RADIUS for VPN Clients to 3Com X-family

Document Version:	1.1
Publication Date:	9th May 2007
Description:	Use of RADIUS by VPN Clients to 3Com X-family
Product:	3Com X-family
3Com TOS Version:	2.5.1.6826
Windows XP Version	Version 5.1 (Build 2600.xpsp_sp2_gdr.061219-0316 : Service Pack 2)
Windows Vista version	Ultimate Edition

Introduction

This document explains how to configure the 3Com X-Family devices to use a RADIUS server to authenticate VPN Clients. The VPN Clients may be from various providers and may use various VPN protocols (PPTP, IPSec Tunnel mode, L2TP/IPSec).

These instructions assume that your corporate network is attached to the LAN security zone of the X-family device, and that external (Internet) traffic is on the WAN security zone.

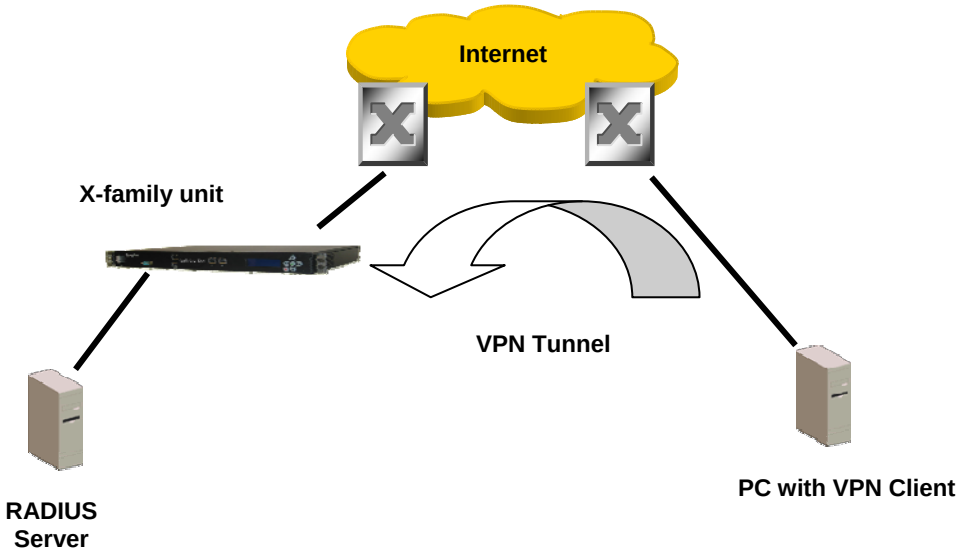
Table of Contents

1 Overview

RADIUS allows the centralized authentication of remote users connecting over VPN tunnels. Compared to holding user account data locally in each X-family device this significantly reduces the workload on IT staff caused by user “churn”. Note that X-family devices do not currently support RADIUS accounting.

The RADIUS server must support CHAP, MSCHAP and MSCHAPv2 authentication. The type of authentication which the X-family will use will depend on what is supported by the VPN client.

2 Network Configuration



IP Addresses for the following example setup are:

Device	Interface	Address	Mask	Gateway
Router	1 (to X-family unit)	10.10.20.1	255.255.255.0	
Router	2 (to VPN Client)	10.10.10.1	255.255.255.0	
X-family	external	10.10.20.147	255.255.255.0	10.10.10.1
X-family	internal	192.168.1.254	255.255.255.0	
VPN Client	external	10.10.10.147	255.255.255.0	10.10.20.1
VPN Client	Tunnel	192.168.1.x	255.255.255.0	192.168.1.254
RADIUS Server		192.168.1.200	255.255.255.0	192.168.1.254

Note: The RADIUS Server(s) can be anywhere on the Network.

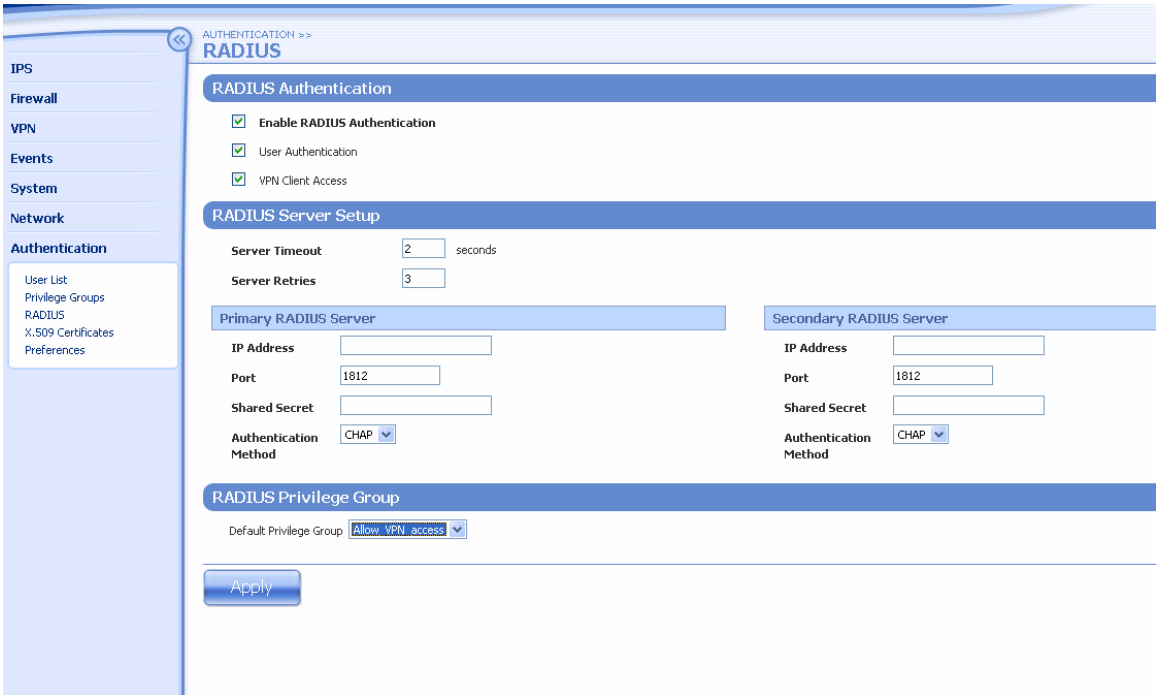
3 Configuration

3.1 High Level Configuration Steps

1) Enable the X-Family RADIUS Client, and configure it with the information required to communicate with the RADIUS Server(s).
2) Configure the RADIUS Server with the information required to communicate with the X-family RADIUS Client.
3) Configure the RADIUS Server with the User Accounts.

3.2 X-Family RADIUS Configuration

The RADIUS client is configured via the LSM in the Authentication > RADIUS page:



1) To configure RADIUS on the X-family you must:
a) Check the “Enable RADIUS Authentication” tickbox.
b) Select which type of user access will be authenticated via RADIUS. This may include Local-Users (e.g. for web access through the X-family) and/or VPN Clients terminating on the X-family.
c) Specify the RADIUS Server (and optional secondary RADIUS Server). The following parameters are required:
   - The IP address of the RADIUS Server.
   - The port number used (1812 is the default for all RADIUS servers).
   - The Shared Secret used to control access to the RADIUS server.

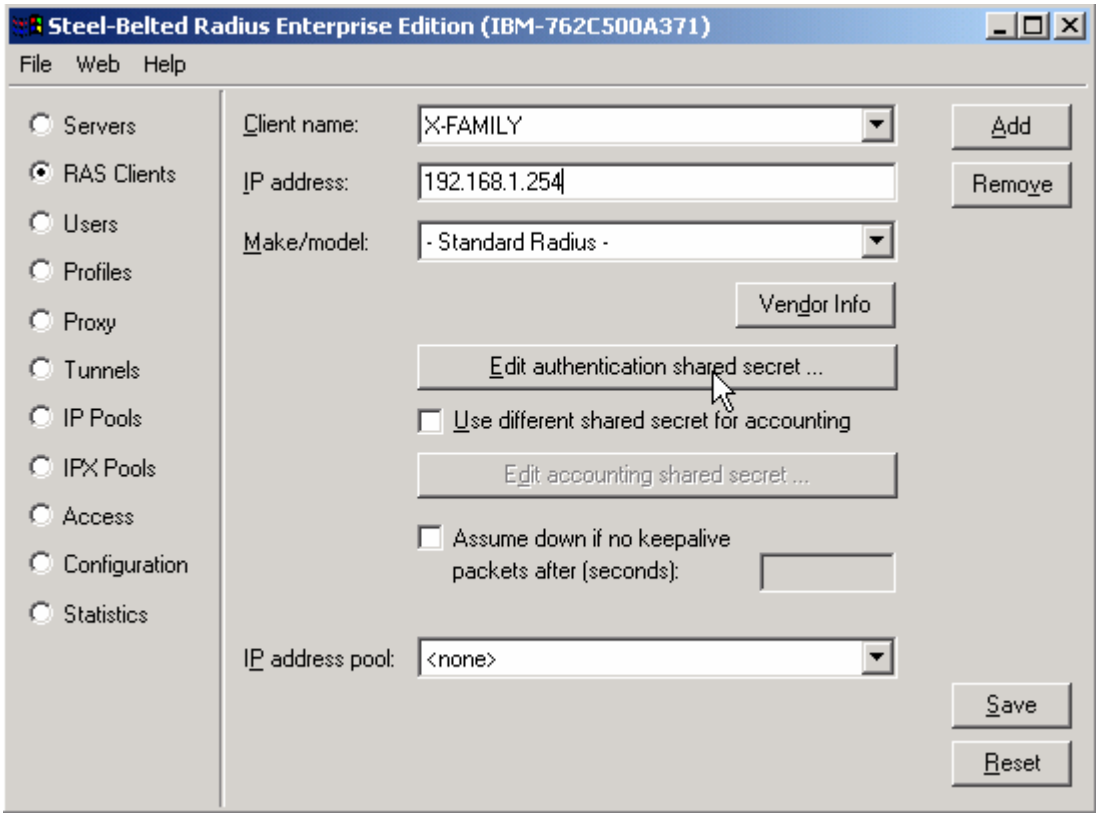
- The *preferred* Authentication Method to use for requests from the X-family to the RADIUS server. CHAP is the preferred authentication scheme. Note that the product will use other schemes to authenticate depending on what it is trying to authenticate, for example RADIUS PPTP user authentication will normally use MS-CHAP or MS-CHAPv2.

d) If RADIUS is only being used for VPN access, set the Default RADIUS Privilege Group to "Allow_VPN_Access". If not, leave the Default RADIUS Privilege Group set to "RADIUS" and see section below "Configuring Privilege Groups on the User Accounts".
e) Click "Apply".

3.3 RADIUS Server Configuration

3.3.1 Configuring the X-Family devices on the RADIUS Server

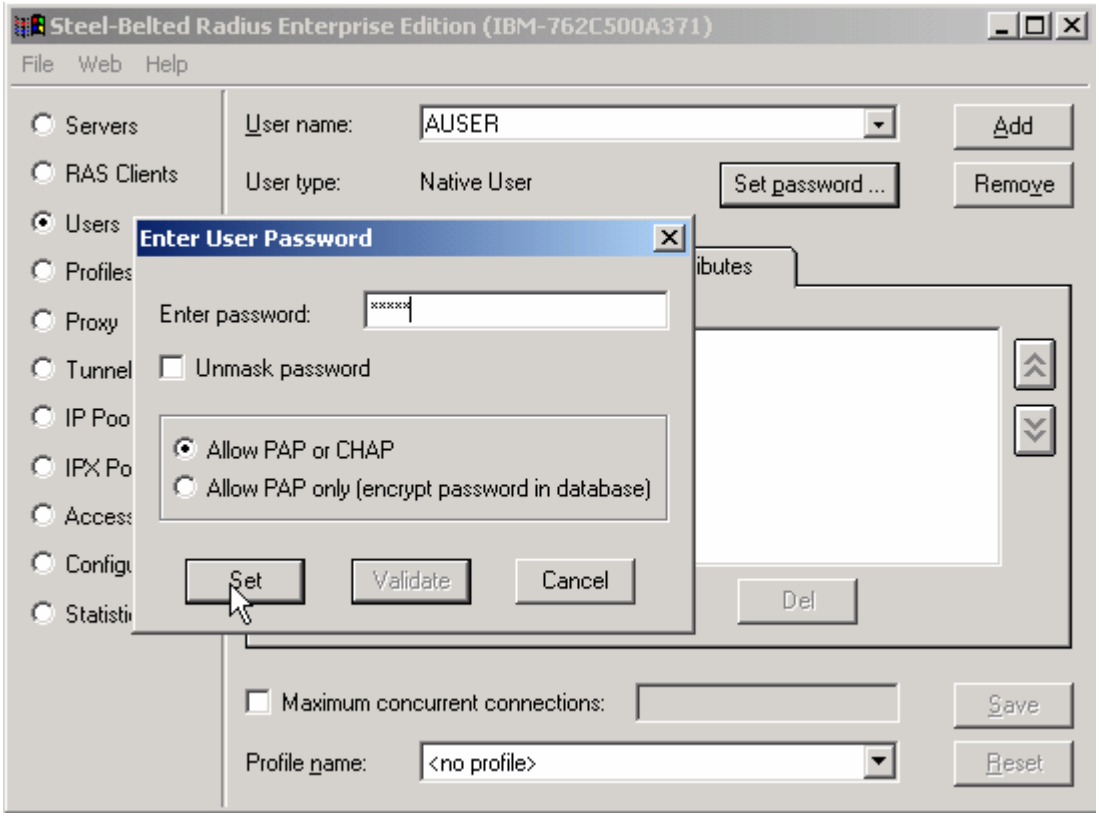
Each X-family device must be configured on the RADIUS server as a RADIUS client. The configuration method varies depending on the RADIUS Server, but it will be similar to the example shown (Funk Software Steel-Belted RADIUS).



Clicking the "Edit authentication shared secret" button opens another form to enter the shared secret, which must match the one configured on the X-family.

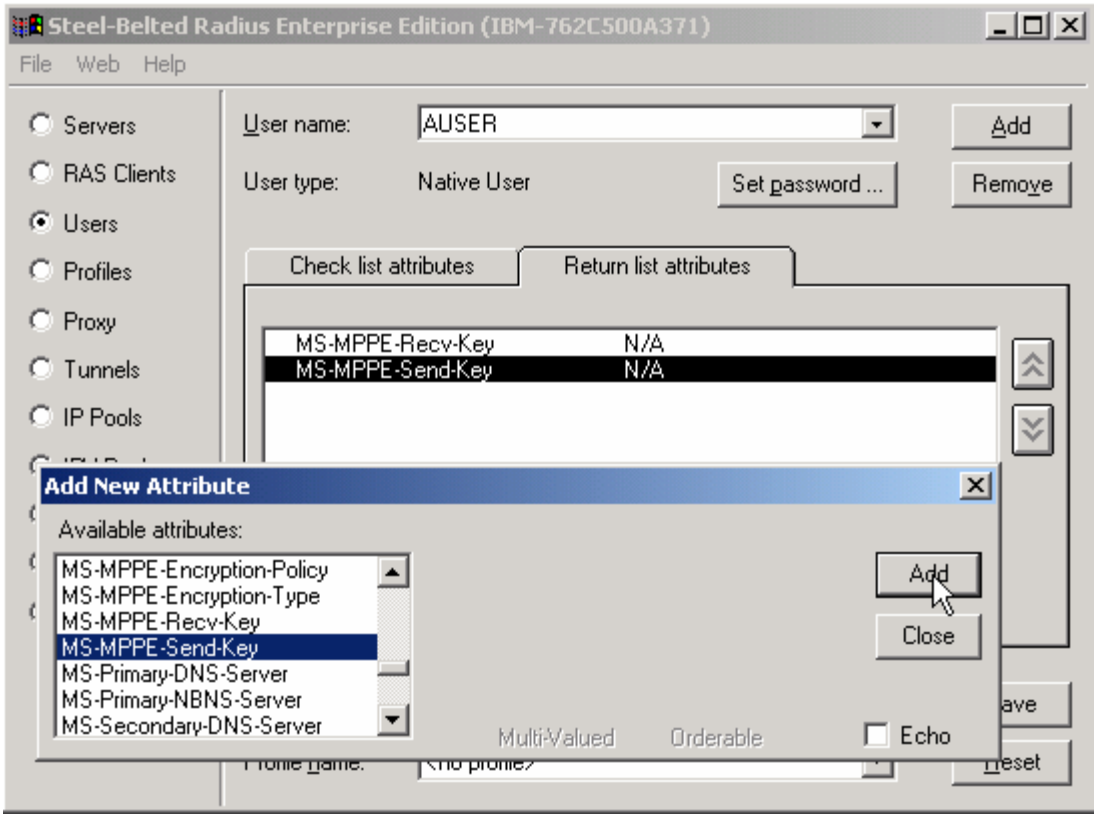
3.3.2 Configuring the User Accounts on the RADIUS Server

Accounts must be configured on the RADIUS Server for all Users. The example shown is again Funk Steel-Belted RADIUS.



3.3.3 Configuring User Accounts for PPTP

If the User will be connecting using the PPTP protocol, the MPPE-key attributes must be set. This is set by default on the Microsoft RADIUS server, but not on others. The example is again Funk Steel-Belted RADIUS.



Examples of RADIUS servers that support this attribute include.

- Funk Software Steel-Belted RADIUS.
- Microsoft Internet Authentication Server.
- Microsoft Windows Server 2003.
- FreeRADIUS.

3.4 Configuration Notes

3.4.1 Configuration Note - Privilege Groups on the User Accounts

In addition to authenticating the user via a password, the RADIUS server can be used to control whether particular user accounts are allowed to create VPN tunnels. This is achieved by controlling whether particular accounts are members of the appropriate X-family privilege groups. Privilege groups control what services a user can access once they have authenticated with the X-family.

RADIUS attributes can be used to set the privilege groups on each account.

The privilege group used for a RADIUS authenticated user is determined as follows:

- If RADIUS is used exclusively for authenticating VPN client users and not local users, then set the “Default Privilege Group” pulldown on the RADIUS configuration web page in the LSM to “Allow_VPN_access” privilege. This

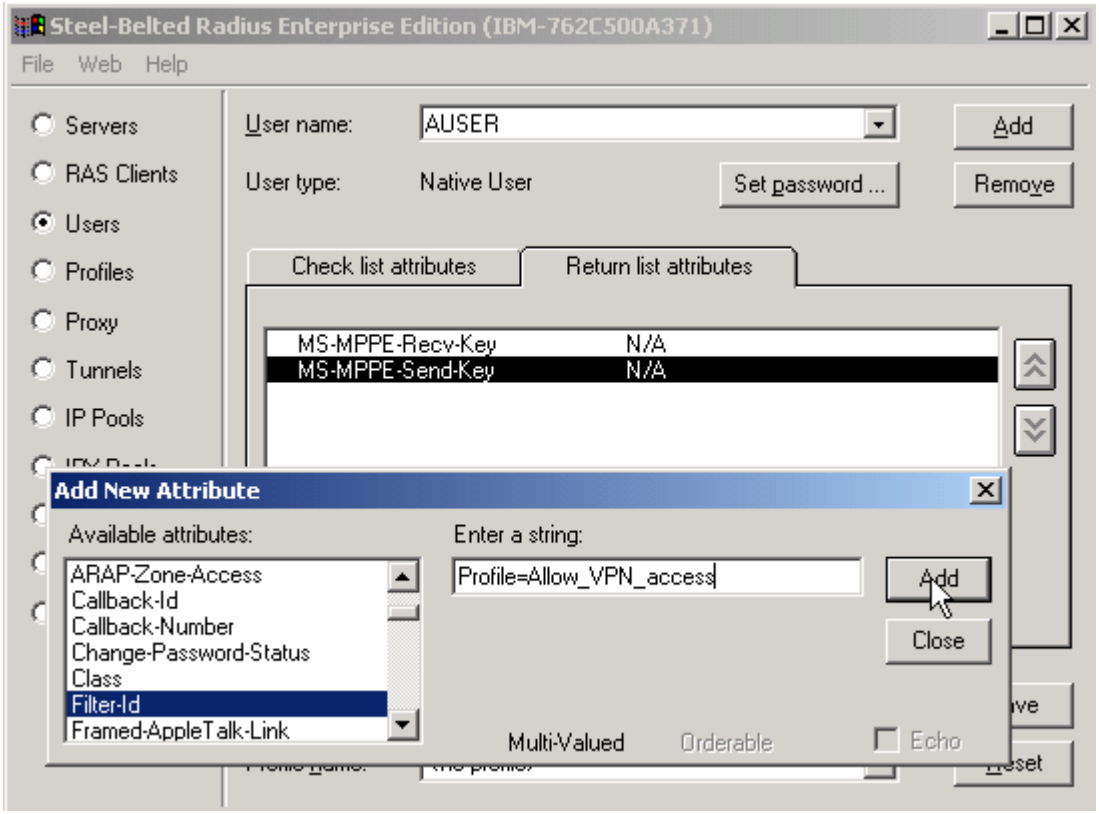
means that all RADIUS users will be assigned this privilege on successful authentication with the RADIUS server.

- If RADIUS is used for both authenticating Local Users and for VPN Users, set the "Default Privilege Group" pulldown on the RADIUS configuration web page in the LSM to "RADIUS" privilege. Then set the RADIUS Server to return a "Filter-Id" attribute. Specify "Profile=<*Priviliege-Group-Name*>" on the Filter-ID attribute on the RADIUS server.

For example, to specify that a RADIUS user account be assigned the "Allow_VPN_access" privilege on the X-family, configure the RADIUS server to return the following Filter-ID attribute:

```
Filter-Id = "Profile=Allow_VPN_access",
```

Again, here is an example using Funk Steel-Belted RADIUS.



If the RADIUS server does not return a Filter-ID attribute, or the Filter-ID attribute contains no "Profile=…" type-value pair then the unit will assign the user the privilege group configured on the X-family in the "Default Privilege Group" pulldown on the RADIUS configuration web page.

3.4.2 Configuration Note – Disabling User Accounts

To prevent a user account from terminating a VPN connection on the X-family, take either of the following steps:

- Set the Default Privilege Group to RADIUS on the X-family, and omit the Filter-ID attribute on the RADIUS account.
- Set the Filter-ID attribute to return a blank value. For example:

```
Filter-Id = "Profile= ",
```

3.4.3 Configuration Note - FreeRADIUS

The FreeRADIUS default dictionary ***dictionary.freeradius.internal*** is sufficient to interoperate with an X-family device.

Select the primary authentication means as "Auth-Type:=Local" to allow any of the authentication protocols to work. Other protocols will be used as a fallback if the primary selection does not work. This will allow a mixture of CHAP, MS-CHAP, MS-CHAPv2, PAP to be used by the X-family. This is required since the X-family will use different authentication algorithms depending on the type of authentication being performed (e.g. some PPTP connections may use MS-CHAP while local user authentication might use CHAP).

An example of configuring the FreeRADIUS server to get an account working for the user "test" with password "test" specifying the privilege group “Allow_VPN_access” is included below:

In /etc/raddb/users add:

```
test   Auth-Type := Local, User-Password == "test"
      Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.16.3.33,
      Framed-IP-Netmask = 255.255.255.0,
      Framed-Routing = Broadcast-Listen,
      Filter-Id = "Profile=Allow_VPN_access",
      Framed-MTU = 1500,
      Framed-Compression = Van-Jacobsen-TCP-IP
```

In /etc/raddb/clients.conf add the following, where 10.0.0.254/32 is the Virtual Interface IP address of the X505 used to send RADIUS requests to the FreeRADIUS server:

```
client 10.0.0.254/32 {
      secret = password
      shortname = x505
}
```


3.4.4 Configuration Note – Juniper Networks (Funk) SteelBelted RADIUS

Steel-Belted RADIUS supports CHAP and MSCHAPv2. It seems that later versions of Steel-Belted RADIUS require MSCHAPv2 to be enabled. Ensure that Steel Belted RADIUS is set to “Allow MSCHAPv2” when setting the user passwords.

4 Troubleshooting RADIUS Authentication

The following is a list of things to check if the RADIUS authentication cannot be established or does not operate correctly:

a) Check the RADIUS server is configured to respond to the X-family device as some RADIUS servers restrict requests from certain IP addresses.
b) Check the shared secret matches for the RADIUS server.
c) Check that the user on the RADIUS server is configured to allow remote access via the “Allow_VPN_access” privilege group.
d) Check that the RADIUS server allows both MSCHAP and MSCHAPv2 authentication for the user.
e) Check that the firewall policy rules on the X-family allow this-device to talk RADIUS to the RADIUS Server on UDP port 1812.
f) Check that the appropriate Attributes have been set in the RADIUS server for the user account, or on the Default Privileges configuration of the X-family to grant “VPN_Client_Access” privilege to the user.
g) If an encrypted PPTP tunnel is being formed, ensure that the RADIUS server has been configured to return the MS-CHAP-MPPE-Key attributes.

