使用 VPDN 组与 TACACS+ 对拨入 VPDN 的配置

目录

简介

本文为拨入虚拟专用拨号网络(VPDN)提供一配置示例，使用VPDN组和终端访问控制器访问控制系统加上(TACACS+)。

先决条件

要求

在尝试此配置前，请保证您符合这些要求：

您需要有：

- 访客接入的(NAS/LAC)一个Cisco路由器和网络访问的(HGW/LNS)一个Cisco路由器与在他们之间的IP连通性。
- 使用的路由器的主机名或者本地名在VPDN组。
- 使用的隧道协议。这可以是以隧道传输(L2T)协议或者第二层转发协议的Layer2。
- 路由器的一个密码能验证通道。
- 隧道标准。这能是域名或者拨号号码识别服务(DNIS)。
- 用户名和密码用户的(客户端正在拨号)。
- IP地址和密钥您的TACACS+服务器的。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

关于虚拟专用拨号网络(VPDN)和VPDN组详细的简介，请参阅了解VPDN。本文在VDPN配置展开，并且添加终端访问控制器访问控制系统加上(TACACS+)。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- NAS/LAC
- HGW/LNS
- NAS/LAC TACACS+配置文件
- HGW/LNS TACACS+配置文件

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+配置文件

```
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+配置文件

```
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 { }
       }
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- 所有活动通道**show vpdn tunnel全**显示详细信息。
- **show users** —显示连接用户的名称。
- **show interface virtual-access -** —使您检查一个特殊虚拟接口的状况在HGW/LNS的。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug vpdn l2x-events** —显示在NAS/LAC和HGW/LNS之间的对话通道或会话创建的。
- **debug ppp authentication** —使您证实客户端是否通过验证。
- **debug ppp协商**—使您证实客户端是否通过PPP协商。您可能发现什么选项(例如，回拨，MLP，等等)，并且什么协议(例如， IP， IPX，等等)协商。
- **debug ppp error** —显示协议错误和错误统计信息，关联与PPP连接协商和操作。
- **debug vtemplate** —显示虚拟访问接口克隆在HGW/LNS的。您能看到，当接口在拨号连接初创建(克隆从虚拟模板)时，并且，当接口毁坏时，当连接是termitated时。
- **debug aaa authentication** —使您证实用户或通道是否由验证、授权和统计(AAA)服务器验证。
- **debug aaa authorization** —使您证实用户是否由AAA服务器授权。
- **debug aaa per-user** —使您检查什么应用给验证的每个用户。这是与以上所列的一般调试不同。

相关信息

- 技术支持页-拨号
- 技术支持 - Cisco Systems