Utilisation de VPN avec la station d'accueil Cisco Aironet

Contenu

Introduction

Les stations de base Cisco Aironet (modèles BSM et ESB) fournissent aux utilisateurs à domicile et aux petits bureaux une connectivité sans fil à un intranet ou à Internet. Le modèle Ethernet de station de base (ESB), doté d'un port Ethernet RJ-45, peut être connecté à Internet par DSL (Digital Subscriber Line) ou par modem câble. Le modèle BSM (Base Station Modem) est équipé d'un modem commuté 56 000 v.90 intégré qui permet à plusieurs ordinateurs d'accéder à Internet via le système téléphonique existant.

Une utilisation typique de l'unité de la station d'accueil consiste à accéder à Internet via une connexion câblée ou DSL en conjonction avec la technologie VPN (Virtual Private Networking) pour fournir un accès rapide et sécurisé au réseau de l'entreprise.

Il est facile de configurer l'unité de la station d'accueil à l'aide de l'utilitaire client de la station d'accueil (BSCU). Ce document montre comment configurer l'unité pour une utilisation avec VPN.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Fonctionnement du réseau VPN
- Configuration de la station de base

Components Used

Les informations de ce document sont basées sur la station de base Cisco Aironet (modèles BSM et ESB).

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.

Configuration du VPN

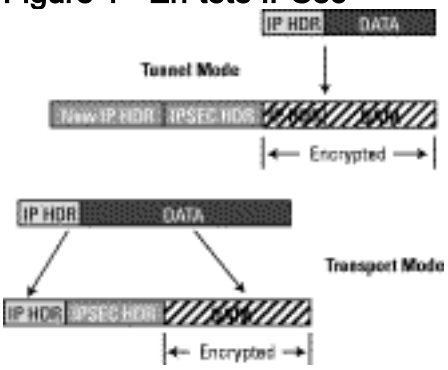
Sécurité IP

La première étape de la configuration VPN consiste à prendre en charge l'utilisation de la technologie IPSec (IP Security), qui est intégrée à la technologie VPN. IPSec utilise la technologie de cryptage pour assurer la confidentialité, l'intégrité et l'authenticité des données entre les homologues participants d'un réseau privé.

IPSec définit un nouvel ensemble d'en-têtes ajoutés aux datagrammes IP. Ces en-têtes sont placés après l'en-tête IP et avant le protocole de couche 4 (généralement TCP [Transmission Control Protocol] ou UDP [User Datagram Protocol]). Le résultat est que les paquets vont du réseau local où le PC est installé à Internet. Ces paquets sont de plus grande taille que les paquets non chiffrés. L'augmentation de la taille peut causer des problèmes aux périphériques qui s'attendent à des paquets de taille normale, parce que les périphériques de réception les considèrent comme des paquets surdimensionnés.

La Figure 1 montre comment l'en-tête IPSec s'insère dans un paquet normal.

Figure 1 - En-tête IPSec



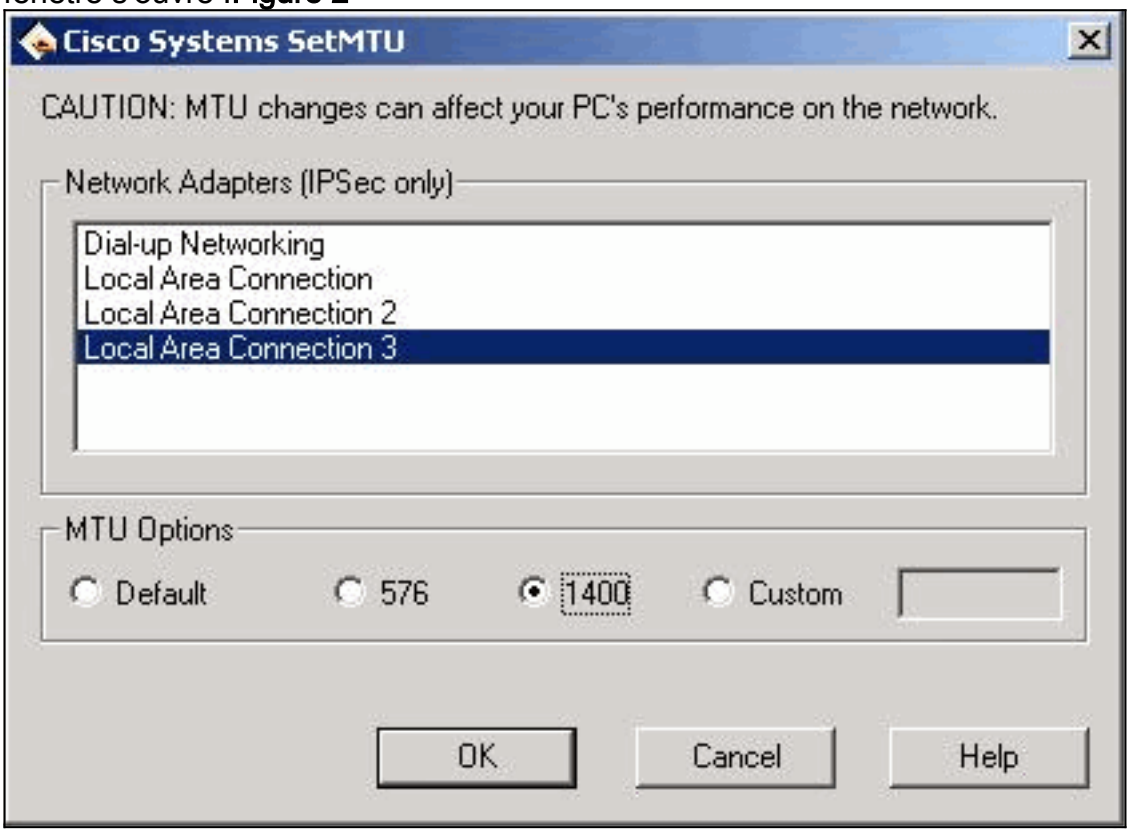
Ajuster la MTU

Afin de vous assurer que les périphériques de réception ne perçoivent pas les paquets comme surdimensionnés, vous devez ajuster la taille de l'unité de transmission maximale (MTU) côté PC/hôte. Ajustez la taille maximale totale que le paquet peut prendre afin qu'elle ne dépasse pas la taille normale d'un paquet Ethernet non chiffré. Les applications VPN offrent généralement la possibilité de personnaliser la taille de MTU.

Complétez ces étapes pour ajuster le MTU dans un client VPN Cisco Systems dans Microsoft

Windows :

1. Choisissez **Démarrer > Programmes > Cisco Systems VPN Client > Définir MTU**. Cette fenêtre s'ouvre :**Figure 2**



2. Sélectionnez l'adaptateur client sans fil que vous utilisez pour vous connecter à votre unité de station d'accueil (dans l'exemple illustré à la Figure 2, Connexion au réseau local 3).
3. Sous **Options MTU**, cliquez sur la case d'option **1400**, puis sur **OK**. Votre PC transmet ainsi des paquets avec 1 400 octets maximum. Par conséquent, l'en-tête IPSec supplémentaire est pris en charge, mais la taille maximale normale de 1 518 octets d'un paquet Ethernet n'est pas dépassée.

Remarque : l'instruction « Les modifications MTU peuvent affecter les performances de votre ordinateur sur le réseau » fait référence au fait qu'en raison de la taille MTU plus petite, deux paquets sont nécessaires pour envoyer les données précédemment contenues dans une seule trame non cryptée.

Pour plus d'informations sur la configuration de votre unité de station de base pour PPP sur Ethernet (PPPoE) et Cable/DSL, reportez-vous à Configuration des stations de base ESB342 et BSM342.

Remarque : le protocole PPTP (Point-to-Point Tunneling Protocol) n'est pas pris en charge

Remarque : installez la carte sans fil *avant* d'installer le client VPN. Si nécessaire, retirez les deux, puis réinstallez la carte suivie du VPN. Bien que cela ait été un problème dans la version 2.x de Cisco du client VPN, il a été corrigé dans les révisions ultérieures.

Informations connexes

- Configuration des stations de base BSE342 et BSM342
- Notes techniques de la gamme Cisco Aironet 340

- Support technique - Cisco Systems