

Uso de la VPN con la estación base Aironet de Cisco.

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración de VPN](#)

[Seguridad IP](#)

[Ajuste de la MTU](#)

[Información Relacionada](#)

Introducción

Las estaciones base Cisco Aironet (modelos BSM y BSE) proporcionan a los usuarios domésticos y a las oficinas pequeñas conectividad inalámbrica a una intranet o a Internet. El modelo Ethernet (BSE) de estación base, con un puerto Ethernet RJ-45, se puede conectar a Internet mediante la línea de suscriptor digital (DSL) o el cable módem. El modelo Base Station Modem (BSM) está equipado con un módem de marcación manual 56k v.90 integrado que permite a varios ordenadores acceder a Internet a través del sistema telefónico antiguo.

Un uso típico de la unidad Base Station es el acceso a Internet a través de una conexión por cable o DSL junto con la tecnología de red privada virtual (VPN) para proporcionar un acceso rápido y seguro a la red de la empresa.

Es fácil configurar la unidad Base Station con la utilidad Base Station Client (BSCU). Este documento muestra cómo configurar la unidad para su uso con VPN.

Prerequisites

Requirements

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- operación de red VPN
- Configuración de estación base

Componentes Utilizados

La información de este documento se basa en la base Cisco Aironet (modelos BSM y 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.

Convenciones

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Configuración de VPN

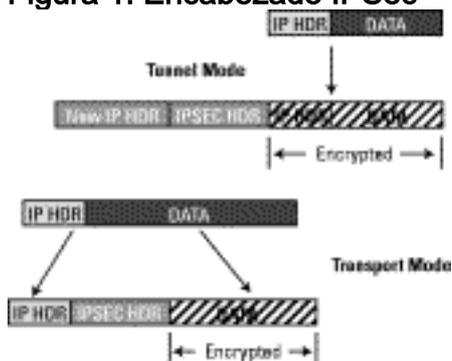
Seguridad IP

El primer paso en la configuración de VPN es adaptarse al uso de la tecnología IP Security (IPSec), que se incorpora en la tecnología VPN. IPSec utiliza tecnología de cifrado para proporcionar confidencialidad, integridad y autenticidad de los datos entre los pares participantes en una red privada.

IPSec define un nuevo conjunto de encabezados que se agregan a los datagramas IP. Estos encabezados se colocan después del encabezado IP y antes del protocolo de la capa 4 (normalmente el protocolo de control de transmisión [TCP] o el protocolo de datagramas de usuario [UDP]). El resultado es que los paquetes van desde la red local donde se instala el PC a través de Internet. Estos paquetes tienen un tamaño mayor que los paquetes no cifrados. El mayor tamaño puede causar problemas a los dispositivos que esperan paquetes de tamaño normal, porque los dispositivos receptores los ven como paquetes de tamaño excesivo.

La figura 1 muestra cómo el encabezado IPSec encaja dentro de un paquete normal.

Figura 1: Encabezado IPSec

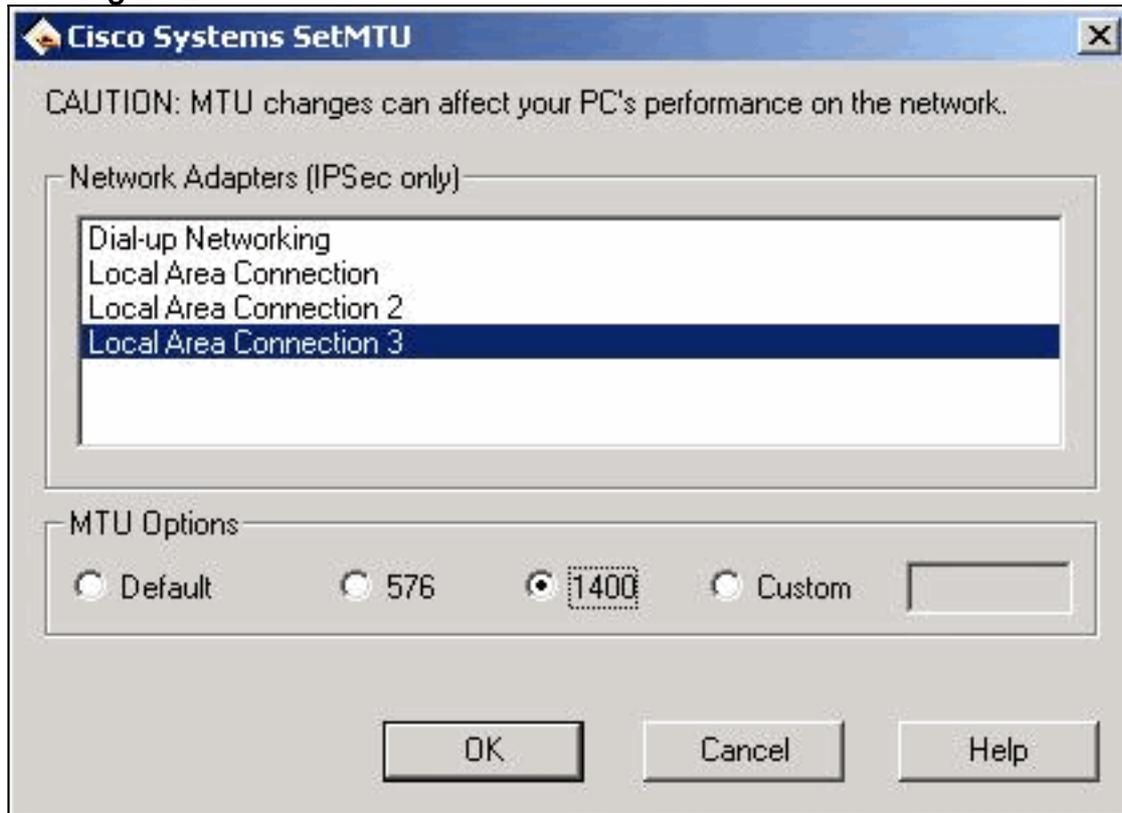


Ajuste de la MTU

Para asegurarse de que los dispositivos de recepción no perciben los paquetes como de tamaño excesivo, debe ajustar el tamaño de la unidad de transmisión máxima (MTU) en el lado de PC/host. Ajuste el tamaño máximo total que el paquete puede tomar para que no exceda el tamaño normal de un paquete Ethernet no cifrado. Las aplicaciones VPN normalmente proporcionan la opción de personalizar el tamaño de la MTU.

Complete estos pasos para ajustar la MTU en un cliente Cisco Systems VPN dentro de Microsoft Windows:

1. Elija Inicio > Programas > Cisco Systems VPN Client > Set MTU. Esta ventana se abre: **Figure 2**



2. Seleccione el adaptador de cliente inalámbrico que utiliza para conectarse a la unidad de estación base (en el ejemplo que se muestra en la figura 2, Conexión de área local 3).
3. En **Opciones de MTU**, haga clic en el botón de radio **1400** y luego haga clic en **Aceptar**. Esto hace que su PC transmita paquetes con 1400 bytes como máximo. Por lo tanto, se admite el encabezado IPsec adicional, pero no se supera el tamaño máximo normal de 1518 bytes de un paquete Ethernet.

Nota: La declaración de que "los cambios de la MTU pueden afectar el rendimiento de su PC en la red" se refiere al hecho de que debido al menor tamaño de la MTU, se necesitan dos paquetes para enviar los datos que anteriormente estaban contenidos en una única trama no cifrada.

Para obtener detalles sobre cómo configurar la unidad de estación base para PPP sobre Ethernet (PPPoE) y Cable/DSL, refiérase a [Configuración de las Estaciones Base BSE342 y BSM342](#).

Nota: No se admite el protocolo de túnel punto a punto (PPTP)

Nota: Instale la tarjeta inalámbrica *antes* de que el cliente VPN esté instalado. Si es necesario, quite ambas, vuelva a instalar la tarjeta seguida de la VPN. Aunque este fue un problema en la versión 2.x de Cisco del cliente VPN, se corrigió en las revisiones posteriores.

[Información Relacionada](#)

- [Configuración de las estaciones base BSE342 y BSM342](#)
- [Notas técnicas de la serie Cisco aironet 340](#)
- [Soporte Técnico - Cisco Systems](#)