

在没有域或 DNIS 信息的情况下配置每用户的 VPDN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[RADIUS 服务器配置](#)

[验证](#)

[show 命令输出示例](#)

[故障排除](#)

[故障排除命令](#)

[调试输出示例](#)

[相关信息](#)

[简介](#)

本文为每用户VPDN提供一配置示例，不用域或DNIS信息。

[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)或以上。
- Cisco IOS软件版本12.1(4)T或以上。

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)方案、网络接入服务器(NAS) (L2TP接入集中器或者LAC中)设立VPDN通道到根据特定用户信息(LNS)的家用网关。此VPDN通道可以是第2层转发(L2F)或第2层隧道协议。确定用户是否应该使用VPDN通道，检查：

- 域名作为用户名一部分，是否包括。例如，与用户名tunnelme@cisco.com，NAS转发此用户到cisco.com的通道。
- 拨叫号码信息服务(DNIS)。这是根据被叫号码的呼叫转接。这意味着NAS能转发所有呼叫用一个特定的被叫号码到适当的通道。例如，如果呼入呼叫有被叫号码5551111，呼叫可以转发到VPDN通道，而一呼叫到5552222没有转发。此功能要求电信网络提供被叫号码信息。

关于VPDN配置的更多信息，请参阅[了解VPDN](#)。

在某些状况下，您可以要求VPDN通道是根据一个每用户名基本类型的已启动，有或没有对a的需要domain-name。例如，而其他用户在NAS，可能终止本地用户ciscouser可以被建立隧道到cisco.com。

注意： 此用户名在前一个示例不包括域信息正如。

第一次路由器与AAA服务器联系，VPDN每位用户配置功能发送整个结构用户名到验证、授权和统计(AAA)服务器。这使Cisco IOS软件定制使用一个普通的域名或DNIS的个人用户的隧道属性。

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

唯一的VPDN命令必要在NAS (LAC)支持每用户VPDN全局配置命令**vpdn enable**和**vpdn authen-before-forward**。**vpdn authen-before-forward**命令指示NAS (LAC)验证完整用户名，在做出一个转发决策前。VPDN通道根据此个人用户的AAA服务器返回的信息然后设立，;如果VPDN信息没有从AAA服务器返回，用户终止本地。在此部分的配置显示**required**命令支持通道，不用在用户名的域信息。

注意： 此配置不是全面配置。仅相关VPDN、接口和AAA命令包括。

注意： 它是超出讨论每个可能的隧道协议和AAA协议的本文的范围之外。因此，此配置实现一个L2TP通道用AAA RADIUS服务器。适用讨论的原理和配置此处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](#)

这是在 Cisco Secure 的一些用户配置 Unix (CSU) RADIUS 服务器的：

1. 将终止本地 NAS 的用户：

```
user1 Password = "cisco"
Service-Type = Framed-User
```
2. VPDN 会话应该建立的用户：

```
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) 以 Cisco-AVPair VPDN 使用指定的属性发起 VPDN 通道到家用网关。保证您配置家用网关接受从 NAS 的 VPDN 通道。

[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** —表示一个特定用户的参数，例如 TTY 线路使用的，异步接口(架子、slot 或者端口)，DS0 信道编号，调制解调器编号，分配的 IP 地址，PPP 和 PPP 捆绑参数，等等。如果您的 Cisco IOS 版本软件不支持此指令，请使用 **show users** 命令。
- **show vpdn** —显示关于活动 L2F 的信息和 L2TP 协议隧道和消息标识符在 VPDN。

[show 命令输出示例](#)

当呼叫连接使用**show caller user username**命令以及**show vpdn**命令验证呼叫是成功的。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认证协议消息，并且包括质询握手验证协议(CHAP)信息包交换和密码认证协议交换。
- **debug aaa authentication** —显示关于AAA/RADIUS验证的信息。
- **debug aaa authorization** —显示关于AAA/RADIUS授权的信息。
- **debug radius** —显示详细的调试信息关联与RADIUS。请使用[Output Interpreter Tool \(仅限注册用户\)](#)解码debug radius消息。例如，参考[Sample Debug Output部分](#)。请使用从debug radius的信息确定什么属性协商。
- **debug tacacs** —显示详细的调试信息关联与TACACS+。
- **debug vpdn event** —显示是一正常隧道建立的一部分或关闭VPDN的L2x错误和事件。
- **debug vpdn error** —显示VPDN协议错误。
- **debug vpdn l2x-event** —显示是一正常隧道建立的一部分或关闭VPDN的详细的L2x错误和事件。
- **debug vpdn l2x-error** —显示VPDN L2x协议错误。

调试输出示例

这是成功的呼叫的**debug**输出。在本例中，请注意NAS从RADIUS服务器得到VPDN通道的属性。

```
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通道的属性值对(AVPs)必要的从RADIUS服务器增加。然而，`debug radius`生成指示AVPs和他们的值的一被编码的输出。您能粘贴在上面粗体字体显示的输出到[Output Interpreter Tool](#) ([仅限注册用户](#))。在粗体的以下输出是从工具得到的解码的输出：

```
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](#)
- [如何配置与RADIUS的Layer2隧道协议验证](#)
- [如何配置与TACACS+的Layer2隧道协议验证](#)
- [接入技术支持页面](#)
- [技术支持 - Cisco Systems](#)