

# Configuración del Cliente PPPoE en un Cisco Secure PIX Firewall

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Información de resolución de problemas](#)

[Comandos para resolución de problemas](#)

[Advertencias conocidas en PIX OS versión 6.2 y 6.3](#)

[Advertencias conocidas en PIX OS versión 6.3](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento describe cómo configurar el cliente PPP (Point-to-Point Protocol) sobre Ethernet (PPPoE) en Cisco Secure PIX Firewall. PIX OS versión 6.2 introduce esta función y está dirigida al PIX de gama baja (501/506).

PPPoE combina dos estándares ampliamente aceptados, Ethernet y PPP, para proporcionar un método autenticado de asignación de direcciones IP a los sistemas cliente. Los clientes PPPoE suelen ser ordenadores personales conectados a un ISP a través de una conexión de banda ancha remota, como DSL o servicio por cable. Los ISP implementan PPPoE porque admiten el acceso de banda ancha de alta velocidad utilizando su infraestructura de acceso remoto existente y porque es más fácil de usar para los clientes. PIX Firewall versión 6.2 introduce la funcionalidad del cliente PPPoE. Esto permite que los usuarios de oficinas pequeñas, oficinas domésticas (SOHO) del firewall PIX se conecten a los ISP mediante módems DSL.

Actualmente, sólo la interfaz exterior del PIX soporta esta función. Una vez que la configuración también está en la interfaz externa, hay encapsulación de todo el tráfico con encabezados PPPoE/PPP. El mecanismo de autenticación predeterminado para PPPoE es el protocolo de autenticación de contraseña (PAP).

PPPoE proporciona un método estándar para utilizar los métodos de autenticación del PPP sobre una red Ethernet. Cuando lo utilizan los ISP, PPPoE permite la asignación autenticada de

direcciones IP. En este tipo de implementación, el cliente y el servidor PPPoE están interconectados por protocolos de puente de Capa 2 que se ejecutan sobre una DSL u otra conexión de banda ancha.

El usuario tiene la opción de configurar manualmente el Protocolo de autenticación por desafío mutuo (CHAP) o MS-CHAP. Las versiones 6.2 y 6.3 del sistema operativo PIX no admiten el protocolo de túnel de capa 2 (L2TP) ni el protocolo de túnel de punto a punto (PPTP) con PPPoE.

PPPoE se compone de dos fases principales:

- Fase de detección activa: en esta fase, el cliente PPPoE localiza un servidor PPPoE, denominado concentrador de acceso. Durante esta fase, se asigna un ID de sesión y se establece la capa PPPoE.
- Fase de Sesión PPP: en esta fase, se negocian las opciones PPP y se realiza la autenticación. Una vez finalizada la configuración del link, PPPoE funciona como un método de encapsulación de Capa 2, lo que permite transferir datos a través del link PPP dentro de los encabezados PPPoE.

En la inicialización del sistema, el cliente PPPoE establece una sesión con el AC mediante el intercambio de una serie de paquetes. Una vez establecida la sesión, se configura un enlace PPP, que incluye la autenticación mediante el protocolo de autenticación de contraseña (PAP). Una vez establecida la sesión PPP, cada paquete se encapsula en los encabezados PPPoE y PPP.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PIX 501 con PIX OS versión 6.3(4)
- Cisco 1721 Router con Cisco IOS® Software Release 12.3(10) configurado como servidor PPPoE

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.

### Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Configurar

Esta sección le presenta la información que puede utilizar para configurar las características que describe este documento.

**Nota:** Para encontrar información adicional sobre los comandos que utiliza este documento, utilice la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

## [Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



## [Configuraciones](#)

Este documento usa estas configuraciones.

- [Router Cisco 1721 como servidor PPPoE](#)
- [PIX \(501 o 506 \) como cliente PPPoE](#)

En esta prueba de laboratorio, un router Cisco 1721 actúa como servidor PPPoE. No lo necesita en su oficina doméstica o remota, ya que el ISP aloja el servidor PPPoE.

### Router Cisco 1721 como servidor PPPoE

```
!--- 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 o 506 ) como cliente PPPoE

```
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 pppoe request dialout
pppoe

!--- Associate the username that the ISP assigns to the
VPDN group. vpdn group pppoe localname cisco

!--- Define authentication protocol. vpdn group pppoe
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:e136533e23231c5bbbf4088cee75a5a
: end
[OK]
pix501#

```

## Verificación

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show ip address outside pppoe**—Muestra la información de configuración actual del cliente PPPoE.
- **show vpdn tunnel pppoe**—Muestra información de túnel para el tipo de túnel específico.
- **show vpdn session pppoe**: muestra el estado de las sesiones PPPoE.
- **show vpdn pppinterface**—Muestra el valor de identificación de la interfaz del túnel PPPoE. Se crea una interfaz virtual PPP para cada túnel PPPoE.
- **show vpdn group**: muestra el grupo definido para el túnel PPPoE.
- **show vpdn username**: muestra la información del nombre de usuario local.

Este es el resultado del comando **show ip address outside pppoe**:

```
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
```

Este es el resultado del comando **show vpdn tunnel pppoe**:

```
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
```

Este es el resultado del comando **show vpdn session pppoe**:

```
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
```

Este es el resultado del comando **show vpdn pppinterface**:

```
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
```

Este es el resultado del comando **show vpdn group**:

```
501(config)#show vpdn group
```

```
vpdn group pppoex request dialout pppoe
vpdn group pppoex localname cisco
vpdn group pppoex ppp authentication pap
```

Este es el resultado del comando **show vpdn username**:

```
501(config)#show vpdn username
```

```
vpdn username cisco password *****
```

## [Troubleshoot](#)

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

### [Información de resolución de problemas](#)

Estos son debugs de ejemplo de configuraciones erróneas comunes en el PIX. Active estas depuraciones.

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

- La autenticación falla (por ejemplo, nombre de usuario/contraseña erróneos).

```
Rcvd Link Control Protocol pkt, Action code is: Echo Reply,
len is: 4 Pkt dump: d0c3305c
```

```
PPP pap rcv authen nak: 41757468656e74696361746966f6e2066661696c757265
PPP PAP authentication failed
```

```
Rcvd Link Control Protocol pkt, Action code is: Termination Request,
len is: 0
```

- El protocolo de autenticación no es válido (por ejemplo, PAP/CHAP mal configurado).

```
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
```

- El servidor PPPoE no responde, vuelva a intentarlo cada 30 segundos.

```
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:SVNAME-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:SVNAME-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:SVNAME-Service Name Len:0
Type:0103:HOSTUNIQ-Host Unique Tag Len:4 00000001
```

**padi timer expired**

## Comandos para resolución de problemas

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

**Nota:** Consulte [Información Importante sobre Comandos Debug](#) antes de ejecutar los comandos debug.

- **debug pppoe packet**—Muestra información del paquete.
- **debug pppoe error**—Muestra mensajes de error.
- **debug pppoe event**—Muestra la información del evento del protocolo.
- **debug ppp negotiation**: permite ver si un cliente pasa información de negociación PPP.
- **debug ppp io** — **Muestra la información de paquete para la interfaz virtual PPTP PPP.**
- **debug ppp upap**—Muestra la autenticación PAP.
- **debug ppp error**: muestra los mensajes de error de la interfaz virtual PPTP PPP.
- **debug ppp chap**: muestra información sobre si un cliente pasa la autenticación.

Utilice estos comandos para habilitar la depuración para el cliente PPPoE:

```
!--- 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

**Este resultado muestra comandos de depuración adicionales para el cliente PPPoE:**

```
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:  
ff03c02101010012010405d40304c023050659d9f6360000000000000000  
000000000000000000000000

**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:

ff03c02102010012010405d40304c023050659d9f636

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:  
ff03c02101020012010405d40304c023050659d9f636000000000000000000  
00000000000000000000000000000000

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:  
ff03c02102020012010405d40304c023050659d9f636

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  
00000000000000000000000000000000

**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: ff03c021090000008609b39f5

PPP xmit, ifc = 0, len: 20 data: ff03c0230101001005636973636f05636973636f

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:  
ff03c0210a00000859d9f63600  
00000000000000000000000000000000

**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:  
ff03c0230201000500  
00000000000000000000000000000000

PPP upap rcvd authen ack:  
ff03c0230201000500  
00000

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:  
ff0380210101000a0306ac15301e00000000000000000000000000000000000000  
00000000000000000000000000000000

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:  
ff0380210301000a03060b0b0b0200000000000000000000000000000000  
00000000000000000000000000000000

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  
00000000000000000000000000000000

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:  
ff0380210202000a03060b0b0b0200000000000000000000000000000000  
00000000000000000000000000000000

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  
00000000000000000000000000000000

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:





000000000000000000000000

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:  
ff03c0210a01000859f4cf25000  
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Reply, len is: 4  
Pkt dump: 59f4cf25

## [Advertencias conocidas en PIX OS versión 6.2 y 6.3](#)

- Si la ruta predeterminada ya está configurada, PIX no establece PPPoE porque no puede sobrescribir la ruta predeterminada existente con la ruta predeterminada que suministra PPPoE. Si desea utilizar la ruta predeterminada del servidor (**opción setroute**), el usuario necesita borrar la ruta predeterminada en la configuración.
- Sólo puede definir el nombre de usuario y un servidor PPPoE.

## [Advertencias conocidas en PIX OS versión 6.3](#)

- Cuando habilita PPPoE y Open Shortest Path First (OSPF) y **write memory** funciona después de la recuperación de una dirección IP, la ruta predeterminada descargada a través de PPPoE o DHCP se guarda en la configuración. La solución alternativa es realizar la **escritura de memoria** antes de que la dirección se descargue del servidor PPPoE.
- La opción PPPoE **setroute**, que utiliza para generar una ruta predeterminada, no es compatible con el protocolo de ruteo dinámico OSPF en el Firewall PIX. La ruta predeterminada que genera PPPoE se elimina de la tabla de ruteo cuando la instrucción "network" se configura bajo el proceso OSPF. La solución temporal es utilizar rutas estáticas.

## [Información Relacionada](#)

- [Página de Soporte de PIX](#)
- [Referencia de Comandos PIX](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)