

VPN gebruiken met Cisco Aironet basisstation

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[VPN instellen](#)

[IP-beveiliging](#)

[MTU aanpassen](#)

[Gerelateerde informatie](#)

Inleiding

Cisco Aironet Base Stations (BSM- en BSE-modellen) bieden thuisgebruikers en kleine kantoren draadloze verbindingen met een intranet of het internet. Het Base Station Ethernet (BSE)-model, met een Ethernet RJ-45-poort, kan door digitale abonneelijn (DSL) of kabelmodems op internet worden aangesloten. Het Base Station Modem (BSM)-model is uitgerust met een geïntegreerde 56k v.90-dialinemodule waarmee meerdere computers toegang hebben tot het internet via het bestaande telefoonsysteem.

Een typisch gebruik van de eenheid van het Station van de Base Station is om toegang te hebben tot het internet via kabel of DSL-verbinding in combinatie met VPN-technologie (Virtual Private Network) om snelle en beveiligde toegang tot het bedrijfsnetwerk te bieden.

Het is gemakkelijk om de eenheid van het basisstation in te stellen met het Base Station Client Utility (BSCU). Dit document toont hoe u de eenheid voor gebruik met VPN kunt instellen.

Voorwaarden

Vereisten

Lezers van dit document zouden kennis moeten hebben van deze onderwerpen:

- VPN-netwerkwerking
- Configuratie basisstation

Gebruikte componenten

De informatie in dit document is gebaseerd op het Cisco Aironet basisstation (BSM- en BSE-modellen).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

VPN instellen

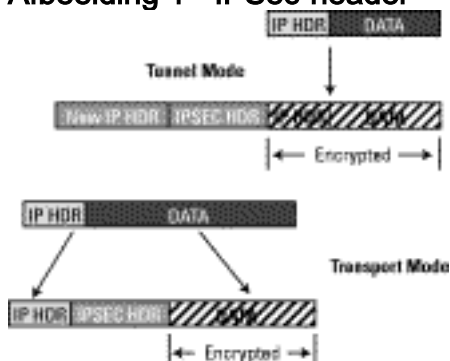
IP-beveiliging

De eerste stap in VPN-instellingen is om ondersteuning te bieden voor het gebruik van IP Security (IPSec) technologie, die binnen de VPN-technologie is geïntegreerd. IPSec gebruikt encryptietechnologie om gegevensvertrouwelijkheid, integriteit en authenticiteit tussen deelnemende peers in een privaat netwerk te verstrekken.

IPSec definieert een nieuwe reeks kopregels die aan IP-datagrammen worden toegevoegd. Deze kopregels worden geplaatst na de IP-header en vóór het Layer 4-protocol (doorgaans Transmission Control Protocol [TCP] of User Datagram Protocol [UDP]). Het resultaat is dat de pakketten van het lokale netwerk gaan waar de PC door op het internet wordt geïnstalleerd. Deze pakketten zijn groter dan niet gecodeerde pakketten. De grotere afmetingen kunnen problemen veroorzaken aan apparaten die normale grote pakketten verwachten, omdat de ontvangende apparaten hen als overmaatse pakketten zien.

Afbeelding 1 toont hoe de IPSec-header binnen een normaal pakket past.

Afbeelding 1 - IPSec-header

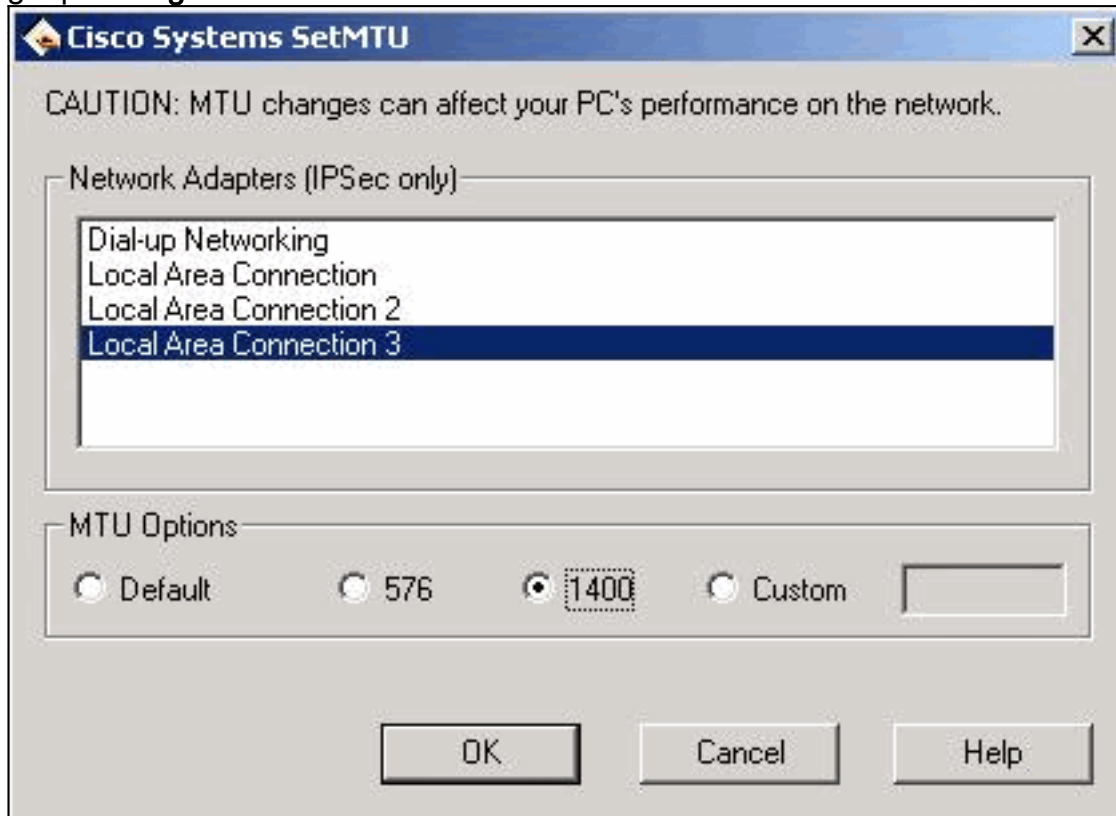


MTU aanpassen

Om ervoor te zorgen dat ontvangende apparaten de pakketten niet als te groot beschouwen, moet u de grootte van de maximale transmissie-eenheid (MTU) aan de PC/host-zijde aanpassen. Stel het totale maximum formaat in dat het pakket kan nemen zodat het de normale grootte van een niet gecodeerd Ethernet-pakket niet overschrijdt. VPN-toepassingen bieden doorgaans de optie om de grootte van de MTU aan te passen.

Voltooi deze stappen om MTU aan te passen in een Cisco Systems VPN-client in Microsoft Windows:

1. Kies **Start > Programma's > Cisco Systems VPN-client > MTU instellen**. Dit venster wordt geopend: **Figuur 2**



2. Selecteer de draadloze clientadapter die u gebruikt voor de aansluiting op uw basisstation-unit (in het voorbeeld in afbeelding 2, Local Area Connection 3).
3. Klik onder **MTU Opties** op de radioknop **1400** en vervolgens op **OK**. Dit zorgt ervoor dat uw PC pakketten met 1400 bytes als maximum verzenden. Daarom wordt de extra IPSec-header ingepast, maar de normale maximale grootte van 1518 bytes van een Ethernet-pakket wordt niet overschreden.

Opmerking: De verklaring dat de "Veranderingen van de MTU kunnen de prestaties van uw PC op het netwerk beïnvloeden" verwijst naar het feit dat wegens de kleinere grootte van MTU, twee pakketten vereist zijn om de gegevens te verzenden die eerder in één niet gecodeerd frame waren.

Voor meer informatie over het configureren van de eenheid van het basisstation voor PPP over Ethernet (PPPoE) en Cable/DSL, raadpleegt u [De basisstations BSE342 en BSM342 configureren](#).

Opmerking: Point-to-Point Tunneling Protocol (PPTP) wordt niet ondersteund

Opmerking: Installeer de draadloze kaart *voordat* de VPN-client is geïnstalleerd. Indien nodig verwijder beide, dan installeer de kaart gevolgd door VPN opnieuw. Hoewel dit een kwestie in de release van Cisco 2.x van de VPN-client was, werd deze in de latere herzieningen vastgelegd.

[Gerelateerde informatie](#)

- [De basisstations BSE342 en BSM342 configureren](#)
- [Cisco Aironet 340 Series Tech Notes](#)
- [Technische ondersteuning - Cisco-systemen](#)