

Dial-in VPDN Configuration Using VPDN Groups and TACACS+

Document ID: 10355

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document provides a sample configuration for dial-in Virtual Private Dialup Networks (VPDN), using VPDN groups and Terminal Access Controller Access Control System Plus (TACACS+).

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

You need to have:

- A Cisco router for client access (NAS/LAC), and a Cisco router for network access (HGW/LNS) with IP connectivity between them.
- Host names of the routers, or local names to use on the VPDN groups.
- The tunneling protocol to use. This can be either Layer 2 Tunneling (L2T) protocol, or Layer 2 Forwarding (L2F) protocol.
- A password for the routers to authenticate tunnel.
- A tunneling criterion. This could be either the domain name, or the Dialed Number Identification Service (DNIS).
- User names and passwords for the user (client dialing in).
- IP addresses and keys for your TACACS+ servers.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

For a detailed introduction to Virtual Private Dialup Networks (VPDN) and VPDN groups, see Understanding VPDN. This document expands on the VPDN configuration, and adds Terminal Access Controller Access Control System Plus (TACACS+).

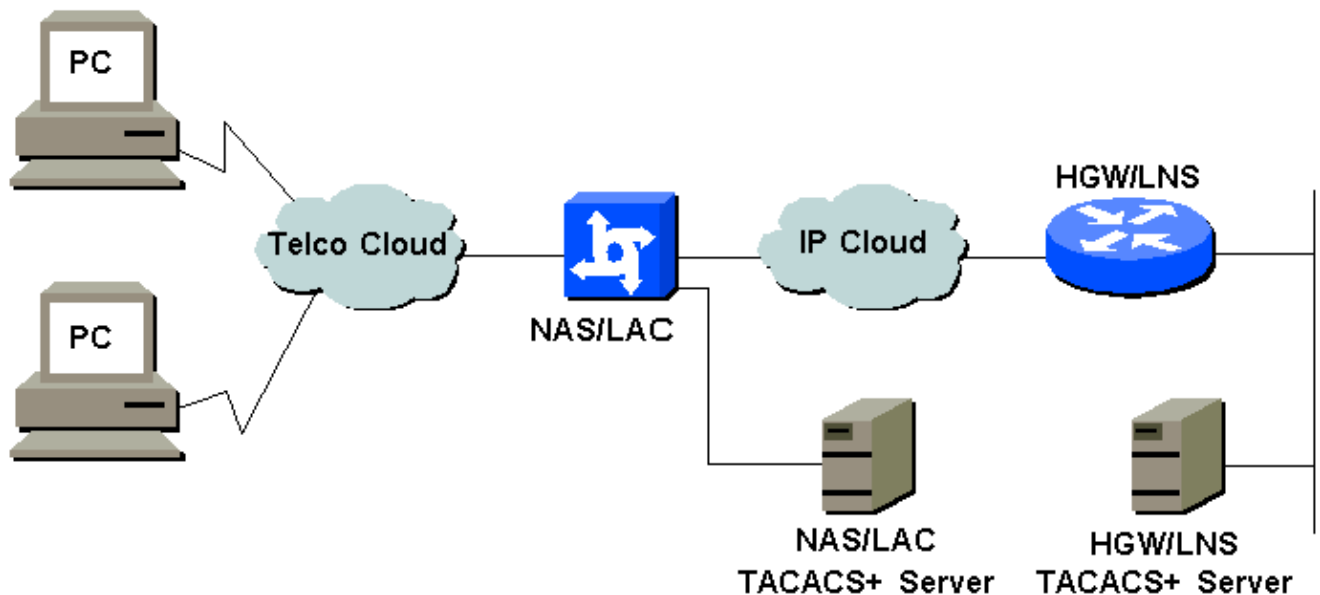
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- NAS/LAC
- HGW/LNS
- NAS/LAC TACACS+ Config File
- HGW/LNS TACACS+ Config File

NAS/LAC

```
!  
version 12.0  
service timestamps debug datetime msec  
service timestamps log datetime msec  
!  
hostname as5300  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication login CONSOLE none  
aaa authentication ppp default if-needed group tacacs+  
aaa authorization network default group tacacs+  
enable password somethingSecret  
!  
username john password 0 secret4me  
!  
ip subnet-zero  
!  
vpdn enable  
!  
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 1  
    linecode b8zs  
    pri-group timeslots 1-24  
!  
controller T1 2  
    framing esf  
    linecode b8zs  
    pri-group timeslots 1-24  
!  
controller T1 3  
    framing esf  
    linecode b8zs  
    pri-group timeslots 1-24  
!  
interface Ethernet0  
    ip address 172.16.186.52 255.255.255.240  
    no ip directed-broadcast  
!  
interface Serial023  
    no ip address  
    no ip directed-broadcast  
    encapsulation ppp  
    ip tcp header-compression passive  
    dialer rotary-group 1  
    isdn switch-type primary-5ess  
    isdn incoming-voice modem  
    no cdp enable  
!  
interface Serial123  
    no ip address  
    no ip directed-broadcast  
    encapsulation ppp  
    ip tcp header-compression passive  
    dialer rotary-group 1
```

```
isdn switch-type primary-5ess
isdn incoming-voice modem
no cdp enable
!
interface Serial223
no ip address
no ip directed-broadcast
encapsulation ppp
ip tcp header-compression passive
dialer rotary-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no cdp enable
!
interface Serial323
no ip address
no ip directed-broadcast
encapsulation ppp
ip tcp header-compression passive
dialer rotary-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no cdp enable
!
interface FastEthernet0
no ip address
no ip directed-broadcast
shutdown
!
interface Group-Async1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
ip tcp header-compression passive
async mode interactive
peer default ip address pool IPAddressPool
no cdp enable
ppp authentication chap
group-range 1 96
!
interface Dialer1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
ip tcp header-compression passive
dialer-group 1
peer default ip address pool IPAddressPool
no cdp enable
ppp authentication chap
!
ip local pool IPAddressPool 10.10.10.1 10.10.10.254
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.186.49
!
tacacs-server host 172.16.171.9
tacacs-server key 2easy
!
line con 0
login authentication CONSOLE
transport input none
line 1 96
autoselect during-login
autoselect ppp
modem Dialin
line aux 0
```

```
line vty 0 4
!
end
```

HGW/LNS

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname access-9
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password somethingSecret
!
ip subnet-zero
!
vpdn enable
!
vpdn-group DEFAULT
! Default L2TP VPDN group
  accept-dialin
  protocol any
  virtual-template 1
  local name LNS
  lcp renegotiation always
  l2tp tunnel password 0 not2tell
!
vpdn-group POP1
  accept-dialin
  protocol l2tp
  virtual-template 2
  terminate-from hostname LAC
  local name LNS
  l2tp tunnel password 0 2secret
!
vpdn-group POP2
  accept-dialin
  protocol l2f
  virtual-template 3
  terminate-from hostname NAS
  local name HGW
  lcp renegotiation always
!
interface FastEthernet0/0
  ip address 172.16.186.1 255.255.255.240
  no ip directed-broadcast
!
interface Virtual-Template1
  ip unnumbered FastEthernet0/0
  no ip directed-broadcast
  ip tcp header-compression passive
  peer default ip address pool IPaddressPool
  ppp authentication chap
!
interface Virtual-Template2
  ip unnumbered Ethernet0/0
  no ip directed-broadcast
  ip tcp header-compression passive
```

```

peer default ip address pool IPAddressPoolPOP1
compress stac
ppp authentication chap
!
interface Virtual-Template3
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPAddressPoolPOP2
 ppp authentication pap
 ppp multilink
!
ip local pool IPAddressPool 10.10.10.1 10.10.10.254
ip local pool IPAddressPoolPOP1 10.1.1.1 10.1.1.254
ip local pool IPAddressPoolPOP2 10.1.2.1 10.1.2.254
ip classless
no ip http server
!
tacacs-server host 172.16.186.9
tacacs-server key not2difficult
!
line con 0

login authentication CONSOLE
transport input none
line 97 120
line aux 0
line vty 0 4
!
!
end

```

NAS/LAC TACACS+ Config File

```

key = 2easy

# Use L2TP tunnel to 172.16.186.1 when 4085555100 is dialed
user = dnis:4085555100 {
    service = ppp protocol = vpdn {
        tunnel-id = anonymous
        ip-addresses = 172.16.186.1
        tunnel-type = l2tp
    }
}

# Password for tunnel authentication
user = anonymous {
    chap = cleartext not2tell
}

###

# Use L2TP tunnel to 172.16.186.1 when 4085555200 is dialed
user = dnis:4085555200 {
    service = ppp protocol = vpdn {
        tunnel-id = LAC
        ip-addresses = 172.16.186.1
        tunnel-type = l2tp
    }
}

# Password for tunnel authentication
user = LAC {
    chap = cleartext 2secret
}

```

```

    }

###

# Use L2F tunnel to 172.16.186.1 when user authenticates with cisco.com domain
user = cisco.com {
    service = ppp protocol = vpdn {
        tunnel-id = NAS
        ip-addresses = 172.16.186.1
        tunnel-type = l2f
    }
}

# Password for tunnel authentication
user = NAS {
    chap = cleartext cisco
}

# Password for tunnel authentication
user = HGW {
    chap = cleartext cisco
}

```

HGW/LNS TACACS+ Config File

```

key = not2difficult

# Password for tunnel authentication
user = NAS {
    chap = cleartext cisco
}

# Password for tunnel authentication
user = HGW {
    chap = cleartext cisco
}

user = santiago {
    chap = cleartext letmein

    service = ppp protocol = lcp { }
    service = ppp protocol = ip { }
}

user = santiago@cisco.com {
    global = cleartext letmein

    service = ppp protocol = lcp { }
    service = ppp protocol = multilink { }
    service = ppp protocol = ip { }
}

```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show vpdn tunnel all** displays details of all active tunnels.

- **show user** displays the name of the user who is connected.
- **show interface virtual-access #** enables you to check the status of a particular virtual interface on the HGW/LNS.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

- **debug vpdn l2x-events** displays the dialog between NAS/LAC and HGW/LNS for tunnel or session creation.
- **debug ppp authentication** enables you to check whether a client is passing authentication.
- **debug ppp negotiation** enables you to check whether a client is passing PPP negotiation. You could see what options (such as, callback, MLP, and so on), and what protocols (such as, IP, IPX, and so on) are being negotiated.
- **debug ppp error** displays protocol errors and error statistics, associated with PPP connection negotiation and operation.
- **debug vtemplate** displays the cloning of virtual access interfaces on the HGW/LNS. You can see when the interface is created (cloned from the virtual template) at the beginning of the dialup connection, and when the interface is destroyed when the connection is terminated.
- **debug aaa authentication** enables you to check whether the user or tunnel is being authenticated by the authentication, authorization, and accounting (AAA) server.
- **debug aaa authorization** enables you to check whether the user is being authorized by the AAA server.
- **debug aaa per-user** enables you to check what is applied to each user who is authenticated. This is different from general debugs listed above.

Related Information

- [Technology Support Pages – Dial](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 04, 2010

Document ID: 10355
