Uso di VPN con la stazione base Cisco Aironet

Sommario

Introduzione

Le stazioni base Cisco Aironet (modelli BSM e BSE) forniscono agli utenti privati e ai piccoli uffici connettività wireless a una Intranet o a Internet. Il modello Base Station Ethernet (BSE), dotato di porta Ethernet RJ-45, può essere collegato a Internet tramite DSL (Digital Subscriber Line) o modem via cavo. Il modello BSM (Base Station Modem) è dotato di un modem di accesso remoto 56k v.90 integrato che consente a più computer di accedere a Internet tramite il sistema telefonico legacy.

Un utilizzo tipico dell'unità della Stazione base consiste nell'accedere a Internet tramite una connessione via cavo o DSL in combinazione con la tecnologia VPN (Virtual Private Networking) per fornire un accesso rapido e sicuro alla rete aziendale.

Èfacile configurare l'unità della Stazione base con la BSCU (Base Station Client Utility). In questo documento viene spiegato come configurare l'unità per l'utilizzo con VPN.

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- Operazione di rete VPN
- Configurazione della Stazione base

Componenti usati

Le informazioni di questo documento si basano sulla stazione base Cisco Aironet (modelli BSM e BSE).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configura VPN

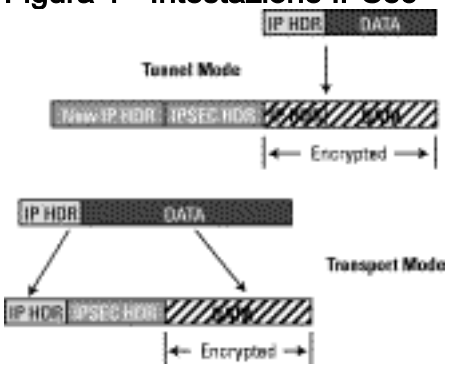
Sicurezza IP

Il primo passo nella configurazione della VPN è consentire l'utilizzo della tecnologia di sicurezza IP (IPSec), integrata nella tecnologia VPN. IPSec utilizza la tecnologia di crittografia per garantire la riservatezza, l'integrità e l'autenticità dei dati tra i peer che partecipano a una rete privata.

IPSec definisce un nuovo insieme di intestazioni che vengono aggiunte ai datagrammi IP. Queste intestazioni vengono posizionate dopo l'intestazione IP e prima del protocollo di layer 4 (in genere TCP (Transmission Control Protocol) o UDP (User Datagram Protocol)). Di conseguenza, i pacchetti passano dalla rete locale in cui è installato il PC a Internet. Questi pacchetti sono di dimensioni maggiori rispetto ai pacchetti non crittografati. L'aumento delle dimensioni può causare problemi ai dispositivi che si aspettano pacchetti di dimensioni normali, in quanto i dispositivi riceventi li vedono come pacchetti di dimensioni eccessive.

Nella figura 1 viene mostrato come l'intestazione IPSec si adatta a un pacchetto normale.

Figura 1 - Intestazione IPSec

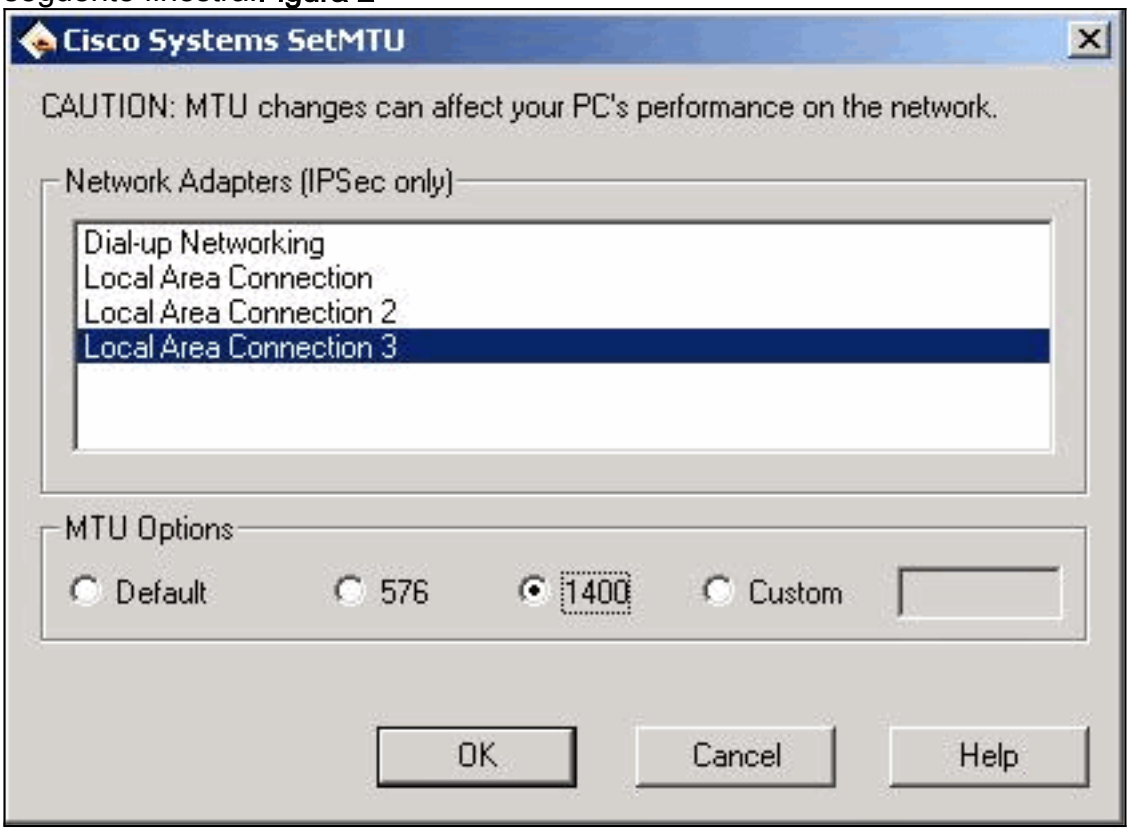


Regolazione dell'MTU

Per evitare che i dispositivi riceventi percepiscano i pacchetti come sovradimensionati, è necessario regolare le dimensioni della MTU (Maximum Transmission Unit) sul lato PC/host. Modificare le dimensioni massime totali che il pacchetto può assumere in modo che non superi le dimensioni normali di un pacchetto Ethernet non crittografato. Le applicazioni VPN in genere offrono l'opzione di personalizzare le dimensioni dell'MTU.

Completare questa procedura per regolare l'MTU in un client VPN di Cisco Systems in Microsoft Windows:

1. Scegliere **Start > Programmi > Cisco Systems VPN Client > Set MTU**. Viene visualizzata la seguente finestra:**Figura 2**



2. Selezionare la scheda client wireless da utilizzare per la connessione all'unità della Stazione base (nell'esempio mostrato nella Figura 2, Connessione LAN 3).
3. In **Opzioni MTU** fare clic sul pulsante di opzione **1400** e quindi su **OK**. In questo modo, il PC trasmette pacchetti con un massimo di 1400 byte. Pertanto, viene alloggiata l'intestazione IPSec aggiuntiva, ma non vengono superate le dimensioni massime normali di un pacchetto Ethernet di 1518 byte.

Nota: l'affermazione che "le modifiche MTU possono influire sulle prestazioni del PC sulla rete" si riferisce al fatto che, a causa delle dimensioni MTU più piccole, sono necessari due pacchetti per inviare i dati precedentemente contenuti in un singolo frame non crittografato.

Per ulteriori informazioni su come configurare l'unità della Stazione base per PPP over Ethernet (PPPoE) e cavo/DSL, consultare il documento sulla configurazione delle Stazioni base BSM342 e BSM342.

Nota: il protocollo PPTP (Point-to-Point Tunneling Protocol) non è supportato

Nota: installare la scheda wireless *prima* del client VPN. Se necessario rimuovere entrambi, quindi reinstallare la scheda seguita dalla VPN. Sebbene questo fosse un problema nella versione Cisco 2.x del client VPN, è stato risolto nelle revisioni successive.

Informazioni correlate

- Configurazione delle stazioni base BSE342 e BSM342
- Note tecniche su Cisco Aironet serie 340
- Supporto tecnico – Cisco Systems