

Configuring the PPPoE Client on a Cisco Secure PIX Firewall

Document ID: 22855

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Information
- Troubleshooting Commands
- Known Caveats in PIX OS Version 6.2 and 6.3
- Known Caveats in PIX OS Version 6.3

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to configure the Point-to-Point Protocol (PPP) over Ethernet (PPPoE) client on the Cisco Secure PIX Firewall. PIX OS version 6.2 introduces this function and is targeted for the low-end PIX (501/506).

PPPoE combines two widely accepted standards, Ethernet and PPP, in order to provide an authenticated method of assigning IP addresses to client systems. PPPoE clients are typically personal computers connected to an ISP over a remote broadband connection, such as DSL or cable service. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use. PIX Firewall version 6.2 introduces PPPoE client functionality. This allows small office, home office (SOHO) users of the PIX Firewall to connect to ISPs using DSL modems.

Currently, only the outside interface of the PIX supports this function. Once the configuration is also on the outside interface, there is encapsulation of all traffic with PPPoE/PPP headers. The default authentication mechanism for PPPoE is Password Authentication Protocol (PAP).

PPPoE provides a standard method of employing the authentication methods of the PPP over an Ethernet network. When used by ISPs, PPPoE allows authenticated assignment of IP addresses. In this type of implementation, the PPPoE client and server are interconnected by Layer 2 bridging protocols that run over a DSL or other broadband connection.

The user has the option to configure Challenge Handshake Authentication Protocol (CHAP) or MS-CHAP manually. PIX OS versions 6.2 and 6.3 do not support Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) with PPPoE.

PPPoE is composed of two main phases:

- Active Discovery Phase In this phase, the PPPoE client locates a PPPoE server, called an access

concentrator. During this phase, a Session ID is assigned and the PPPoE layer is established.

- **PPP Session Phase** In this phase, PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method, allowing data to be transferred over the PPP link within PPPoE headers.

At system initialization, the PPPoE client establishes a session with the AC by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication (PAP) protocol. Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- PIX 501 with PIX OS version 6.3(4)
- Cisco 1721 router with Cisco IOS® Software Release 12.3(10) configured as a PPPoE server

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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

This section presents you with the information you can use in order to configure the features this document describes.

Note: In order to find additional information on the commands this document uses, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations.

- Cisco 1721 Router as PPPoE Server
- PIX (501 or 506) as PPPoE Client

In this lab test, a Cisco 1721 router acts as a PPPoE server. You do not need this in your home/remote office since your ISP hosts the PPPoE server.

Cisco 1721 Router as PPPoE Server

```
!--- 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 or 506) as PPPoE Client

```
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 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#

```

Verify

This section provides information you can use in order to confirm that your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show ip address outside pppoe** Displays the current PPPoE client configuration information.
- **show vpdn tunnel pppoe** Displays tunnel information for the specific tunnel type.
- **show vpdn session pppoe** Displays the status of PPPoE sessions.
- **show vpdn pppinterface** Displays the interface identification value of the PPPoE tunnel. A PPP virtual interface is created for each PPPoE tunnel.
- **show vpdn group** Displays the group defined for the PPPoE tunnel.
- **show vpdn username** Displays the local username information.

This is the output for the **show ip address outside pppoe** command:

```

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

```

This is the output for the **show vpdn tunnel pppoe** command:

```

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

```

This is the output for the **show vpdn session pppoe** command:

```

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
```

This is the output for the **show vpdn pppinterface** command:

```
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
```

This is the output for the **show vpdn group** command:

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

This is the output for the **show vpdn username** command:

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

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Troubleshooting Information

These are sample debugs from common misconfigurations on the PIX. Turn on these debugs.

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

- Authentication fails (for example, bad username/password).

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

```
PPP pap rcv authen nak: 41757468656e74696336174696f6e206661696c757265
PPP PAP authentication failed
Rcvd Link Control Protocol pkt, Action code is: Termination Request,
len is: 0
```

- Authentication protocol is invalid (for example, PAP/CHAP misconfigured).

```
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 server does not respond, retry every 30 seconds.

```
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

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you issue **debug** commands.

- **debug pppoe packet** Displays packet information.
- **debug pppoe error** Displays error messages.
- **debug pppoe event** Displays protocol event information.
- **debug ppp negotiation** Allows you to see if a client passes PPP negotiation information.
- **debug ppp io** Displays the packet information for the PPTP PPP virtual interface.
- **debug ppp upap** Displays PAP authentication.
- **debug ppp error** Displays PPTP PPP virtual interface error messages.
- **debug ppp chap** Displays information about whether a client passes authentication.

Use these commands in order to enable debugging for the PPPoE client:

!--- 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

This output shows additional debugging commands for the PPPoE client:

```
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:
ff03c02101020012010405d40304c023050659d9f6360000000000000000
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:
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:
ff03c0210201000a0506609b39f500000000000000000000000000000000
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: ff03c02109000008609b39f5

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:
ff0380210301000a03060b0b0200000000000000000000000000000000000000
00000000000000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: **Config NAK**, len is: 6
Pkt dump: 03060b0b02
IPCP Option: Config IP, IP = 11.11.11.1

Xmit IP Control Protocol pkt, Action code is: Config Request, len is: 6
Pkt dump: 03060b0b02

```

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:
ff03c0210901000c59d9f636015995a100000000000000000000000000000000
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:
ff0380210202000a03060b0b0b02000000000000000000000000000000000000
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:
ff03c0210902000c59d9f6360159937b00000000000000000000000000000000
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:
ff03c0210a01000859d9f6360000000000000000000000000000000000000000
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Echo Reply, len is: 4
Pkt dump: 59d9f636

```

Debugging When You Use the ppp ms-chap Command for Authentication

When you configure PPP MS-CHAP authentication, this line is the only change that you need in the PIX (all the rest remain the same).

The **vpdn group pppoex ppp authentication pap** command changes to **vpdn group pppoex ppp authentication mschap**.

Enable debug for the new authentication method.

```

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
00000000000000000000000000000000

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:
ff03c0210201000a05063ff50e18000000000000000000000000000000000000
00000000000000000000000000000000

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:
ff03c2230103001508bfe11df6d8fb5243333634302020202000000000000
00000000000000000000000000000000

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:
ff03c0210a00000859f4cf2500
00000000000000000000000000000000

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:
ff03c2230303000400
00000000000000000000000000000000

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210101000a0306ac15301e000000000000000000000000000000000000
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:
ff0380210301000a03060b0b0b0200000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000

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:
ff0380210202000a03060b0b0b0200000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000

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:
ff03c0210901000c59f4cf2501592b7e0000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000

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:
ff03c0210a01000859f4cf250000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000

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

```

Known Caveats in PIX OS Version 6.2 and 6.3

- If the default route is already configured, PIX does not establish the PPPoE because it cannot overwrite the existing default route with the default route that the PPPoE supplies. If you wish to use the default route from the server (**setroute** option), the user needs to erase the default route on the

configuration.

- You define username and one PPPoE server only.

Known Caveats in PIX OS Version 6.3

- When you enable PPPoE and Open Shortest Path First (OSPF) and **write memory** performs after the retrieval of an IP address , the downloaded default route through PPPoE or DHCP saves to the configuration. The workaround is to perform **write memory** before the address downloads from the PPPoE server.
- The PPPoE **setroute** option, which you use to generate a default route, is not compatible with the OSPF dynamic routing protocol on the PIX Firewall. The default route that the PPPoE generates is removed from the routing table when the "network" statement is configured under the OSPF process. The workaround is to use static routes.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Using PIX Firewall in SOHO Networks](#)
- [PIX Support Page](#)
- [Documentation for PIX Firewall](#)
- [PIX Command Reference](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 22855