在 Cisco Secure PIX 防火墙上配置 PPPoE 客户端

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[验证](#)
[故障排除](#)
[故障排除信息](#)
[故障排除命令](#)
[PIX OS 6.2 和 6.3 版本中的已知警告](#)
[PIX OS 6.3 版本中的已知警告](#)
[相关信息](#)

简介

本文档介绍如何在 Cisco Secure PIX 防火墙上配置以太网上的点对点协议 (PPPoE) 客户端。PIX OS 6.2 版引入了此功能，该版本适用于低端 PIX (501/506)。

PPPoE 结合两种广泛接受的标准（以太网和 PPP），以提供一种经过身份验证的向客户端系统分配 IP 地址的方法。PPPoE 客户端通常是通过远程宽带连接（例如 DSL 或电缆服务）连接到 ISP 的个人计算机。ISP 会部署 PPPoE，因为 PPPoE 支持使用其现有的远程访问基础设施进行高速宽带接入，且更便于客户使用。PIX 防火墙 6.2 版引入了 PPPoE 客户端功能。这样使小型办公室、家庭办公室 (SOHO) 中的 PIX 防火墙用户可使用 DSL 调制解调器连接到 ISP。

目前，仅 PIX 的外部接口支持此功能。在外部接口上也进行配置后，将用 PPPoE/PPP 报头封装所有流量。PPPoE 的默认身份验证机制是口令身份验证协议 (PAP)。

PPPoE 提供一种在以太网网络上部署 PPP 身份验证方法的标准方法。ISP 使用该方法时，PPPoE 允许对 IP 地址进行经过身份验证的分配。在这种类型的实现中，PPPoE 客户端和服务器由通过 DSL 或其他宽带连接运行的第 2 层桥接协议互联。

用户可手动选择配置质询握手身份验证协议 (CHAP) 或 MS-CHAP。PIX OS 6.2 和 6.3 版不支持第二层隧道协议 (L2TP) 和点对点隧道协议 (PPTP) 与 PPPoE 配合使用。

PPPoE 由以下两个主要阶段组成：

- 即时发现逐渐采用此相位， PPPoE客户端找出PPPoE服务器，呼叫接入集中器。在此阶段期间，将分配会话 ID 并建立 PPPoE 层。
- PPP会话逐渐采用此相位， PPP选项协商，并且验证执行。完成链路建立后，PPPoE 即充当第 2 层封装方法，从而使数据可以在 PPPoE 报头中通过 PPP 链路进行传输。

在系统初始化时，PPPoE 客户端通过交换一系列的数据包与 AC 建立会话。建立会话后，即建立 PPP 链路，其中包括使用口令身份验证协议 (PAP) 进行身份验证。建立 PPP 会话后，每个数据包会封装在 PPPoE 和 PPP 报头中。

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：

- 含 PIX OS 6.3(4) 版的 PIX 501
- 配置为 PPPoE 服务器的含 Cisco IOS® 软件 12.3(10) 版的 Cisco 1721 路由器

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。

配置

本部分提供了可用于配置本文所述功能的信息。

注意： 要查找有关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。

- Cisco 1721 路由器作为 PPPoE 服务器
- PIX (501 或 506) 作为 PPPoE 客户端

在此实验室测试中，Cisco 1721 路由器充当 PPPoE 服务器。在您的家庭/远程办公室中不需要此设备，因为您的 ISP 将托管 PPPoE 服务器。

Cisco 1721 路由器作为 PPPoE 服务器

```
!--- Username matches that on the PIX. username cisco
password cisco !--- Enable virtual private dial-up
network (VPDN). vpdn enable ! !--- Define the VPDN group
that you use for PPPoE. vpdn-group pppoex accept-dialin
protocol pppoe virtual-template 1 ! interface Ethernet0
ip address 172.21.48.30 255.255.255.224 !--- Enable
PPPoE sessions on the interface. pppoe enable !
interface Virtual-Template1 mtu 1492 !--- Do not use a
static IP assignment within a virtual template since !--
- routing problems can occur. Instead, use the ip
unnumbered command !--- when you configure a virtual
template. ip unnumbered Ethernet0 peer default ip
address pool pixpool !--- Define authentication
protocol. ppp authentication pap ! ip local pool pixpool
11.11.11.1 11.11.11.100
```

PIX (501 或 506) 作为 PPPoE 客户端

```
pix501#write terminal Building configuration... : Saved
: PIX Version 6.3(4) interface ethernet0 10baset
interface ethernet1 100full nameif ethernet0 outside
security0 nameif ethernet1 inside security100 enable
password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted hostname pix501 domain-name
cisco.com fixup protocol dns maximum-length 512 fixup
protocol ftp 21 fixup protocol h323 h225 1720 fixup
protocol h323 ras 1718-1719 fixup protocol http 80 fixup
protocol rsh 514 fixup protocol rtsp 554 fixup protocol
sip 5060 fixup protocol sip udp 5060 fixup protocol
skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet
1521 fixup protocol tftp 69 names pager lines 24 mtu
outside 1500 mtu inside 1500 !--- Enable PPPoE client
functionality on the interface. !--- It is off by
default. The setroute option creates a default !---
route if no default route exists. ip address outside
pppoe setroute ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 global
(outside) 1 interface nat (inside) 1 192.168.1.0
255.255.255.0 0 0 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server TACACS+ max-
failed-attempts 3 aaa-server TACACS+ deadtime 10 aaa-
server RADIUS protocol radius aaa-server RADIUS max-
failed-attempts 3 aaa-server RADIUS deadtime 10 aaa-
server LOCAL protocol local no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable telnet
timeout 5 ssh timeout 5 console timeout 0 !--- Define
the VPDN group that you use for PPPoE. !--- Configure
this first. vpdn group pppoex request dialout pppoe !---
Associate the username that the ISP assigns to the VPDN
group. vpdn group pppoex localname cisco !--- Define
authentication protocol. vpdn group pppoex ppp
```

```
authentication pap !--- Create a username and password
pair for the PPPoE !--- connection (which your ISP
provides). vpdn username cisco password *********
terminal width 80
Cryptochecksum:e136533e23231c5bbbbf4088cee75a5a : end
[OK] pix501#
```

验证

本部分提供的信息可用于确认您的配置是否正常运行。

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 ip address outside pppoe** - 显示当前的 PPPoE 客户端配置信息。
- **show vpdn tunnel pppoe** - 显示特定隧道类型的隧道信息。
- **show vpdn session pppoe** - 显示 PPPoE 会话的状态。
- **show vpdn pppinterface** - 显示 PPPoE 隧道的接口标识值。为每个 PPPoE 隧道创建一个 PPP 虚拟接口。
- **show vpdn group** - 显示为 PPPoE 隧道定义的组。
- **show vpdn username** - 显示本地用户名信息。

以下是 **show ip address outside pppoe** 命令的输出：

```
501(config)#show ip address outside pppoe PPPoE Assigned IP addr: 11.11.11.1 255.255.255.255 on
Interface: outside Remote IP addr: 172.21.48.30
```

以下是 **show vpdn tunnel pppoe** 命令的输出：

```
501(config)#show vpdn tunnel pppoe PPPoE Tunnel Information (Total tunnels=1 sessions=1) Tunnel
id 0, 1 active sessions time since change 20239 secs Remote MAC Address 00:08:E3:9C:4C:71 3328
packets sent, 3325 received, 41492 bytes sent, 0 received
```

以下是 **show vpdn session pppoe** 命令的输出：

```
501(config)#show vpdn session pppoe PPPoE Session Information (Total tunnels=1 sessions=1)
Remote MAC is 00:08:E3:9C:4C:71 Session state is SESSION_UP Time since event change 20294 secs,
interface outside PPP interface id is 1 3337 packets sent, 3334 received, 41606 bytes sent, 0
received
```

以下是 **show vpdn pppinterface** 命令的输出：

```
501(config)#show vpdn pppinterface PPP virtual interface id = 1 PPP authentication protocol is
PAP Server ip address is 172.21.48.30 Our ip address is 11.11.11.1 Transmitted Pkts: 3348,
Received Pkts: 3345, Error Pkts: 0 MPPE key strength is None MPPE_Encrypt_Pkts: 0,
MPPE_Encrypt_Bytes: 0 MPPE_Decrypt_Pkts: 0, MPPE_Decrypt_Bytes: 0 Rcvd_Out_Of_Seq_MPPE_Pkts: 0
```

以下是 **show vpdn group** 命令的输出：

```
501(config)#show vpdn group vpdn group pppoex request dialout pppoe vpdn group pppoex localname
cisco vpdn group pppoex ppp authentication pap
```

以下是 **show vpdn username** 命令的输出：

```
501(config)#show vpdn username vpdn username cisco password *********
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

故障排除信息

以下是 PIX 上常见错误配置中的示例调试。开启这些调试。

```
pix#show debug debug ppp negotiation debug pppoe packet debug pppoe error debug pppoe event
```

- 身份验证故障（例如用户名/口令有误）。Rcvd Link Control Protocol pkt, Action code is: Echo Reply,
  len is: 4 Pkt dump: d0c3305c

  PPP pap recv authen nak: 41757468656e7469636174696f6e206661696c757265 PPP PAP authentication failed Rcvd Link Control Protocol pkt, Action code is: Termination Request, len is: 0
- 身份验证协议无效（例如 PAP/CHAP 配置有误）。
  Xmit Link Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 05064a53ae2a LCP Option: MAGIC_NUMBER, len: 6, data: 4a53ae2a **Rcvd Link Control Protocol pkt, Action code is: Config Request, len is: 14** Pkt dump: 010405d40304c0230506d0c88668 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023 LCP Option: MAGIC_NUMBER, len: 6, data: d0c88668 **Xmit Link Control Protocol pkt, Action code is: Config NAK, len is: 5** Pkt dump: 0305c22305 LCP Option: AUTHENTICATION_TYPES, len: 5, data: c22305 Rcvd Link Control Protocol pkt, Action code is: Config ACK, len is: 6 Pkt dump: 05064a53ae2a LCP Option: MAGIC_NUMBER, len: 6, data: 4a53ae2a
- PPPoE 服务器不响应，每 30 秒重试一次。send_padi:(Snd) Dest:ffff.ffff.ffff Src:0007.5057.e27e T
  ype:0x8863=PPPoE-Discovery

  Ver:1 Type:1 Code:09=PADI Sess:0 Len:12
  Type:0101:SVCNAME-Service Name Len:0
  Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001

  padi timer expired send_padi:(Snd) Dest:ffff.ffff.ffff Src:0007.5057.e27e Type:0x8863=PPPoE-Discovery Ver:1 Type:1 Code:09=PADI Sess:0 Len:12 Type:0101:SVCNAME-Service Name Len:0 Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001 **padi timer expired** send_padi:(Snd) Dest:ffff.ffff.ffff Src:0007.5057.e27e Type:0x8863=PPPoE-Discovery Ver:1 Type:1 Code:09=PADI Sess:0 Len:12 Type:0101:SVCNAME-Service Name Len:0 Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001 **padi timer expired**

故障排除命令

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。

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

- **debug pppoe packet** - 显示数据包信息。
- **debug pppoe error** - 显示错误消息。
- **debug pppoe event** - 显示协议事件信息。
- **debug ppp negotiation** - 使您可以查看客户端是否传递 PPP 协商信息。
- **debug ppp io** -显示PPTP PPP虚拟接口的数据包信息。
- **debug ppp upap** - 显示 PAP 身份验证。
- **debug ppp error**—显示 PPTP PPP 虚拟接口的错误消息。
- **debug ppp chap** - 显示有关客户端是否通过身份验证的信息。

要对 PPPoE 客户端启用调试，请使用以下这些命令：

```
!--- Displays packet information. 501(config)#debug pppoe packet !--- Displays error messages.
501(config)#debug pppoe error !--- Displays protocol event information. 501(config)#debug pppoe
event send_padi:(Snd) Dest:ffff.ffff.ffff Src:0008.a37f.be88 Type:0x8863=PPPoE-Discovery Ver:1
```

Type:1 Code:09=PADI Sess:0 Len:12 Type:0101:SVCNAME-Service Name Len:0 Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001 padi timer expired PPPoE:(Rcv) Dest:0008.a37f.be88 Src:0008.e39c.4c71 Type:0x8863=PPPoE-Discovery Ver:1 Type:1 Code:07=PADO Sess:0 Len:45 Type:0101:SVCNAME-Service Name Len:0 Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001 Type:0102:ACNAME-AC Name Len:9 3640 Type:0104:ACCOOKIE-AC Cookie Len:16 D69B0AAF 0DEBC789 FF8E1A75 2E6A3F1B PPPoE: PADO send_padr:(Snd) Dest:0008.e39c.4c71 Src:0008.a37f.be88 Type:0x8863=PPPoE-Discovery Ver:1 Type:1 Code:19=PADR Sess:0 Len:45 Type:0101:SVCNAME-Service Name Len:0 Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001 Type:0102:ACNAME-AC Name Len:9 3640 Type:0104:ACCOOKIE-AC Cookie Len:16 D69B0AAF 0DEBC789 FF8E1A75 2E6A3F1B PPPoE:(Rcv) Dest:0008.a37f.be88 Src:0008.e39c.4c71 Type:0x8863=PPPoE-Discovery Ver:1 Type:1 Code:65=PADS Sess:1 Len:45 Type:0101:SVCNAME-Service Name Len:0 Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001 Type:0102:ACNAME-AC Name Len:9 3640 Type:0104:ACCOOKIE-AC Cookie Len:16 D69B0AAF 0DEBC789 FF8E1A75 2E6A3F1B PPPoE: PADS IN PADS from PPPoE tunnel PPPoE: Virtual Access interface obtained.PPPoE: Got ethertype=800 on PPPoE interface=outside PPPoE: Got ethertype=800 on PPPoE interface=outside PPPoE: Got ethertype=800 on PPPoE interface=outside

以下输出显示 PPPoE 客户端的其他调试命令：

501(config)#**debug ppp negotiation** 501(config)#**debug ppp io** 501(config)#**debug ppp upap** 501(config)#**debug ppp error PPP virtual access open**, ifc = 0 Xmit Link Control Protocol pkt, Action code is: **Config Request**, len is: 6 Pkt dump: 0506609b39f5 LCP Option: MAGIC_NUMBER, len: 6, data: 609b39f5 PPP xmit, ifc = 0, len: 14 data: ff03c0210101000a0506609b39f5 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c02101010010012010405d40304c023050659d9f6360000000000000000000 00000000000000000000000 **Rcvd Link Control Protocol** pkt, Action code is: **Config Request**, len is: 14 Pkt dump: 010405d40304c023050659d9f636 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023 LCP Option: MAGIC_NUMBER, len: 6, data: 59d9f636 **Xmit Link Control Protocol** pkt, Action code is: **Config ACK**, len is: 14 Pkt dump: 010405d40304c023050659d9f636 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023 LCP Option: MAGIC_NUMBER, len: 6, data: 59d9f636 PPP xmit, ifc = 0, len: 22 data: ff03c02102010010012010405d40304c023050659d9f636 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c02101020010012010405d40304c023050659d9f6360000000000000000000 00000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: **Config Request**, len is: 14 Pkt dump: 010405d40304c023050659d9f636 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023 LCP Option: MAGIC_NUMBER, len: 6, data: 59d9f636 Xmit Link Control Protocol pkt, Action code is: **Config ACK**, len is: 14 Pkt dump: 010405d40304c023050659d9f636 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 4, data: c023 LCP Option: MAGIC_NUMBER, len: 6, data: 59d9f636 PPP xmit, ifc = 0, len: 22 data: ff03c02102020010012010405d40304c023050659d9f636 Xmit Link Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 0506609b39f5 LCP Option: MAGIC_NUMBER, len: 6, data: 609b39f5 PPP xmit, ifc = 0, len: 14 data: ff03c0210101000a0506609b39f5 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0210201000a0506609b39f5000000000000000000000000000000000000 00000000000000000000000 **Rcvd Link Control Protocol pkt**, Action code is: **Config ACK**, len is: 6 Pkt dump: 0506609b39f5 LCP Option: MAGIC_NUMBER, len: 6, data: 609b39f5 Xmit Link Control Protocol pkt, Action code is: Echo Request, len is: 4 Pkt dump: 609b39f5 PPP xmit, ifc = 0, len: 12 data: ff03c02109000008609b39f5 PPP xmit, ifc = 0, len: 20 data: ff03c0230101001001005636973636f05636973636f PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0210a00000859d9f6360000000000000000000000000000000000000000 00000000000000000000000 **Rcvd Link Control Protocol pkt**, Action code is: **Echo Reply**, len is: 4 Pkt dump: 59d9f636 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0230201000500000000000000000000000000000000000000000000000000 00000000000000000000000 PPP upap rcvd authen ack: ff03c023020100050000000000000000000000000000000000000000000000000000000000000000000000000000 00000 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff0380210101000a0306ac15301e000000000000000000000000000000000000 00000000000000000000000 Rcvd IP Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 0306ac15301e IPCP Option: Config IP, IP = 172.21.48.30 Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 030600000000 IPCP Option: Config IP, IP = 0.0.0.0 PPP xmit, ifc = 0, len: 14 data: ff0380210101000a030600000000 Xmit IP Control Protocol pkt, Action code is: Config ACK, len is: 6 Pkt dump: 0306ac15301e IPCP Option: Config IP, IP = 172.21.48.30 PPP xmit, ifc = 0, len: 14 data: ff0380210201000a0306ac15301e PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff0380210301000a03060b0b0b020000000000000000000000000000000000 00000000000000000000000 Rcvd IP Control Protocol pkt, Action code is: **Config NAK**, len is: 6 Pkt dump: 03060b0b0b02 IPCP Option: Config IP, IP = 11.11.11.1 Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 03060b0b0b02 IPCP Option: Config IP, IP = 11.11.11.1 PPP xmit, ifc = 0, len: 14 data: ff0380210102000a03060b0b0b02 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:

ff03c0210901000c59d9f636015995a1000000000000000000000000000000 00000000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: Echo Request, len is: 8 Pkt dump: 59d9f636015995a1 Xmit Link Control Protocol pkt, Action code is: Echo Reply, len is: 8 Pkt dump: 609b39f5015995a1 PPP xmit, ifc = 0, len: 16 data: ff03c0210a01000c609b39f5015995a1 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff0380210202000a03060b0b0b020000000000000000000000000000000000 00000000000000000000000000 Rcvd IP Control Protocol pkt, Action code is: Config ACK, len is: 6 Pkt dump: 03060b0b0b02 IPCP Option: Config IP, IP = 11.11.11.1 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0210902000c59d9f6360159937b000000000000000000000000000000 00000000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: Echo Request, len is: 8 Pkt dump: 59d9f6360159937b Xmit Link Control Protocol pkt, Action code is: Echo Reply, len is: 8 Pkt dump: 609b39f50159937b PPP xmit, ifc = 0, len: 16 data: ff03c0210a02000c609b39f50159937b Xmit Link Control Protocol pkt, Action code is: Echo Request, len is: 4 Pkt dump: 609b39f5 PPP xmit, ifc = 0, len: 12 data: ff03c02109010008609b39f5 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0210a01000859d9f6360000000000000000000000000000000000000000 00000000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: Echo Reply, len is: 4 Pkt dump: 59d9f636

使用 ppp ms-chap 命令进行身份验证时进行调试

配置 PPP MS-CHAP 身份验证时，此线路是您在 PIX 中需要做出的唯一更改（所有其余线路保持不变）。

vpdn group pppoex ppp authentication pap 命令更改为 vpdn group pppoex ppp authentication mschap。

对新的身份验证方法启用调试。

501(config)#**debug ppp negotiation** 501(config)#**debug ppp io** 501(config)#**debug ppp upap** 501(config)#**debug ppp error** 501(config)#**debug ppp chap** PPP virtual access open, ifc = 0 Xmit Link Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 05063ff50e18 LCP Option: MAGIC_NUMBER, len: 6, data: 3ff50e18 PPP xmit, ifc = 0, len: 14 data: ff03c0210101000a05063ff50e18 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c02101010010013010405d40305c22380050659f4cf2500000000000000 00000000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: Config Request, len is: 15 Pkt dump: 010405d40305c22380050659f4cf25 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 5, data: c22380 LCP Option: MAGIC_NUMBER, len: 6, data: 59f4cf25 Xmit Link Control Protocol pkt, Action code is: Config ACK, len is: 15 Pkt dump: 010405d40305c22380050659f4cf25 LCP Option: Max_Rcv_Units, len: 4, data: 05d4 LCP Option: AUTHENTICATION_TYPES, len: 5, data: c22380 LCP Option: MAGIC_NUMBER, len: 6, data: 59f4cf25 PPP xmit, ifc = 0, len: 23 data: ff03c02102010010013010405d40305c22380050659f4cf25 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0210201000a05063ff50e1800000000000000000000000000000000000000 00000000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: Config ACK, len is: 6 Pkt dump: 05063ff50e18 LCP Option: MAGIC_NUMBER, len: 6, data: 3ff50e18 Xmit Link Control Protocol pkt, Action code is: Echo Request, len is: 4 Pkt dump: 3ff50e18 PPP xmit, ifc = 0, len: 12 data: ff03c021090000083ff50e18 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c2230103001508bfe11df6d8fb52433336343020202020000000000000 00000000000000000000000000 **PPP chap receive challenge: rcvd a type MS-CHAP-V1 pkt** PPP xmit, ifc = 0, len: 63 data: ff03c2230203003b31488506adb9ae0f4cac35866242b2bac2863870291e4a88e1458f0 12526048734778a210325619092d3f831c3bcf3eb7201636973636f PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c0210a00000859f4cf2500000000000000000000000000000000000000 00000000000000000000000000 Rcvd Link Control Protocol pkt, Action code is: Echo Reply, len is: 4 Pkt dump: 59f4cf25 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff03c22303030004000000000000000000000000000000000000000000000000 00000000000000000000000000 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff0380210101000a0306ac15301e000000000000000000000000000000000000 00000000000000000000000000 Rcvd IP Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 0306ac15301e IPCP Option: Config IP, IP = 172.21.48.30 Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 030600000000 IPCP Option: Config IP, IP = 0.0.0.0 PPP xmit, ifc = 0, len: 14 data: ff0380210101000a030600000000 Xmit IP Control Protocol pkt, Action code is: Config ACK, len is: 6 Pkt dump: 0306ac15301e IPCP Option: Config IP, IP = 172.21.48.30 PPP xmit, ifc = 0, len: 14 data: ff0380210201000a0306ac15301e PPP rcvd, ifc = 0, pppdev: 1, len: 42, data: ff0380210301000a03060b0b0b020000000000000000000000000000000000 00000000000000000000000000 Rcvd IP Control Protocol pkt, Action code is: Config NAK, len is: 6 Pkt dump: 03060b0b0b02 IPCP Option: Config IP, IP = 11.11.11.1 Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6 Pkt dump: 03060b0b0b02 IPCP Option: Config IP, IP = 11.11.11.1 PPP xmit, ifc = 0, len: 14

```
data: ff0380210102000a03060b0b0b02 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210202000a03060b0b0b020000000000000000000000000000000000 0000000000000000000000000 Rcvd IP
Control Protocol pkt, Action code is: Config ACK, len is: 6 Pkt dump: 03060b0b0b02 IPCP Option:
Config IP, IP = 11.11.11.1 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210901000c59f4cf2501592b7e0000000000000000000000000000000000 0000000000000000000000000 Rcvd Link
Control Protocol pkt, Action code is: Echo Request, len is: 8 Pkt dump: 59f4cf2501592b7e Xmit
Link Control Protocol pkt, Action code is: Echo Reply, len is: 8 Pkt dump: 3ff50e1801592b7e PPP
xmit, ifc = 0, len: 16 data: ff03c0210a01000c3ff50e1801592b7e Xmit Link Control Protocol pkt,
Action code is: Echo Request, len is: 4 Pkt dump: 3ff50e18 PPP xmit, ifc = 0, len: 12 data:
ff03c021090100083ff50e18 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210a01000859f4cf250000000000000000000000000000000000000000 0000000000000000000000000 Rcvd Link
Control Protocol pkt, Action code is: Echo Reply, len is: 4 Pkt dump: 59f4cf25
```

PIX OS 6.2 和 6.3 版本中的已知警告

- 如果已配置了默认路由，则 PIX 不会建立 PPPoE，因为 PIX 不能用 PPPoE 提供的默认路由改写现有的默认路由。如果希望从服务器(setroute选项)上使用默认路由，用户需要清除配置上的默认路由。
- 只能定义用户名和一个 PPPoE 服务器。

PIX OS 6.3 版本中的已知警告

- 启用 PPPoE 和开放最短路径优先 (OSPF)，并且在检索 IP 地址后执行 **write memory** 时，通过 PPPoE 或 DHCP 下载的默认路由将保存到配置。解决方法是先执行 **write memory**，然后再从 PPPoE 服务器下载地址。
- 用于生成默认路由的 PPPoE **setroute** 选项与 PIX 防火墙上的 OSPF 动态路由协议不兼容。在 OSPF 进程下配置“network”语句后，将从路由表中删除 PPPoE 生成的默认路由。解决方法是使用静态路由。

相关信息

- PIX 支持页
- PIX 命令参考
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems