Utilisation de VPN avec la station d'accueil Cisco Aironet

Contenu

Introduction

Les stations de base de Cisco Aironet (des modèles BSM et ESB) fournissent à des utilisateurs privés et à de petits bureaux la connexion sans fil à un intranet ou à l'Internet. Les Ethernets de station de base (ESB) modèlent, avec un port RJ45 d'Ethernets, peuvent être connectés à l'Internet par la ligne d'abonné numérique (DSL) ou le modem câble. Le modèle du modem de station de base (BSM) est équipé d'un modem commuté intégré 56K v.90 ce de plusieurs ordinateurs d'enables pour accéder à l'Internet par le système téléphonique existant.

Une utilisation typique de l'unité de station de base est d'accéder à l'Internet au-dessus de l'un ou l'autre de jonction de DSL ou câble en même temps que la technologie de la mise en réseau privé virtuel (VPN) pour fournir vite et l'accès sécurisé au réseau de société.

Il est facile d'installer l'unité de station de base avec l'utilitaire client de station de base (BSCU). Ce document affiche comment installer l'unité pour l'usage avec le VPN.

Conditions préalables

Conditions requises

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

- Exécution de réseau VPN
- Configuration de station de base

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Installation VPN

Sécurité IP

La première étape dans l'installation VPN est de faciliter pour l'usage de la technologie de sécurité IP (IPSec), qui est incorporée dans la technologie VPN. IPSec emploie la technologie de cryptage pour fournir la confidentialité des données, l'intégrité, et l'authenticité entre les pairs participants dans un réseau privé.

IPSec définit un nouvel ensemble d'en-têtes qui sont ajoutées aux datagrammes IP. Ces en-têtes sont placées après l'en-tête IP et avant le protocole de la couche 4 (typiquement Transmission Control Protocol [TCP] ou User Datagram Protocol [UDP]). Le résultat est que les paquets vont du réseau local où le PC est installé sur l'Internet. Ces paquets sont plus de grande taille les paquets que non chiffrés. La taille accrue peut poser des problèmes aux périphériques qui attendent les paquets normaux de taille, parce que les périphériques récepteurs les voient en tant que paquets surdimensionnés.

La figure 1 affiche comment les adaptations d'en-tête d'IPSec dans un paquet normal.

Figure 1 – En-tête d'IPSec

Ajustez le MTU

Afin de s'assurer que les périphériques récepteurs ne perçoivent pas les paquets comme surdimensionnés, vous devez ajuster la taille du Maximum Transmission Unit (MTU) du côté PC/host. Ajustez toute la taille maximale que le paquet peut prendre de sorte qu'il ne dépasse pas la taille normale d'un paquet Ethernet non chiffré. Les applications VPN fournit typiquement l'option de personnaliser la taille de MTU.

Terminez-vous ces étapes pour ajuster le MTU dans un client vpn de Cisco Systems dans Microsoft Windows :

1. Choisissez le **début > les programmes > le client vpn de Cisco Systems > placent le MTU**. Cette fenêtre s'ouvre :**Figure 2**
2. Sélectionnez l'adaptateur client sans fil que vous utilisez pour connecter à votre unité de station de base (dans l'exemple présenté dans la figure 2, connexion au réseau local 3).
3. Sous des **options de MTU**, cliquez sur la case d'option **1400**, et puis cliquez sur OK. Ceci fait transmettre votre PC des paquets avec 1400 octets comme maximum. Par conséquent, l'en-

tête supplémentaire d'IPSec est facilitée, mais la taille maximale normale de 1518 octets d'un paquet Ethernet n'est pas dépassée.

Remarque: La déclaration que le « MTU change peut affecter la représentation de votre PC sur le réseau » se rapporte au fait qui en raison de la taille plus petite de MTU, deux paquets sont exigés pour envoyer les données précédemment contenues dans une trame non chiffrée simple.

Pour des détails sur la façon dont configurer votre unité de station de base pour le PPP au-dessus des Ethernets (PPPoE) et de Cable/DSL, référez-vous à configurer les stations de base BSE342 et BSM342.

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

Remarque: Installez la carte Sans fil *avant que le* client vpn soit installé. S'il y a lieu retirez chacun des deux, puis réinstallez la carte suivie du VPN. Bien que c'ait été une question dans la release de Cisco 2.x du client vpn, il a été réparé dans les révisions postérieures.

Informations connexes

- Configuration des stations de base BSE342 et BSM342
- Notes en tech de Gamme Cisco Aironet 340
- Support technique - Cisco Systems