

# Configurar al Cliente de PPPoE en un Cisco Secure PIX Firewall

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información de Troubleshooting](#)

[Comandos para resolución de problemas](#)

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

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

[Información Relacionada](#)

## [Introducción](#)

Este documento describe cómo configurar el Point-to-Point Protocol (PPP) sobre el cliente de los Ethernetes (PPPoE) en el Cisco Secure PIX Firewall. El PIX OS de la versión 6.2 introduce esta función y se apunta para el PIX de menor capacidad (501/506).

El PPPoE combina dos estándares extensamente validados, los Ethernetes y PPP, para proporcionar un método autenticado de asignar los IP Addresses a los sistemas del cliente. Los Clientes de PPPoE son típicamente computadoras personales conectadas con un ISP sobre una conexión de banda ancha remota, tal como DSL o servicio de cable. Los ISP despliegan el PPPoE porque soporta el acceso por banda ancha de alta velocidad usando su infraestructura existente del Acceso Remoto y porque es más fácil que los clientes utilicen. La versión 6.2 del firewall PIX introduce las funciones del Cliente de PPPoE. Esto permite que los usuarios del oficina pequeña, oficina en el hogar (SOHO) del firewall PIX conecten con los ISP usando los módems DLS.

Actualmente, solamente la interfaz exterior de los soportes de PIX esta función. Una vez que la configuración está también en la interfaz exterior, hay encapsulación de todo el tráfico con las encabezados PPPoE/PPP. El mecanismo de autenticación predeterminada para el PPPoE es el protocolo password authentication (PAP).

El PPPoE proporciona un método estándar de emplear los métodos de autenticación del PPP

sobre una red Ethernet. Cuando es utilizado por los ISP, el PPPoE permite la asignación de IP Address autenticada. En este tipo de implementación, los protocolos que interligan de la capa 2 interconectan al Cliente de PPPoE y el servidor que ejecutado encima el DSL o la otra conexión de banda ancha.

El usuario tiene la opción para configurar el Challenge Handshake Authentication Protocol (CHAP) o el MS-CHAP manualmente. Los PIX OS de la versión 6.2 y 6.3 no soportan el protocolo Layer 2 Tunneling Protocol (L2TP) y el Point-to-Point Tunneling Protocol (PPTP) con el PPPoE.

El PPPoE se compone de dos fases principales:

- Fase de la detección activa — En esta fase, el Cliente de PPPoE localiza a un servidor PPPoE, llamado un concentrador de acceso. Durante esta fase, se asigna un ID de sesión y se establece la capa PPPoE.
- Fase de la sesión PPP — En esta fase, se negocian las opciones PPP y se realiza la autenticación. La configuración del link se completa una vez, las funciones PPPoE como método de encapsulación de la capa 2, permitiendo que los datos sean transferidos sobre el link PPP dentro de los encabezados PPPoE.

En la inicialización del sistema, el Cliente de PPPoE establece una sesión con el AC intercambiando una serie de paquetes. Una vez que se establece la sesión, se configura un link PPP, que incluye la autenticación usando el protocolo de la autenticación de contraseña (PAP). Una vez que establecen a la sesión PPP, cada paquete se encapsula en el PPPoE y los encabezados PPP.

## prerrequisitos

### Requisitos

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Configurar

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

**Nota:** Para encontrar la información adicional en los comandos que este documento utiliza, que utilice la [herramienta de búsqueda de comandos](#) ([clientes registrados solamente](#)).

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

Este documento usa estas configuraciones.

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

En este prueba de laboratorio, un Cisco 1721 Router actúa como servidor PPPoE. Usted no necesita esto en su hogar/oficina remota puesto que su ISP recibe al servidor PPPoE.

### Cisco 1721 Router 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 de 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:e136533e23231c5bfff4088cee75a5a : end
[OK] pix501#

```

## Verificación

Esta sección proporciona la información que usted puede utilizar para confirmar que su configuración trabaja correctamente.

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

- **muestre el IP Address fuera del pppoe** — Visualiza la información de la configuración actual del Cliente de PPPoE.
- **muestre el pppoe del túnel del vpdn** — Visualiza la información del túnel para el tipo de túnel específico.
- **muestre el pppoe de la sesión del vpdn** — Visualiza el estatus de las sesiones PPPoE.
- **muestre el pppinterface del vpdn** — Visualiza el valor de identificación de la interfaz del túnel PPPoE. Una interfaz virtual PPP se crea para cada túnel PPPoE.
- **muestre el grupo del vpdn** — Visualiza al grupo definido para el túnel PPPoE.
- **muestre el nombre de usuario del vpdn** — Visualiza la información de nombre de usuario local.

Ésta es la salida para el 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
```

Ésta es la salida para el 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
```

Ésta es la salida para el 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
```

Ésta es la salida para el 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
```

Ésta es la salida para el 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
```

Ésta es la salida para el comando **show vpdn username**:

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

## Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

### Información de Troubleshooting

Éstos son debugs de la muestra de las configuraciones erróneas más comunes en el PIX. Gire estos debugs.

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

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

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

PPP pap rcv authen nak: 41757468656e74696361746966f6e206661696c757265 PPP PAP authentication
failed Rcvd Link Control Protocol pkt, Action code is: Termination Request, len is: 0
```
- El protocolo de autenticación es inválido (por ejemplo, PAP/CHAP configurado mal).

```
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, revisa 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: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
```

## 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 en los comandos debug](#) antes de ejecutar los comandos debug.

- **debug pppoe packet** — Visualiza la información del paquete.
- **debug pppoe error** — Visualiza los mensajes de error.
- **debug pppoe event** — Visualiza la información del evento del protocolo.
- **negociación ppp del debug** — Permite que usted vea si un cliente pasa la información de la negociación PPP.
- **debug ppp io** — Muestra la información de paquete para la interfaz virtual PPTP PPP.
- **debug ppp upap** — Autenticación PAP de las visualizaciones.
- **debug ppp error** — Mensajes de error de interfaz virtual de las visualizaciones PPTP PPP.
- **PPP chap del debug** — Visualiza la información sobre si un cliente pasa la autenticación.

Utilice estos comandos para habilitar el debugging para el Cliente de 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
```

Esta salida muestra los comandos de debugging adicionales para el Cliente de 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:
```



## Debug del permiso para el nuevo método de autenticación.

```
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:
ff03c02101010013010405d40305c22380050659f4cf250000000000000000 00000000000000000000 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: ff03c02102010013010405d40305c22380050659f4cf25 PPP rcvd, ifc = 0,
pppdev: 1, len: 42, data: ff03c0210201000a05063ff50e180000000000000000000000000000000000000000
00000000000000000000 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:
ff03c2230103001508bfe11df6d8fb52433363430202020200000000000 000000000000000000000000000000000000 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: ff03c0210a00000859f4cf2500000000000000000000000000000000000000000000000000000000000000000000 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: ff03c2230303000400000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000 PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210101000a0306ac15301e000000000000000000000000000000000000000000000000000000000000000000000000 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:
ff0380210301000a03060b0b0b020000000000000000000000000000000000000000000000000000000000000 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:
ff0380210202000a03060b0b0b020000000000000000000000000000000000000000000000000000000000000 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:
ff03c0210901000c59f4cf2501592b7e00000000000000000000000000000000000000000000000000000000000000000000 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:
ff03c0210a01000859f4cf2500000000000000000000000000000000000000000000000000000000000000000000 Rcvd Link
Control Protocol pkt, Action code is: Echo Reply, len is: 4 Pkt dump: 59f4cf25
```

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

- Si la ruta predeterminado se configura ya, el PIX no establece el PPPoE porque no puede sobregabar la ruta predeterminado existente con la ruta predeterminado que el PPPoE suministra. Si usted desea utilizar la ruta predeterminado del servidor (**opción setroute (establecer ruta)**), el usuario necesita borrar la ruta predeterminado en la configuración.
- Usted define el nombre de usuario y a un servidor PPPoE solamente.

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



- Cuando usted habilita el PPPoE y el Open Shortest Path First (OSPF) y **escribe la memoria** se realiza después de la extracción de una dirección IP, la ruta predeterminado descargada con el PPPoE o el DHCP guarda a la configuración. La solución alternativa es realizarse **escribe la memoria** antes de que las descargas del direccionamiento del servidor PPPoE.
- La opción setroute (establecer ruta) de PPPoE, que usted utiliza para generar una ruta predeterminado, no es compatible con el Dynamic Routing Protocol OSPF en el firewall PIX. La ruta predeterminado que el PPPoE genera se quita de la tabla de ruteo cuando la declaración de la “red” se configura bajo proceso OSPF. La solución alternativa es utilizar las Static rutas.

## [Información Relacionada](#)

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