

CiscoSecure Profile and NAS Configuration Examples

As previously noted, to successfully implement the CiscoSecure profile attributes that you assign to your users, you must also configure support for those attributes on the NAS through which those users log in to the network.

This chapter provides examples of some typical CiscoSecure user profiles coupled with the NAS configurations that support those profiles. Both TACACS+ and RADIUS examples are provided. Examples include:

- TACACS+—Limited EXEC Session Authorization
- TACACS+—Shell Filter Access and Limitations (Allow and Refuse)
- TACACS+—Asynchronous PPP Connections with CHAP Authentication
- RADIUS—EXEC Session Authorization
- RADIUS—Asynchronous PPP Connections with CHAP Authentication
- TACACS+—VPDN Example
- RADIUS—VPDN Example

TACACS+—Limited EXEC Session Authorization

The following CiscoSecure profile and NAS configurations enable a TACACS+ user to run a limited set of EXEC session commands: the **show version** command on the router, and the **Telnet** command to IP address 10.6.8.11 only. It will deny all other commands.

A system administrator may want to grant his/her group administrators access to a limited set of EXEC query commands on specified routers to allow them to look up configuration information in support of support-line troubleshooting.

User Profile for Limited EXEC Session Authorization in TACACS+

The following user profile, generated through the Java-based CiscoSecure Administrator advanced configuration program, grants user `ga_simpson` permission to run the **show version** and **Telnet** commands only on the NAS that he/she is logging into.

```
user = ga_simpson{
  member = groupf
  password = clear "sesame1"
  service=shell {
    cmd=show {
      permit version
    }
    cmd=telnet {
      permit 10.6.8.11
    }
  }
}
```

NAS Support for Limited EXEC Session Authorization in TACACS+

The following configuration, entered at the NAS through which user ga_simpson logs in, supports the limited EXEC session authorization configured in the earlier section, “User Profile for Limited EXEC Session Authorization in TACACS+.” Commands significant to this support are annotated below.

```
!
version 11.3
!
hostname as5200
!
! Turn on Authentication, Authorization, Accounting
aaa new-model

! 'vtymethod', 'conmethod' are the names of lists for authentication
! methods. If authentication fails due to CiscoSecure not being
! started, the enable password will be accepted because it is in each
! list
aaa authentication login vtymethod local tacacs+ enable
aaa authentication login conmethod local tacacs+ enable

! Set the commands at level 1 authorization.
aaa authorization commands 1 tacacs+
enable password cisco
!
username cisco password 0 cisco
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.6.8.21 255.0.0.0
!
```

TACACS+—Limited EXEC Session Authorization

```
interface Group-Async1
  ip unnumbered Ethernet0
  encapsulation ppp
  no ip route-cache
  no ip mroute-cache
  async dynamic routing
  async mode interactive
  no peer default ip address
  ppp authentication chap
  group-range 1 24
!
router rip
  network 10.0.0.0
!
! Specify the CiscoSecure server
tacacs-server host 10.6.8.20

! Time (10 seconds) to wait for CiscoSecure server to reply
tacacs-server timeout 10

! Set TACACS+ encryption key
tacacs-server key SECRET12345
!
line con 0
  exec-timeout 0 0
  password cisco
  login authentication conmethod
line 1 24
  autoselect ppp
  modem InOut
  transport input all
  telnet transparent
line aux 0
line vty 0
  exec-timeout 0 0
  password cisco
  login authentication vtymethod
  width 110
line vty 1 4
  exec-timeout 0 0
  password cisco
  login authentication vtymethod
!
end
```

Verification of Limited EXEC Session Authorization in TACACS+

To verify the limited EXEC session authorization configuration, the administrator, in the example below, Telnets to a NAS at IP address 10.6.8.21, logs in as user `ga_simpson`, and runs the authorized **show version** and **Telnet 10.6.8.11** commands. For example:

```
telnet 10.6.8.21
Trying 10.6.8.21...
Connected to 10.6.8.21.
Escape character is '^]'.
User Access Verification
Username: ga_simpson
Password: sesame1

as5200> sh ver
Cisco Internetwork Operating System Software
IOS (tm) 5200 Software (C5200-J-L), Version 11.3(1), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Tue 16-Dec-97 02:49 by richardd
Image text-base: 0x22048730, data-base: 0x00005000
ROM: System Bootstrap, Version 11.1(474) [tamb 474], RELEASE SOFTWARE
(fc1)
BOOTFLASH: 5200 Software (AS5200-B00T-L), Version 11.1(474), RELEASE
SOFTWARE (f
c1)

as5200 uptime is 3 hours, 29 minutes
System restarted by reload
System image file is "flash:c5200-j-l_113-1.bin", booted via flash
cisco AS5200 (68030) processor (revision A) with 16384K/16384K bytes of
memory.
Processor board ID 03678427
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.0.
Mother board without terminator card.
1 Ethernet/IEEE 802.3 interface(s)
26 Serial network interface(s)
24 terminal line(s)
2 Channelized T1/PRI port(s)
128K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)
```

TACACS+—Limited EXEC Session Authorization

```
8192K bytes of processor board Boot flash (Read/Write)
Configuration register is 0x2102
```

```
as5200> telnet 10.6.8.11
Trying 10.6.8.11 ... Open
UNIX(r) System V Release 4.0 (NOC1)
login: root
Password:
Last login: Thu Apr 16 14:52:02 from 10.6.8.21
Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996
xhost: Command not found
NOC1# exit
NOC1# logout
[Connection to 10.6.8.11 closed by foreign host]
```

After establishing a Telnet connection to the authorized IP address and running the authorized EXEC commands, the system administrator then verifies the profile limitations by attempting unauthorized commands. For example:

```
as5200> sh ip route
Authorization - Failed command line

as5200> ping 10.6.8.11
Authorization - Failed command
as5200>
```

TACACS+—Shell Filter Access and Limitations (Allow and Refuse)

The following CiscoSecure profile and NAS configuration use the TACACS+ allow and refuse attributes, also known as filter attributes, to allow the user, `admn_tfong`, to start an EXEC session at a specified (NAS) IP address through any TTY port on that NAS and from any remote address.

User Profiles with Shell Filter Access and Limitations in TACACS+

For TACACS+, the allow and refuse attributes have three different parameters: the NAS name or IP address, the port that is being requested, and the remote IP address of the requesting user.

The following user profile, generated through the Java-based CiscoSecure Administrator advanced configuration program, applies the shell filter allow and refuse attributes to:

- Allow user `admn_tfong` to start an EXEC session on the NAS located at IP address 10.6.8.21 through any TTY port on that NAS from any remote IP address.
- Refuse user `admn_tfong` EXEC session access to any other (NAS) IP address.

```
user = admn_tfong {  
  member = groupB  
  password = clear "cisco"  
  service=shell {  
    allow "^10\\.6\\.8\\.21$" "tty.*" ".*"  
    refuse ".*" ".*" ".*"  
  }  
}
```

Note The standard UNIX pattern characters, `^`, `\`, and `$` are inserted in this example to prevent misinterpretation of the IP addresses and TTY port ranges. For example, if the `\` character were not inserted before the periods in the IP addresses, then under standard UNIX pattern matching, the periods would be interpreted as wildcard characters, thus enabling user `admn_tfong` to run shell sessions not only on the NAS at 10.6.8.21, but also at addresses not necessarily intended.

NAS Support for Shell Filter Access and Limitations in TACACS+

The following configuration, entered at the NAS through which user `admn_tfong` logs in, supports shell service filter attributes applied in the profile configured in the “User Profiles with Shell Filter Access and Limitations in TACACS+” section on page 12-7. Commands significant to this support are annotated below.

```
version 11.3
!
hostname as5200
!
aaa new-model
aaa authentication login vtymethod local tacacs+ enable
aaa authentication login conmethod local tacacs+ enable

! Set the EXEC authorization
aaa authorization exec tacacs+
aaa authorization commands 1 tacacs+
enable password cisco
!
username cisco password 0 cisco
isdn switch-type primary-5ess
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
interface Ethernet0
ip address 10.6.8.21 255.0.0.0
!
interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
no ip route-cache
no ip mroute-cache
async dynamic routing
async mode interactive
no peer default ip address
ppp authentication chap
group-range 1 24
!
```

```
router rip
 network 10.0.0.0
!
tacacs-server host 10.6.8.20
tacacs-server timeout 10
tacacs-server key SECRET12345
!
line con 0
 exec-timeout 0 0
 password cisco
 login authentication conmethod
line 1 24
 autoselect ppp
 modem InOut
 transport input all
 telnet transparent
line aux 0
line vty 0
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
 width 110
line vty 1 4
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
!
end
```

Verification of Shell Filter Access and Limitations on EXEC Session Access in TACACS+

To verify the ability of user `adm_n_tfong` to start an EXEC session, the administrator, in the example below, Telnets to the authorized IP address, 10.6.8.21 and logs in as user, `adm_n_tfong`. Any attempt to Telnet to a NAS at any other IP address would be refused.

```
telnet 10.6.8.21
Trying 10.6.8.21...
Connected to 10.6.8.21.
Escape character is '^['.
```

User Access Verification

```
Username: adm_n_tfong
Password: cisco
```

```
as5200>
```

TACACS+—Asynchronous PPP Connections with CHAP Authentication

The following CiscoSecure profile and NAS configurations support a TACACS+ and PPP protocol user logging in with CHAP authentication. The user is assigned an IP address out of the IP address pool (nas1-pools).

User Profiles for Asynchronous PPP Connections in TACACS+

The following two user profiles are generated through the Java-based CiscoSecure Administrator advanced configuration program.

- The first profile sets up user bliu for PPP connection and assigns user bliu to IP address pool aaa:

```
user = bliu {  
  member = groupA  
  password = chap "sesame2"  
  service=ppp {  
    protocol=ip {  
      set addr-pool=aaa  
    }  
    protocol=lcp {  
    }  
  }  
}
```

- The second profile sets up a “user” nas1-pools and defines an IP address range to the “aaa” pool from 10.6.8.31 to 10.6.8.33:

```
user = nas1-pools{  
  member = Examples  
  service=ppp {  
    protocol=ip {  
      set pool-def#1="aaa 10.6.8.31 10.6.8.33"  
      set pool-timeout=60  
    }  
  }  
}
```

NAS Support for PPP Connection in TACACS+

The following configuration, entered at the NAS through which user bliu logs in, supports the PPP connection configured in the earlier section, “User Profiles for Asynchronous PPP Connections in TACACS+.” Commands significant to this support are annotated below.

```
version 11.3
!
hostname as5200
!
aaa new-model
aaa authentication login vtymethod local tacacs+ enable
aaa authentication login conmethod local tacacs+ enable

! Set ppp default authentication list
aaa authentication ppp default tacacs+
aaa authorization exec tacacs+
aaa authorization commands 1 tacacs+

! Set ppp authorization
aaa authorization network tacacs+

! Set ppp accounting
aaa accounting network start-stop tacacs+

! Set username of a pool to download the ip address pool
aaa configuration config-username nas1-pools
enable password cisco
!
username cisco password 0 cisco
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.6.8.21 255.0.0.0
!
```

```
interface Group-Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 no ip route-cache
 no mroute-cache
 async dynamic routing
 async mode interactive
 no peer default ip address
 ppp authentication chap
 group-range 1 24
!
router rip
 network 10.0.0.0
!
tacacs-server host 10.6.8.20
tacacs-server timeout 10
tacacs-server key SECRET12345
!
line con 0
 exec-timeout 0 0
 password cisco
 login authentication conmethod
line 1 24
 autoselect ppp
 modem InOut
 transport input all
 telnet transparent
line aux 0
line vty 0
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
 width 110
line vty 1 4
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
!
end
```

Verification of Asynchronous PPP Connection in TACACS+

To verify the asynchronous PPP connection configuration, the administrator, in the example below, sets up a Windows 95 workstation for PPP connection and tests it:

- Step 1** In Windows select **Start>Programs>Accessories>Dial-Up Networking**.
- Step 2** Select **Connections>Make New Connection** and enter a name for your connection.
- Step 3** Enter your modem-specific information and under Configure/General choose the highest speed of your modem, but do not check the box below this.
- Step 4** Under Configure/Connection, use 8 data bits, no parity, and 1 stop bit. Under Call preferences select **Wait for dial tone before dialing** or **Cancel the call if not connected after 200 seconds**.
- Step 5** Under Advanced, select only the **Hardware Flow Control** or **Modulation Type Standard** options.
- Step 6** Under Configure/Options, check nothing except options under status control.
- Step 7** Click **OK** and click **Next**.
- Step 8** On the next screen, enter the telephone number of the destination, click **Next**, and then click **Finish**.
- Step 9** When the new connection icon appears, right click on it, select **Properties**, and then select **Server Type**.
- Step 10** Select **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** and do not check any advanced options.
Check **require encrypted password only**.
- Step 11** Under TCP/IP settings, select **Server assigned IP address** and **Server assigned name server addresses**.
- Step 12** Under Allowed Network Protocols, check **TCP/IP**.
- Step 13** Check **Use default gateway on remote network** and click **OK**.
- Step 14** Double click the Connect icon to bring up the Connect To window. Fill in the User Name and Password fields and click **Connect**.

RADIUS—EXEC Session Authorization

The following CiscoSecure profile and NAS configurations enable a RADIUS protocol user to run an EXEC session.

User Profile for EXEC Session Authorization in RADIUS

The following user profile, generated through the Java-based CiscoSecure Administrator advanced configuration program, grants user `adm_nmkumar` authorization to run EXEC session commands on the NAS that he is logging into. No restrictions are specified.

```
user = adm_nmkumar {  
  member = groupL  
  radius=Cisco {  
    check_items= {  
      2=sesame4  
    }  
    reply_attributes= {  
      6=7  
    }  
  }  
}
```

Note `2=sesame4` translates to `password=sesame4`; `6=7` translates to `User-Service-Type=Shell-User`.

NAS Support for EXEC Session Authorization in RADIUS

The following configuration, entered at the NAS through which user `admn_mkumar` logs in, supports the EXEC session authorization configured in the “User Profile for EXEC Session Authorization in RADIUS” section on page 12-15.

```
version 11.3
!
hostname as5200
!
aaa new-model
aaa authentication
aaa authentication login vtymethod local radius enable
aaa authentication login conmethod local radius enable
enable password cisco
!
username cisco password 0 cisco
isdn switch-type primary-5ess
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
interface Ethernet0
ip address 10.6.8.21 255.0.0.0
!
interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
no ip courte-cache
no ip mroute-cache
async dynamic routing
async mode interactive
no peer default ip address
ppp authentication chap
group-range 1 24
!
router rip
network 10.0.0.0
!
radius-server host 10.6.8.20 auth-port 1645 acct-port 1646
radius-server timeout 10
radius-server key SECRET12345
```

```
!  
line con 0  
  exec-timeout 0 0  
  password cisco  
  login authentication conmethod  
line 1 24  
  autoselect ppp  
  modem InOut  
  transport input all  
  telnet transparent  
line aux 0  
line vty 0  
  exec-timeout 0 0  
  password cisco  
  login authentication vtymethod  
  width 110  
line vty 1 4  
  exec-timeout 0 0  
  password cisco  
  login authentication vtymethod  
!  
end
```

Verification of EXEC Session Authorization in RADIUS

To verify the ability of user `admn_mkumar` to start an EXEC session on any NAS, the administrator, in the example below, Telnets to NAS IP address 10.6.8.21 and logs in as user, `admn_mkumar`. User `admn_mkumar` should have the authority to run EXEC sessions on any NAS on the network.

```
telnet 10.6.8.21  
Trying 10.6.8.21...  
Connected to 10.6.8.21.  
Escape character is '^['.
```

User Access Verification

```
Username: admn_mkumar  
Password: sesame4
```

```
as5200>
```

RADIUS—Asynchronous PPP Connections with CHAP Authentication

The following CiscoSecure profile and NAS configurations support a RADIUS and PPP protocol user logging in with CHAP authentication. The user is assigned an IP address out of the IP address pool(nas1-pools).

User Profiles for Asynchronous PPP Connections in RADIUS

The following two user profiles are generated through the Java-based CiscoSecure Administrator advanced configuration program.

- The first profile sets up user pbradley for PPP connection and assigns user pbradley to IP address pool, bbb:

```
user = pbradley {  
  member = groupG  
  radius=Cisco {  
    check_items= {  
      2=sesame5  
    }  
    reply_attributes= {  
      7=1  
      6=2  
      9,1="ip:addr-pool=bbb"  
    }  
  }  
}
```

- The second profile sets up a “user” nas1-pools and defines an IP address range to the “bbb” pool from 10.6.8.31 to 10.6.8.33:

```
user = nas1-pools{  
  member = Examples  
  radius=Cisco {  
    reply_attributes= {  
      6=5  
      9,1="ip:pool-def#1=bbb 10.6.8.34 10.6.8.35"  
    }  
  }  
}
```

NAS Support for PPP Connection in RADIUS

The following configuration, entered at the NAS through which user pbradley logs in, supports the PPP Connection configured in the “User Profiles for Asynchronous PPP Connections in RADIUS” section on page 12-18. Commands significant to this support are annotated below.

```

!
version 11.3
!
hostname as5200
!
aaa new-model
aaa authentication
aaa authentication login vtymethod local radius enable
aaa authentication login connmethod local radius enable

! Set PPP default authentication list
aaa authentication ppp default radius

! Set PPP authorization
aaa authorization network radius

! Set PPP accounting
aaa accounting network start-stop radius

! Set username of a pool to download
aaa configuration config-username nas1-pools
enable password cisco
!
username cisco password 0 cisco
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.6.8.21 255.0.0.0
!

```

RADIUS—Asynchronous PPP Connections with CHAP Authentication

```
interface Group-Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 async dynamic routing
 async mode interactive
 no peer default ip address
 ppp authentication chap
 group-range 1 24
!
router rip
 network 10.0.0.0
!
radius-server host 10.6.8.20 auth-port 1645 acct-port 1646
radius-server timeout 10
radius-server key SECRET12345
!
line con 0
 exec-timeout 0 0
 password cisco
 login authentication conmethod
line 1 24
 autoselect ppp
 modem InOut
 transport input all
 telnet transparent
line aux 0
line vty 0
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
 width 110
line vty 1 4
 exec-timeout 0 0
 password cisco
 login authentication vtymethod
!
end
```

Verification of Asynchronous PPP Connection in RADIUS

To verify the asynchronous PPP connection configuration, the administrator, in the example below, sets up a Windows 95 workstation for PPP connection and tests it:

- Step 1** In Windows select **Start>Programs>Accessories>Dial-Up Networking**.
- Step 2** Select **Connections>Make New Connection** and enter a name for your connection.
- Step 3** Enter your modem-specific information and under Configure/General choose the highest speed of your modem, but do not check the box below this.
- Step 4** Under Configure/Connection, use 8 data bits, no parity, and 1 stop bit. Under Call preferences select **Wait for dial tone before dialing** or **Cancel the call if not connected after 200 seconds**.
- Step 5** Under Advanced, select only the **Hardware Flow Control** or **Modulation Type Standard** options.
- Step 6** Under Configure/Options, check only **Options under Status Control**.
- Step 7** Click **OK** and click **Next**.
- Step 8** On the next screen, enter the telephone number of the destination, click **Next**, and then click **Finish**.
- Step 9** When the new connection icon appears, right click on it, select **Properties**, and then select **Server Type**.
- Step 10** Select **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** and don't check any advanced options.
Check **require encrypted password only**.
- Step 11** Under TCP/IP settings, select **Server assigned IP address** and **Server assigned name server addresses**.
- Step 12** Under Allowed Network Protocols, check **TCP/IP**.
- Step 13** Check **Use default gateway on remote network** and click **OK**.
- Step 14** Double-click the Connect icon to bring up the Connect To window. Fill in the User name and Password fields and click **Connect**.

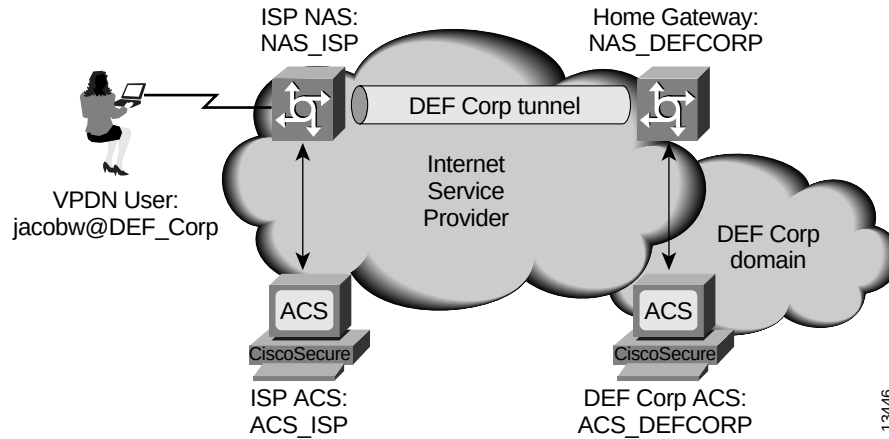
TACACS+—VPDN Example

The following sample VPDN profiles, user profiles, and NAS configurations set up a customer-managed virtual private dial-up network (VPDN) within a larger ISP-managed network and support users that are logging in to the VPDN through a remote ISP-run NAS.

In the following sample illustration:

- 1 User jacobw, a DEF Corp employee, whose user profile in a company database is accessible only by the DEF Corp ACS, dials in to the ISP network through the remote ISP-run NAS (NAS_ISP), as **jacobw@DEF_Corp**, DEF_Corp, being a VPDN set up by the ISP.
- 2 The ISP-run NAS (NAS_ISP) strips off “jacobw@” from the login string and forwards an authorization request for DEF_Corp to the ISP-run ACS (ACS_ISP), which has a VPDN profile for DEF_Corp already configured.
- 3 ACS_ISP returns DEF_Corp VPDN profile information to NAS_ISP, which engages in a two-way authentication process with the DEF Corp-run home gateway NAS (NAS_DEFCORP) and, if successful, establishes a VPDN tunnel to NAS_DEFCORP.
- 4 The “jacobw@DEF_Corp” login string is forwarded from NAS_ISP through the VPDN tunnel to NAS_DEFCORP and then to the DEF Corp-run ACS (ACS_DEFCORP), which is configured through CiscoSecure administration web page settings to strip off “@DEF_Corp” and authenticate “jacobw” from the DEF Corp database of authorized users.

Figure 12-1 Sample TACACS+ User Login to a VPDN



TACACS+ Profiles to Set Up at the ISP-Run ACS

To support the above scenario, you need to set up some special CiscoSecure profiles at the ISP-run ACS and at the home gateway ACS.

Set up a special VPDN profile and special NAS profiles at the ISP-run ACS, ACS_ISP.

- **The VPDN Profile.** The following profile specifies the VPDN, DEF_Corp:

```
user = DEF_Corp {
  service = ppp {
    protocol = vpdn{
      set-ipaddress = 10.10.1.1
      set-tunnelid = defcorp_tunnel
    }
  }
}
```

Note `protocol=vpdn` makes the DEF_Corp profile a VPDN; `set-ipaddress=` specifies the IP address of DEF Corp's home gateway NAS; `set-tunnelid=` is an arbitrary character string; however it must match the name of the tunnel ID profile.

- **The tunnel ID profile.** The following profile specifies the tunnel to DEF Corp's home gateway NAS.

```
user = defcorp_tunnel {  
    password = cisco  
}
```

- **The home gateway NAS profile.** Set the following profile for the DEF Corp's gateway NAS, NAS_DEFCORP:

```
user = NAS_DEFCORP {  
    password = cisco  
}
```

TACACS+ Profiles to Set Up at the Customer-Run Home Gateway ACS

Set up a profile for each VPDN user logging in to the home gateway NAS and set up special NAS profiles at the DEF_Corp home gateway ACS (ACS_DEFCORP).

- **A profile for each VPDN user logging in to the home gateway NAS.** If the optional domain stripping feature has been configured for the home gateway ACS (see the “Supporting ACS AAA Domain Web Page Configuration” section on page 12-25), this one profile will support the same user whether that user is dialing in directly to NAS_DEFCORP or dialing in through the remote NAS_ISP. The following profile specifies the user, jacobw:

```
user = jacobw {  
    password=sesame8  
    service = ppp {  
        protocol = ip  
        protocol = lcp  
        protocol = multilink  
    }  
}
```

- **The tunnel ID profile.** The following profile specifies the tunnel to DEF Corp's home gateway NAS:

```
user = defcorp_tunnel {  
    password = cisco  
}
```

- **The home gateway NAS profile.** Set the following profile for the home gateway NAS, NAS_DEFCORP:

```
user = NAS_DEFCORP{  
    password =  
    cisco  
}
```

Supporting ACS AAA Domain Web Page Configuration

To support the optional domain name stripping described in this example, use the CiscoSecure ACS Administration **AAA>Domain** web page at both the ISP-run ACS (in this case ACS_ISP) and the VPDN home ACS (in this case ACS_DEFCORP) to specify the "@DEF_Corp" domain name as local or remote.

- In the AAA>Domain web page for the ISP-run ACS, ACS_ISP, specify the following settings:
 - Domain Name: **DEF_Corp**
 - Delimiter: **@**
 - Domain Name Position: **After**
 - Domain Type: **Remote**

At the ISP-run ACS, this setting strips off the locally meaningless "jacobw@" from the login string and uses the remaining domain name portion to associate session accounting information with the correct customer profile, in this case, DEF_Corp.

Note This configuration is required if you want to enforce VPDN max sessions settings as described in the chapter "Limiting and Tracking Sessions Per User, Group, or VPDN."

TACACS+ ISP NAS Support for the VPDN

- In the AAA>Domain web page for the DEF Corp-run ACS, ACS_DEFCORP, specify the following settings:
 - Domain Name: **DEF_Corp**
 - Delimiter: **@**
 - Domain Name Position: **After**
 - Domain Type: **Local**

Note At the home gateway ACS, this configuration allows user jacobw to use one login string, “jacobw@DEF_Corp” at either a remote NAS or the home gateway NAS.

TACACS+ ISP NAS Support for the VPDN

To support the VPDN, the following configuration is set up at the ISP-run NAS (NAS_ISP):

```
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS_ISP
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin tacacs+
aaa authentication ppp default local
aaa authentication ppp dialin if-needed tacacs+
aaa authorization network tacacs+
aaa accounting exec start-stop tacacs+
aaa accounting network start-stop tacacs+
!
! Enabling AAA services
!
enable secret cisco
!
```

```
username admin password cisco
!
vpdn enable
!
! enables vpdn connections
!
! vpdn search-order domain dnis
!
! If this example were for an ISP NAS
! running Cisco IOS 11.3 or later, you
! require the following string after
! "vpdn enable" in order to change the
! change the default Dialed-number
! information server(DNIS) VPDN search
! order.
!
async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!
controller T1 0
    framing esf
    clock source line primary
    linecode b8zs
    pri-group timeslots 1-24
!
controller T1 1
    framing esf
    clock source line secondary
    linecode b8zs
    pri-group timeslots 1-24
!
interface Loopback0
    ip address 10.1.2.254 255.255.255.0
!
interface Ethernet0
    ip address 10.1.1.10 255.255.255.0
    ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial0
    no ip address
    shutdown
!
```

```
interface Serial1
  no ip address
  shutdown
!
interface Serial0:23
  no ip address
  encapsulation ppp
  isdn incoming-voice modem
  dialer rotary-group 0
  dialer-group 1
  no fair-queue
  no cdp enable
!
interface Serial1:23
  no ip address
  encapsulation ppp
  isdn incoming-voice modem
  dialer rotary-group 0
  dialer-group 1
  no fair-queue
  no cdp enable
!
interface Group-Async1
  ip unnumbered Loopback0
  encapsulation ppp
  async mode interactive
  peer default ip address pool dialin_pool
  no cdp enable
  ppp authentication chap pap dialin
  group-range 1 48
!
interface Dialer0
  ip unnumbered Loopback0
  no ip mroute-cache
  encapsulation ppp
  peer default ip address pool dialin_pool
  dialer in-band
  dialer-group 1
  no fair-queue
  no cdp enable
  ppp authentication chap pap dialin
  ppp multilink
!
```

```
router eigrp 10
 network 10.0.0.0
 passive-interface Dialer0
 no auto-summary
!
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1
ip classless
tacacs-server host 10.1.3.60
tacacs-server key letmein
tacacs-timeout 20
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line 1 48
 autoselect ppp
 autoselect during-login
 login authentication dialin
 modem DialIn
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

TACACS+ Home Gateway NAS Support

To support the VPDN, the following configuration is set up at the DEF_Corp home gateway, NAS_DEFCORP:

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname NAS_DEFCORP  
!  
aaa new-model  
aaa authentication login default tacacs+ enable  
aaa authentication ppp default tacacs+  
aaa authorization exec tacacs+ if-authenticated  
aaa authorization commands 15 tacacs+ if-authenticated  
aaa authorization network tacacs+  
aaa accounting exec start-stop tacacs+  
aaa accounting network start-stop tacacs+  
!  
vpdn enable  
!  
vpdn incoming defcorp_tunnel NAS_DEFCORP virtual-template 1  
!  
! Specifies the virtual device through which NAS_DEFCORP  
! receives tunneled login data from NAS_ISP.  
!  
interface Ethernet0  
 ip address 4.1.1.1 255.255.255.0  
!  
interface Ethernet1  
 no ip address  
 shutdown  
!  
interface Serial0  
 ip address 10.10.1.1 255.255.255.252  
 encapsulation ppp  
!  
interface Serial1  
 no ip address  
 shutdown  
!
```

```
interface Serial2
  no ip address
  shutdown
!
interface Serial3
  no ip address
  shutdown
!
interface Virtual-Template 1
ip unnumbered Ethernet0
peer default ip address pool corp1_pool
ppp authentication chap pap
ppp multilink
!
! Defines the virtual port through
! which tunneled login requests from
! NAS_ISP are received by NAS_DEFCORP
!
router eigrp 2
  network 2.0.0.0
  no auto-summary
!
ip local pool corp1_pool 4.1.1.3 4.1.1.52
ip classless
tacacs-server host 4.1.1.60
tacacs-server key arachnid
!
line con 0
line aux 0
line vty 0 4
```

Verifying the TACACS+ VPDN Setup

Verify the success of the VPDN example setup as follows:

- Step 1** At a Windows workstation, use the Microsoft dial-up networking client software to dial in to NAS_ISP as user jacobw@DEF_Corp with password, sesame8.

If you can connect, the VPDN is up and working.

- Step 2** If you are unable to connect, enter the following commands at both NASes to enable VPDN and AAA debugging:

```
debug vpdn 12f-errors
debug vpdn 12f-events

debug aaa authorization
debug aaa authentication
debug aaa accounting
debug tacacs
show tacacs
```

RADIUS—VPDN Example

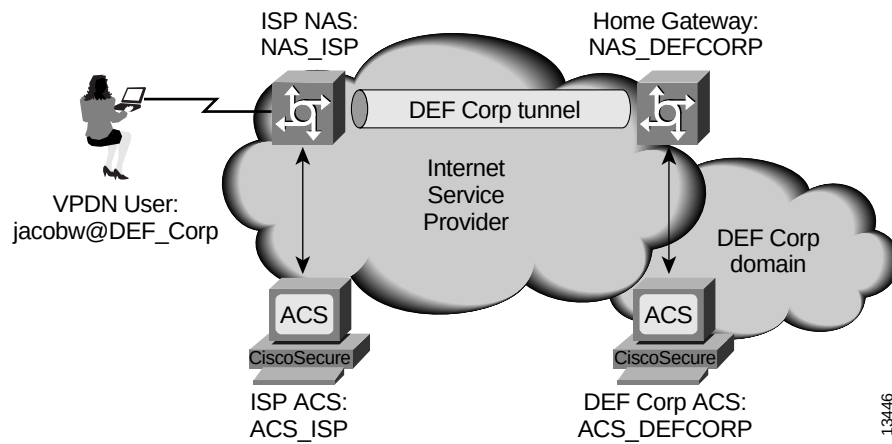
The following sample VPDN profiles, user profiles, and NAS configurations set up a virtual private dial-up network (VPDN) within a larger ISP network and support users that are logging in to a virtual private dial-up network.

In the following sample illustration:

- 1 User jacobw, a DEF Corp employee, whose user profile in a company database is accessible only by the DEF Corp ACS, dials in to the ISP network through the ISP-run NAS (NAS_ISP), as **jacobw@DEF_Corp**, DEF_Corp being a VPDN set up by the ISP.
- 2 The ISP NAS (NAS_ISP) strips off “jacobw@” from the login string and forwards an authorization request for DEF_Corp to the ISP-run ACS (ACS_ISP), which has a VPDN profile for DEF_Corp already configured.
- 3 ACS_ISP returns DEF_Corp VPDN profile information to NAS_ISP, which engages in a two-way authentication process with the DEF Corp home gateway NAS (NAS_DEFCORP) and, if successful, establishes a VPDN tunnel to NAS_DEFCORP.

- 4 The “jacobw@DEF_Corp” login string is forwarded from NAS_ISP through the VPDN tunnel to NAS_DEFCORP and then to CiscoSecure ACS for NAS_DEFCORP, (ACS_DEFCORP), which is configured through CiscoSecure administration web page settings to strip off “@DEF_Corp” and authenticate “jacobw” from the DEF Corp database of authorized users.

Figure 12-2 Sample User Login to a VPDN



RADIUS Profiles to Set Up at the ISP ACS

To support the above scenario, you need to set up some special profiles at the ISP gateway ACS and at the home gateway ACS.

Set up a special VPDN profile and special NAS profiles at the CiscoSecure ACS_ISP.

- **The VPDN Profile.** The following profile specifies the VPDN, DEF_Corp:

```
user = DEF_Corp {
    radius = Cisco {
        check_items = {
            2 = cisco {
            }
        }
        reply_attributes = {
            6= 5
            9,1 = "vpdn:gw-password=cisco"
            9,1 = "vpdn:nas-password=cisco"
            9,1 = "vpdn:ip-addresses=10.10.1.1"
            9,1 = "vpdn:tunnel-id=defcorp_tunnel"
        }
    }
}
```

Note **2=cisco** translates to password = cisco in RADIUS. **6=5** translates to type = outbound-user (for security); **9,1 = "vpdn: ipaddresses=** specifies the IP address of DEF Corp's home gateway NAS; **9,1 = "vpdn: tunnel-id=** is an arbitrary character string; **9,1 = "vpdn: nas-password=** specifies the password for the tunnel-ID profile; **9,1 = "vpdn: gw-password=** specifies the password for the home gateway NAS profile.

RADIUS Profiles to Set Up at the Home Gateway ACS

Set up a profile for each VPDN user logging in to the home gateway NAS and set up special NAS profiles at the DEF_Corp home gateway ACS (ACS_DEFCORP).

- **A profile for each VPDN user logging in to the home gateway NAS.** If the optional domain stripping feature has been configured for the home gateway ACS (see the "Supporting ACS AAA Domain Web Page Configuration" section on page 12-36), this

one profile will support the same user whether that user is dialing in directly to NAS_DEFCORP or dialing in through the remote NAS_ISP. The following profile specifies the user, jacobw.

```
user = jacobw {  
    radius=cisco {  
        check_items = {  
            2=cisco  
        }  
        reply_items = {  
            6=2  
            7=1  
        }  
    }  
}
```

- **The tunnel ID profile.** The following profile specifies the tunnel to DEF Corp's home gateway NAS:

```
user = defcorp_tunnel{  
    radius = cisco {  
        check_items = {  
            2 = cisco  
        }  
    }  
}
```

Supporting ACS AAA Domain Web Page Configuration

To support the optional domain name stripping described in this example, use the CiscoSecure ACS Administration **AAA>Domain** web page at both the ISP-run ACS (in this case ACS_ISP) and the VPDN home ACS (in this case ACS_DEFCORP) to specify the “@DEF_Corp” domain name as local or remote.

- In the AAA>Domain web page for the ISP-run ACS, ACS_ISP, specify the following settings:
 - Domain Name: **DEF_Corp**
 - Delimiter: **@**
 - Domain Name Position: **After**
 - Domain Type: **Remote**

At the ISP-run ACS, this setting strips off the locally meaningless “jacobw@” from the login string and uses the remaining domain name portion to associate session accounting information with the correct customer profile, in this case, DEF_Corp.

Note This configuration is required if you want to enforce VPDN Max Sessions settings as described in the chapter “Limiting and Tracking Sessions Per User, Group, or VPDN.”

- In the AAA>Domain web page for the DEF Corp-run ACS, ACS_DEFCORP, specify the following settings:
 - Domain Name: **DEF_Corp**
 - Delimiter: **@**
 - Domain Name Position: **After**
 - Domain Type: **Local**

Note At the home gateway ACS, this configuration allows user jacobw to use one login string, “jacobw@DEF_Corp” at either a remote NAS or the home gateway NAS.

RADIUS ISP NAS Support for the VPDN

To support the VPDN, the following configuration is set up at the ISP gateway NAS (NAS_ISP).

Note Because this is a RADIUS example, you must make sure this NAS has been associated with its ACS using the Java-based CiscoSecure Administrator advanced configuration program. Start the CiscoSecure Administrator, click the NAS tab, and specify the IP address and shared secret of the ISP gateway NAS. See the “Adding and Configuring NASes as RADIUS Clients” section on page 5-5 in the chapter “ACS and NAS Management.”

```
version 11.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS_ISP
!
aaa new-model
aaa authentication login default radius
aaa authentication login console enable
aaa authentication login vty local
aaa authentication login dialin radius
aaa authentication ppp default radius
aaa authentication ppp dialin if-needed radius
aaa authorization network radius
aaa accounting exec start-stop radius
aaa accounting network start-stop radius
enable secret cisco
!
username admin password cisco
!
vpdn enable
! enables vpdn connections
!
```

RADIUS—VPDN Example

```
! vpdn search-order domain dnis
!
! If this example were for an ISP NAS
! running Cisco IOS 11.3 or later, you
! require the following string after
! "vpdn enable" in order to change the
! change the default Dialed-number
! information server(DNIS) VPDN search
! order.
!
async-bootp dns-server 10.1.3.1 10.1.3.2
isdn switch-type primary-5ess
!

controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.1.2.254 255.255.255.0
!
interface Ethernet0
 ip address 10.1.1.10 255.255.255.0
 ip summary address eigrp 10 10.1.2.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
```

```
interface Serial0:23
  no ip address
  encapsulation ppp
  isdn incoming-voice modem
  dialer rotary-group 0
  dialer-group 1
  no fair-queue
  no cdp enable
!
interface Serial1:23
  no ip address
  encapsulation ppp
  isdn incoming-voice modem
  dialer rotary-group 0
  dialer-group 1
  no fair-queue
  no cdp enable
!
interface Group-Async1
  ip unnumbered Loopback0
  encapsulation ppp
  async mode interactive
  peer default ip address pool dialin_pool
  no cdp enable
  ppp authentication chap pap dialin
  group-range 1 48
!
interface Dialer0
  ip unnumbered Loopback0
  no ip mroute-cache
  encapsulation ppp
  peer default ip address pool dialin_pool
  dialer in-band
  dialer-group 1
  no fair-queue
  no cdp enable
  ppp authentication chap pap dialin
  ppp multilink
!
router eigrp 10
  network 10.0.0.0
  passive-interface Dialer0
  no auto-summary
!
```

RADIUS—VPDN Example

```
ip local pool dialin_pool 10.1.2.1 10.1.2.50
ip default-gateway 10.1.1.1
ip classless

radius-server host 10.1.3.60 auth-port 1645 acct-port 1646
radius-server key letmein
radius timeout 20
!
dialer-list 1 protocol ip permit
!
line con 0
 login authentication console
line 1 48
 autoselect ppp
 autoselect during-login
 login authentication dialin
 modem DialIn
line aux 0
 login authentication console
line vty 0 4
 login authentication vty
 transport input telnet rlogin
!
end
```

RADIUS Home Gateway NAS Support

To support the VPDN, the following configuration is set up at the DEF_Corp home gateway, NAS_DEFCORP.

Note The tunnel cannot be initially authenticated using RADIUS. You must use the line “AAA authentication PPP default radius local” and have local user accounts for the tunnel-id and home gateway identifier on the home gateway NAS. You must also configure the tunnel-id profile in the ACS.

```
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname NAS_DEFCORP
!
aaa new-model
aaa authentication login default radius enable
aaa authentication ppp default radius local
! Required to support local tunnel
! authentication in RADIUS
!
aaa authorization exec radius if-authenticated
aaa authorization commands 15 radius if-authenticated
aaa authorization network radius
aaa accounting exec start-stop radius
aaa accounting network start-stop radius
!!
username NAS_DEFCORP pass cisco
! Sets up a local NAS account for the
! home gateway NAS

username defcorp_tunnel pass cisco
! Sets up a local NAS account for the
! VPDN tunnel
!
vpdn enable
vpdn incoming defcorp_tunnel NAS_DEFCORP virtual-template 1
! Specifies the virtual device through which NAS_DEFCORP
! receives tunneled login data from NAS_ISP.
```

RADIUS—VPDN Example

```
!  
interface Ethernet0  
  ip address 4.1.1.1 255.255.255.0  
!  
interface Ethernet1  
  no ip address  
  shutdown  
!  
interface Serial0  
  ip address 10.10.1.1 255.255.255.252  
  encapsulation ppp  
!  
interface Serial1  
  no ip address  
  shutdown  
!  
interface Serial2  
  no ip address  
  shutdown  
!  
interface Serial3  
  no ip address  
  shutdown  
!  
interface Virtual-Template 1  
  ip unnumbered Ethernet0  
  peer default ip address pool corp1_pool  
  ppp authentication chap pap  
  ppp multilink  
!  
! Defines the virtual tty port through  
! which tunneled login requests from  
! NAS_ISP are received by NAS_DEFCORP  
!  
router eigrp 2  
  network 2.0.0.0  
  no auto-summary  
!  
ip local pool corp1_pool 4.1.1.3 4.1.1.52  
ip classless  
radius-server host 4.1.1.60  
radius-server key arachnid  
radius timeout 20
```

```
!  
!  
line con 0  
line aux 0  
line vty 0 4
```

Verifying the RADIUS VPDN Setup

Verify the success of the VPDN example setup as follows:

- Step 1** At a Windows workstation, use the Microsoft dial-up networking client software to dial in to NAS_ISP as user jacobw@DEF_Corp with password, sesame8.

If you can connect, the VPDN is up and working.

- Step 2** If you are unable to connect, enter the following commands at both NASes to enable VPDN debugging:

```
debug vpdn 12f-errors  
debug vpdn 12f-events  
  
debug aaa authorization  
debug aaa authentication  
debug aaa accounting  
debug radius
```

Combined TACACS+ and RADIUS VPDN Implementation

The two previous sections, “TACACS+—VPDN Example” and “RADIUS—VPDN Example,” provide examples supporting VPDN implementation on homogenous security protocol systems, in which the remote ISP-run NAS/ACS sites and the VPDN home gateway NAS/ACS sites are both configured totally for TACACS+ or totally configured for RADIUS.

However, CiscoSecure also supports heterogeneous networks in which, for example, the remote ISP-run NAS/ACS site is TACACS+ configured, and the VPDN home gateway NAS/ACS site is RADIUS configured or vice-versa. As long as you configure your ISP-run NAS/ACS sites and VPDN home gateway NAS/ACS sites according to the examples in the

Combined TACACS+ and RADIUS VPDN Implementation

section “TACACS+—VPDN Example” or “RADIUS—VPDN Example” and keep the tunnel naming and passwords consistent, VPDN connectivity between the TACACS+—configured site and the RADIUS—configured site will be preserved.