma porta dos Ethernet RJ-45, pode ser conectado ao Internet pelo digital subscriber line (DSL) ou pelo modem a cabo. O modelo do Base Station Modem (BSM) é equipado com um modem dialup integrado 56K v.90 que permita computadores múltiplos de alcançar o Internet através do sistema de telefone legado.

Um uso típico da unidade de estação de base é alcançar o Internet sobre o cabo ou a conexão DSL conjuntamente com a tecnologia do Virtual Private Networking (VPN) para fornecer rapidamente e o acesso seguro à rede de empresa.

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

Pré-requisitos

Requisitos

Os leitores deste documento devem estar cientes destes tópicos:

- Operação da rede VPN
- Configuração de estação base

Componentes Utilizados

A informação neste documento é baseada na estação base do Cisco Aironet (modelos BSM e BSE).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Estabelecer o VPN

Segurança de IP

A primeira etapa na instalação VPN é acomodar para o uso da tecnologia da Segurança IP (IPsec), que é incorporada dentro da tecnologia de VPN. O IPsec usa a tecnologia de criptografia para fornecer a confidencialidade de dados, a integridade, e a autenticidade entre peer participantes em uma rede privada.

O IPsec define um novo conjunto de cabeçalho que é adicionado às datagramas IP. Estes encabeçamentos são colocados após o cabeçalho IP e antes do protocolo da camada 4 (tipicamente [TCP] do protocolo Protocolo de control de transmisión (TCP) ou [UDP] do protocolo de datagrama de usuário). O resultado é que os pacotes vão da rede local onde o PC é instalado completamente ao Internet. Estes pacotes são um tamanho maior do que pacotes não codificados. O tamanho crescente pode causar problemas aos dispositivos que esperam pacotes de tamanho normal, porque os dispositivos receptores os veem como pacotes grandes demais.

Figura 1 mostra como os ajustes do cabeçalho IPsec dentro de um pacote normal.

Figura 1 – Cabeçalho IPsec

Ajuste o MTU

A fim assegurar-se de que os dispositivos receptores não percebam os pacotes como desproporcionados, você deve ajustar o tamanho da unidade de transmissão máxima (MTU) no lado PC/host. Ajuste o tamanho máximo total que o pacote pode tomar de modo que não exceda o tamanho normal de um pacote de Ethernet não cifrado. Os aplicativos VPN fornecem tipicamente a opção para personalizar o tamanho do MTU.

Termine estas etapas para ajustar o MTU em um Cisco Systems VPN client dentro de Microsoft Windows:

1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > Definir MTU**. Este indicador abre: **Figura 2**
2. Selecione o adaptador de cliente Wireless que você se usa para conectar a sua unidade de estação de base (no exemplo mostrado em figura 2, na conexão de área local 3).
3. Sob **opções MTU**, clique o botão de rádio **1400**, e clique então a **APROVAÇÃO**. Isto faz com que seu PC transmita pacotes com 1400 bytes como o máximo. Consequentemente, o

cabeçalho IPSec adicional é acomodado, mas o tamanho máximo normal de 1518 bytes de um pacote de Ethernet não é excedido.

Nota: A indicação que o “MTU muda pode afetar o desempenho do seu PC na rede” refere o fato que devido ao tamanho do MTU menor, dois pacotes é exigido para enviar os dados contidos previamente em um único quadro NON-cifrado.

Para detalhes em como configurar sua unidade de estação de base para o PPP over Ethernet (PPPoE) e o Cabo/DSL, refira [configurar as estações base BSE342 e BSM342](#).

Nota: O Point-to-Point Tunneling Protocol (PPTP) não é apoiado

Nota: Instale a placa Wireless *antes que* o cliente VPN esteja instalado. Caso necessário remova ambos, a seguir reinstale o cartão seguido pelo VPN. Embora esta fosse uma edição na liberação de Cisco 2.x do cliente VPN, foi fixado nas revisões mais atrasadas.

[Informações Relacionadas](#)

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