Verwenden von VPN mit der Cisco Aironet-Basisstation

Inhalt

Einführung

Cisco Aironet-Basisstationen (BSM- und BSE-Modelle) bieten Heimbenutzern und kleinen Büros Wireless-Verbindungen zum Intranet oder Internet. Das Base Station Ethernet-Modell (BSE) mit einem Ethernet RJ-45-Port kann über DSL (Digital Subscriber Line) oder Kabelmodem mit dem Internet verbunden werden. Das BSM-Modell (Base Station Modem) ist mit einem integrierten 56k v.90-Einwahlmodem ausgestattet, das mehreren Computern den Zugriff auf das Internet über das Legacy-Telefonsystem ermöglicht.

Eine typische Verwendung der Basisstation besteht darin, über Kabel- oder DSL-Verbindungen in Verbindung mit Virtual Private Networking (VPN)-Technologie auf das Internet zuzugreifen, um einen schnellen und sicheren Zugriff auf das Unternehmensnetzwerk zu ermöglichen.

Die Basisstation lässt sich mit dem Base Station Client Utility (BSCU) einfach einrichten. Dieses Dokument zeigt, wie Sie die Einheit für die Verwendung mit VPN einrichten.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten folgende Themen kennen:

- VPN-Netzwerkbetrieb
- Konfiguration der Basisstation

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Aironet-Basisstation (BSM- und BSE-Modelle).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

VPN einrichten

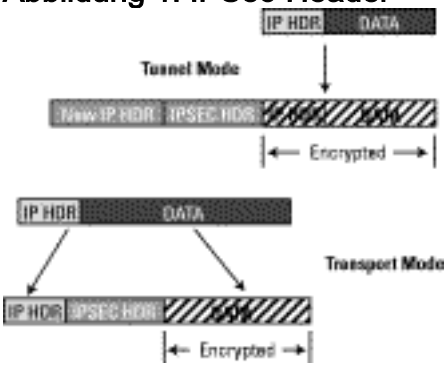
IP-Sicherheit

Der erste Schritt bei der VPN-Einrichtung besteht darin, die IP Security (IPSec)-Technologie, die in die VPN-Technologie integriert ist, zu nutzen. IPSec verwendet Verschlüsselungstechnologie, um Datensicherheit, Integrität und Authentizität zwischen den beteiligten Peers in einem privaten Netzwerk zu gewährleisten.

IPSec definiert einen neuen Satz von Headern, die IP-Datagrammen hinzugefügt werden. Diese Header werden nach dem IP-Header und vor dem Layer-4-Protokoll platziert (normalerweise Transmission Control Protocol [TCP] oder User Datagram Protocol [UDP]). Das Ergebnis ist, dass die Pakete vom lokalen Netzwerk, in dem der PC installiert ist, ins Internet übertragen werden. Diese Pakete sind größer als nicht verschlüsselte Pakete. Die höhere Größe kann Geräte, die normale Pakete erwarten, Probleme bereiten, da sie von den Empfangsgeräten als übergroße Pakete angesehen werden.

Abbildung 1 zeigt, wie der IPSec-Header in ein normales Paket passt.

Abbildung 1: IPSec-Header

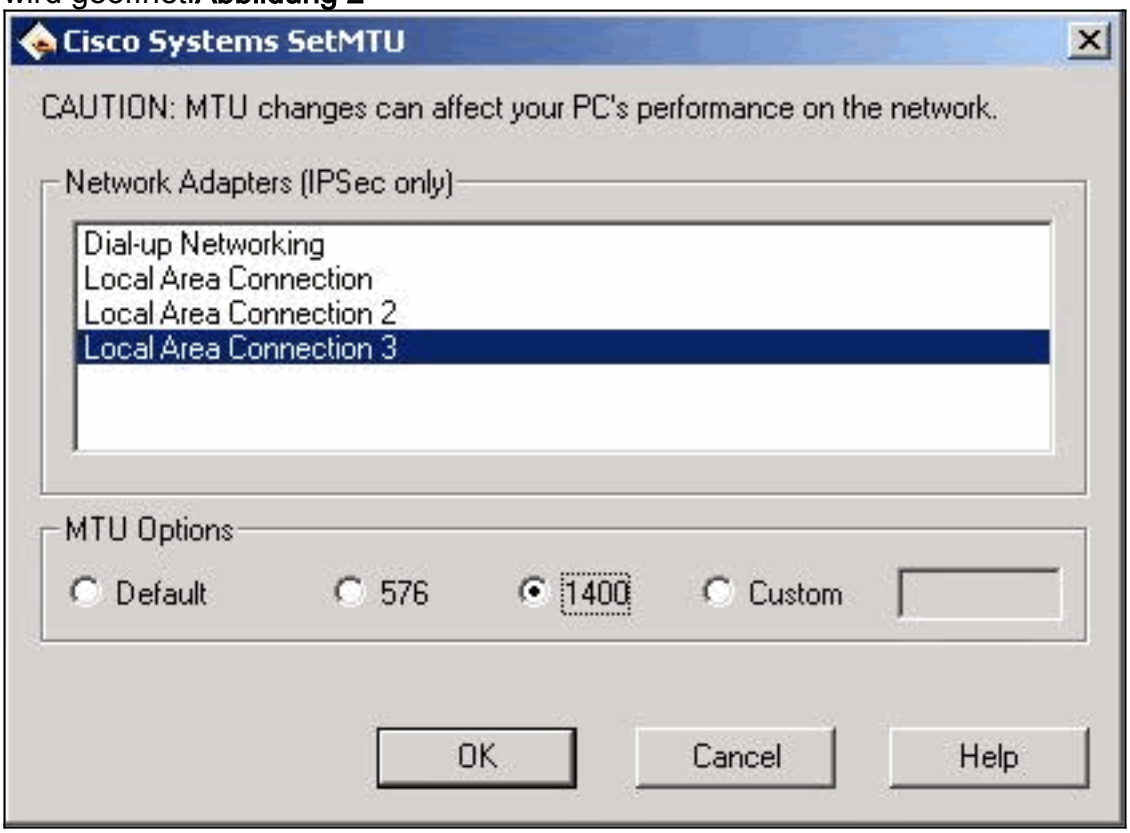


Ändern der MTU

Um sicherzustellen, dass die Empfangsgeräte die Pakete nicht als übergroß wahrnehmen, müssen Sie die Größe der Maximum Transmission Unit (MTU) auf PC-/Host-Seite anpassen. Passen Sie die maximale Gesamtgröße des Pakets an, sodass die normale Größe eines nicht verschlüsselten Ethernet-Pakets nicht überschritten wird. VPN-Anwendungen bieten in der Regel die Möglichkeit, die MTU-Größe anzupassen.

Gehen Sie wie folgt vor, um die MTU in einem Cisco Systems VPN Client in Microsoft Windows anzupassen:

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > Set MTU aus**. Dieses Fenster wird geöffnet:**Abbildung 2**



2. Wählen Sie den Wireless-Client-Adapter aus, den Sie für die Verbindung mit der Basisstation verwenden (im Beispiel in Abbildung 2, LAN-Verbindung 3).
3. Klicken Sie unter **MTU Options** auf das Optionsfeld **1400** und klicken Sie anschließend auf **OK**. Dies bewirkt, dass Ihr PC Pakete mit maximal 1400 Byte überträgt. Aus diesem Grund wird der zusätzliche IPSec-Header unterstützt, aber die normale maximale Größe von 1518 Byte eines Ethernet-Pakets wird nicht überschritten.

Hinweis: Die Aussage, dass MTU-Änderungen die Leistung Ihres PCs im Netzwerk beeinflussen können, bezieht sich auf die Tatsache, dass aufgrund der kleineren MTU-Größe zwei Pakete erforderlich sind, um die zuvor in einem einzigen nicht verschlüsselten Frame enthaltenen Daten zu senden.

Weitere Informationen zur Konfiguration der Basisstation-Einheit für PPP over Ethernet (PPPoE) und Kabel/DSL finden Sie unter Konfigurieren der BSE342- und BSM342-Basisstationen.

Hinweis: Point-to-Point Tunneling Protocol (PPTP) wird nicht unterstützt.

Hinweis: Installieren Sie die Wireless-Karte, *bevor* der VPN-Client installiert wird. Entfernen Sie ggf. beide Karten, und installieren Sie anschließend die Karte neu, gefolgt vom VPN. Obwohl es sich um ein Problem in der Cisco 2.x-Version des VPN-Clients handelte, wurde es in den späteren Versionen behoben.

Zugehörige Informationen

- Konfigurieren der BSE342- und BSM342-Basisstationen

- Technische Hinweise zur Cisco Aironet Serie 340
- Technischer Support - Cisco Systems