在没有域或 DNIS 信息的情况下配置每用户的 VPDN

目录

简介

本文档为没有域或DNIS信息的每用户VPDN提供配置示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS®软件版本12.1(4)或更高版本。
- 思科IOS软件版本12.1(4)T或更高版本。

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

在虚拟专用拨号网络(VPDN)场景中，网络接入服务器(NAS)（L2TP接入集中器或LAC）根据用户特定信息建立到家庭网关(LNS)的VPDN隧道。此VPDN隧道可以是第2级转发(L2F)或第2层隧道协议(L2TP)。 要确定用户是否应使用VPDN隧道，请检查：

- 域名是否包含在用户名中。例如，使用用户名tunnelme@cisco.com,NAS将此用户转发到cisco.com的隧道。
- 拨号号码信息服务(DNIS)。 这是基于被叫号码的呼叫转移。这意味着NAS可以将具有特定被叫号码的所有呼叫转接到相应的隧道。例如，如果来电的被叫号码为5551111，则呼叫可以转接到VPDN隧道，而呼叫5552222的呼叫不会转接。此功能要求Telco网络提供被叫号码信息。

有关VPDN配置的详细信息，请参阅了解VPDN。

在某些情况下，您可能需要按用户名启动VPDN隧道，无论是否需要域名。例如，用户**ciscouser**可以通过隧道传**输到cisco.com**，而其他用户可以在NAS上本地终止。

注意：此用户名不包括上例中的域信息。

VPDN每用户配置功能在路由器首次联系AAA服务器时将整个结构化用户名发送到身份验证、授权和记帐(AAA)服务器。这使Cisco IOS软件能够为使用公用域名或DNIS的个人用户自定义隧道属性。

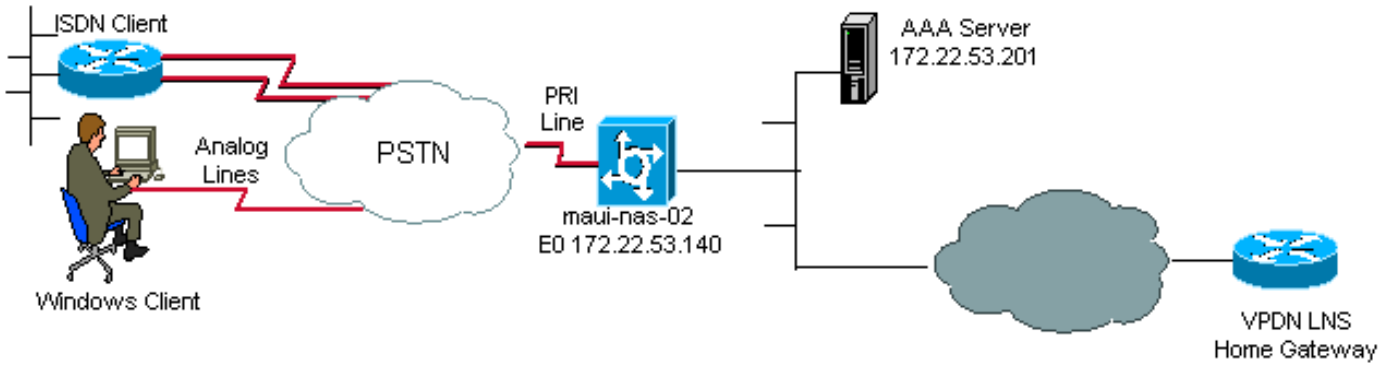
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用以下网络设置：



配置

NAS(LAC)上支持每用户VPDN的唯一必要VPDN命令是全局配置命令**vpdn enable**和**vpdn authen-**

beforward。vpdn authen-before-forward命令指示NAS(LAC)在做出转发决策之前对完整用户名进行身份验证。然后，根据AAA服务器为此个别用户返回的信息，建立VPDN隧道；如果AAA服务器未返回VPDN信息，则用户在本地终止。本节中的配置显示了在用户名中没有域信息的情况下支持隧道所需的命令。

注意：此配置不全面。仅包含相关VPDN、接口和AAA命令。

注意：讨论每个可能的隧道协议和AAA协议已超出本文档的范围。因此，此配置使用AAA RADIUS服务器实施L2TP隧道。根据此处讨论的原则和配置来配置其他隧道类型或AAA协议。

本文档使用以下配置：

- VPDN NAS(LAC)

VPDN NAS(LAC)

```
aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
server host. !--- This AAA server will supply the
NAS(LAC) with the VPDN attributes for the user. radius-
server key cisco !--- The RADIUS server key.
```

RADIUS 服务器配置

以下是Cisco Secure for Unix(CSU)RADIUS服务器上的一些用户配置：

1. 要在NAS上本地终止的用户：
   ```
   user1 Password = "cisco"
   Service-Type = Framed-User
   ```
2. 应为其建立VPDN会话的用户：
   ```
   user2           Password = "cisco"
   Service-Type = Framed-User,
   Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
   Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
   Cisco-AVPair = "vpdn:tunnel-type=l2tp"
   ```

NAS(LAC)使用Cisco-AVPair VPDN指定的属性来启动到家庭网关的VPDN隧道。确保将家庭网关配置为接受来自NAS的VPDN隧道。

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。**

- **show caller user** — 显示特定用户的参数，如使用的TTY线路、异步接口（机架、插槽或端口）、DS0通道号、调制解调器号、分配的IP地址、PPP和PPP捆绑参数等。如果您的Cisco IOS版本不支持本命令，请使用show user命令。
- **show vpdn** — 显示有关VPDN中活动L2F和L2TP协议隧道和消息标识符的信息。

show 命令输出示例

当呼叫连接时，使用**show caller user username*命***令和show vpdn命令来验证呼叫是否成功。输出示例如下所示：

```
maui-nas-02#show caller user vpdn_authen

  User: vpdn_authen, line tty 12, service Async
        Active time 00:09:01, Idle time 00:00:05
  Timeouts:            Absolute  Idle      Idle
                                 Session   Exec
      Limits:          -         -         00:10:00
      Disconnect in:   -         -         -
  TTY: Line 12, running PPP on As12
  DS0: (slot/unit/channel)=0/0/5
  Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
  Status: Ready, Active, No Exit Banner, Async Interface Active
          HW PPP Support Active
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
                Modem Callout, Modem RI is CD,
                Line is permanent async interface, Integrated Modem
  Modem State: Ready

  User: vpdn_authen, line As12, service PPP
        Active time 00:08:58, Idle time 00:00:05
  Timeouts:            Absolute  Idle
      Limits:          -         -
      Disconnect in:   -         -
  PPP: LCP Open, CHAP (<- AAA)
  IP: Local 172.22.53.140
  VPDN: NAS , MID 4, MID Unknown
        HGW , NAS CLID 0, HGW CLID 0, tunnel open
   !--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no buffer 0 input
errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0 output errors, 0
collisions, 0 interface resets maui-nas-02#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions
6318  3     HGW           est    172.22.53.141   1701  1

LocID RemID TunID Intf       Username      State  Last Chg Fastswitch
4     3     6318  As12       vpdn_authen   est    00:09:33 enabled
!--- The tunnel for user vpdn_authen is in established state. %No active L2F tunnels %No active
PPTP tunnels %No active PPPoE tunnel
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

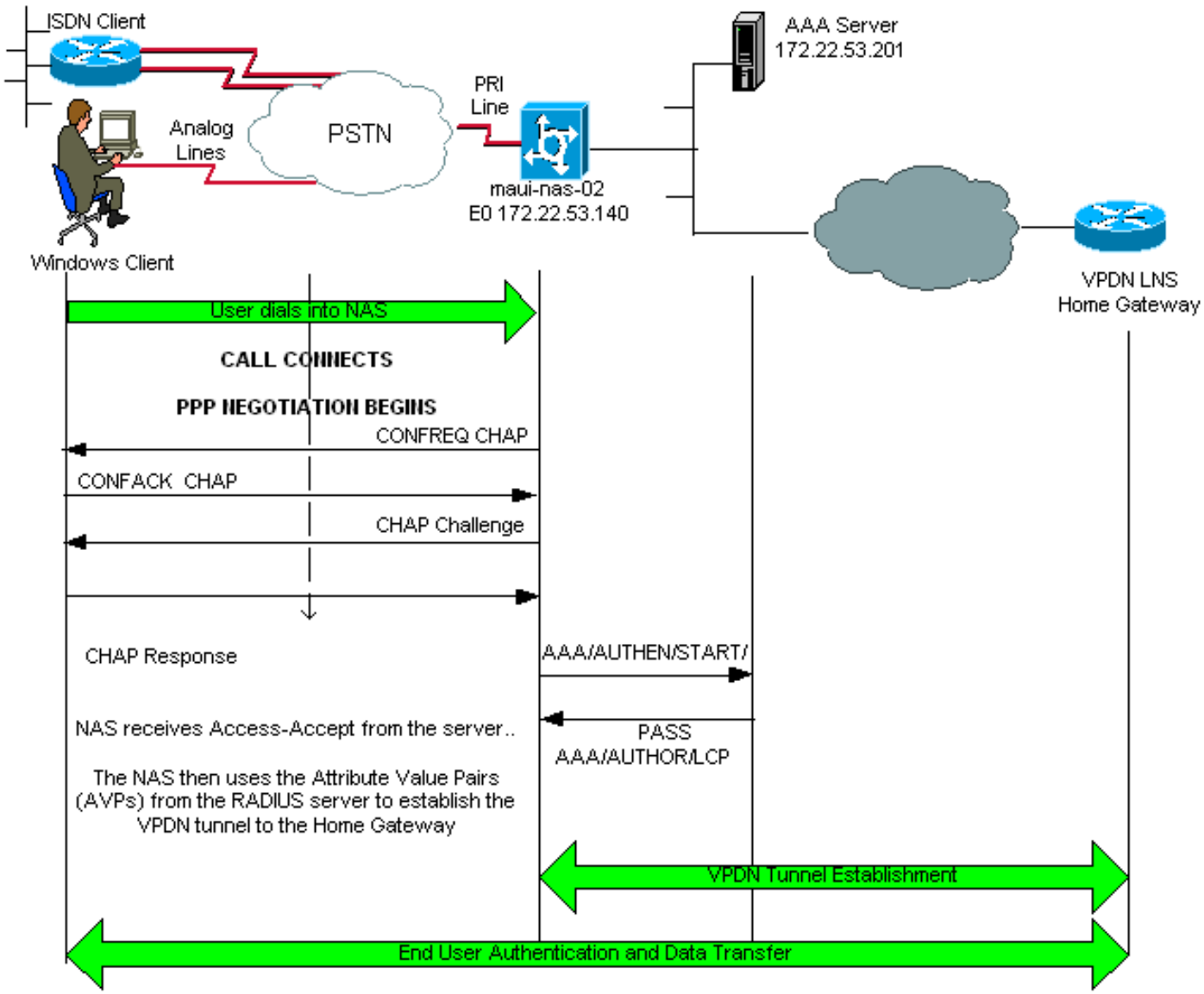
故障排除命令

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

- **debug ppp authentication** — 显示PPP身份验证协议消息，包括质询握手身份验证协议(CHAP)数据包交换和密码身份验证协议(PAP)交换。
- **debug aaa authentication** — 显示有关AAA/RADIUS身份验证的信息。
- **debug aaa authorization** — 显示有关AAA/RADIUS授权的信息。
- **debug radius - 显示与 RADIUS 关联的详细调试信息。**使用输出解释器工具(仅注册客户)解码调试RADIUS消息。例如，请参阅“调试输出示例”部分。使用来自调试**radius的**信息确定要协商的属性。
- **debug tacacs** — 显示与TACACS+关联的详细调试信息。
- **debug vpdn event** — 显示L2x错误和事件，这些错误和事件是VPDN正常隧道建立或关闭的一部分。
- **debug vpdn error** — 显示VPDN协议错误。
- **debug vpdn l2x-event** — 显示VPDN正常隧道建立或关闭过程中的详细L2x错误和事件。
- **debug vpdn l2x-error** — 显示VPDN L2x协议错误。

调试输出示例

以下是成功**调用**的调试输出。在本示例中，请注意，NAS从Radius服务器获取VPDN隧道的属性。




```
maui-nas-02#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
PPP:
  PPP authentication debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is onRadius protocol debugging is on
maui-nas-02#
*Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface Serial0:5 is now connected
to N/A N/A
!--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN: Interface Async12, changed state to up
*Jan 21 19:07:55.352: As12 PPP: Treating connection as a dedicated line *Jan 21 19:07:55.352:
As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21 19:07:55.604: As12 CHAP: O CHALLENGE id
1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12 CHAP: I RESPONSE id 1 len 32 from
"vpdn_authen"
!--- Incoming CHAP response from user vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12
idb type=10 tty=12 *Jan 21 19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=12 channel=0 *Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1
*Jan 21 19:07:55.732: AAA: name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0
channel=5 *Jan 21 19:07:55.732: AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5 *Jan 21
19:07:55.732: AAA/MEMORY: create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12'
```

```
rem_addr='async/81560' authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): port='Async12' list='' action=LOGIN service=PPP *Jan 21
19:07:55.732: AAA/AUTHEN/START (4048817807): using "default" list *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct
sharecount=1 *Jan 21 19:07:55.736: RADIUS: Initial Transmit Async12 id
6 172.22.53.201:1645, Access-Request, len 89
*Jan 21 19:07:55.736:         Attribute 4 6 AC16358C
*Jan 21 19:07:55.736:         Attribute 5 6 0000000C
*Jan 21 19:07:55.736:         Attribute 61 6 00000000
*Jan 21 19:07:55.736:         Attribute 1 13 7670646E
*Jan 21 19:07:55.736:         Attribute 30 7 38313536
*Jan 21 19:07:55.736:         Attribute 3 19 014CF9D6
*Jan 21 19:07:55.736:         Attribute 6 6 00000002
*Jan 21 19:07:55.736:         Attribute 7 6 00000001
*Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645,
Access-Accept, len 136
*Jan 21 19:07:55.740:         Attribute 6 6 00000002
*Jan 21 19:07:55.740:         Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:         Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:         Attribute 26 30 0000000901187670
```

VPDN隧道所需的属性值对(AVP)从RADIUS服务器向下推送。但是，**debug radius**会生成一个编码输出，指示AVP及其值。您可以将上面粗体字**显示的**输出粘贴到输出解释程序工具(仅限注册客户)。 以下粗体输出是从工具获取的解码输出：

```
Access-Request 172.22.53.201:1645 id 6
Attribute Type 4:  NAS-IP-Address is 172.22.53.140
Attribute Type 5:  NAS-Port is 12
Attribute Type 61: NAS-Port-Type is Asynchronous
Attribute Type 1:  User-Name is vpdn
Attribute Type 30: Called-Station-ID(DNIS) is 8156
Attribute Type 3:  CHAP-Password is (encoded)
Attribute Type 6:  Service-Type is Framed
Attribute Type 7:  Framed-Protocol is PPP
        Access-Accept 172.22.53.201:1645 id 6
Attribute Type 6:  Service-Type is Framed
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS
...
...
...
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
*Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
 !--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be
authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !---
the VPDN tunnel establishment debug output is omitted.
```

相关信息

- 了解 VPDN

- 配置虚拟专用拨号网络
- 如何使用RADIUS配置第2层隧道协议身份验证
- 如何使用TACACS+配置第2层隧道协议身份验证
- 接入技术支持页面
- 技术支持 - Cisco Systems