

Cisco Secure PIX Firewall에서 PPPoE 클라이언트 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 정보](#)

[문제 해결 명령](#)

[PIX OS 버전 6.2 및 6.3의 알려진 주의 사항](#)

[PIX OS 버전 6.3의 알려진 주의 사항](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Secure PIX Firewall에서 PPPoE(Point-to-Point Protocol) over Ethernet(PPPoE) 클라이언트를 구성하는 방법에 대해 설명합니다.PIX OS 버전 6.2는 이 기능을 도입하며 로우엔드 PIX(501/506)를 대상으로 합니다.

PPPoE는 클라이언트 시스템에 IP 주소를 할당하는 인증된 방법을 제공하기 위해 널리 사용되는 두 가지 표준인 이더넷과 PPP를 결합합니다.PPPoE 클라이언트는 일반적으로 DSL 또는 케이블 서비스와 같은 원격 광대역 연결을 통해 ISP에 연결된 개인용 컴퓨터입니다.ISP는 PPPoE를 구축합니다. PPPoE는 기존 원격 액세스 인프라를 사용하여 고속 광대역 액세스를 지원하고 고객이 더 쉽게 사용할 수 있기 때문입니다.PIX Firewall 버전 6.2에는 PPPoE 클라이언트 기능이 도입되었습니다. 이렇게 하면 PIX Firewall의 소규모 사무실, 홈 오피스(SOHO) 사용자가 DSL 모뎀을 사용하여 ISP에 연결할 수 있습니다.

현재 PIX의 외부 인터페이스만 이 기능을 지원합니다.컨피그레이션이 외부 인터페이스도 구성되면 PPPoE/PPP 헤더로 모든 트래픽을 캡슐화합니다.PPPoE의 기본 인증 메커니즘은 PAP>Password Authentication Protocol)입니다.

PPPoE는 이더넷 네트워크를 통해 PPP의 인증 방법을 사용하는 표준 방법을 제공합니다.ISP에서 사용할 경우 PPPoE는 인증된 IP 주소 할당을 허용합니다.이러한 유형의 구현에서 PPPoE 클라이언트와 서버는 DSL 또는 기타 광대역 연결을 통해 실행되는 레이어 2 브리징 프로토콜로 상호 연결됩니다.

사용자는 CHAP(Challenge Handshake Authentication Protocol) 또는 MS-CHAP를 수동으로 구성할 수 있습니다. PIX OS 버전 6.2 및 6.3은 PPPoE를 사용하여 L2TP(Layer 2 Tunneling Protocol) 및 PTP(Point-to-Point Tunneling Protocol)를 지원하지 않습니다.

PPPoE는 두 가지 주요 단계로 구성됩니다.

- Active Discovery Phase(활성 검색 단계) - 이 단계에서는 PPPoE 클라이언트가 액세스 집중기라는 PPPoE 서버를 찾습니다. 이 단계에서 세션 ID가 할당되고 PPPoE 레이어가 설정됩니다.
- PPP Session Phase(PPP 세션 단계) - 이 단계에서는 PPP 옵션이 협상되고 인증이 수행됩니다. 링크 설정이 완료되면 PPPoE는 레이어 2 캡슐화 방식으로 작동하여 PPPoE 헤더 내의 PPP 링크를 통해 데이터를 전송할 수 있습니다.

시스템 초기화 시 PPPoE 클라이언트는 일련의 패킷을 교환하여 AC와 세션을 설정합니다. 세션이 설정되면 PAP(Password Authentication) 프로토콜을 사용한 인증을 포함하는 PPP 링크가 설정됩니다. PPP 세션이 설정되면 각 패킷은 PPPoE 및 PPP 헤더에 캡슐화됩니다.

[사전 요구 사항](#)

[요구 사항](#)

이 문서에 대한 특정 요건이 없습니다.

[사용되는 구성 요소](#)

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 501(PIX OS 버전 6.3(4) 포함)
- Cisco IOS® Software Release 12.3(10)이 PPPoE 서버로 구성된 Cisco 1721 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

[구성](#)

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 사용할 수 있는 정보를 제공합니다.

참고: 이 문서에서 사용하는 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용합니다.

[네트워크 다이어그램](#)

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- [Cisco 1721 Router as PPPoE Server](#)
- [PIX\(501 또는 506 \) 를 PPPoE 클라이언트로 사용](#)

이 랩 테스트에서는 Cisco 1721 라우터가 PPPoE 서버 역할을 합니다. ISP에서 PPPoE 서버를 호스팅하기 때문에 홈/원격 사무소에서 이 기능이 필요하지 않습니다.

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 또는 506) 를 PPPoE 클라이언트로 사용

```

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#
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show** 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- **show ip address outside pppoe** - 현재 PPPoE 클라이언트 컨피그레이션 정보를 표시합니다.
- **show vpdn tunnel pppoe** - 특정 터널 유형에 대한 터널 정보를 표시합니다.
- **show vpdn session pppoe** - PPPoE 세션의 상태를 표시합니다.
- **show vpdn pppinterface** - PPPoE 터널의 인터페이스 식별 값을 표시합니다. 각 PPPoE 터널에 대해 PPP 가상 인터페이스가 생성됩니다.
- **show vpdn group** - PPPoE 터널에 대해 정의된 그룹을 표시합니다.
- **show vpdn username** - 로컬 사용자 이름 정보를 표시합니다.

다음은 **show ip address outside pppoe** 명령의 출력입니다.

```
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
```

다음은 **show vpdn tunnel pppoe** 명령의 출력입니다.

```
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
```

다음은 **show vpdn session pppoe** 명령의 출력입니다.

```
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

다음은 show vpdn pinterface 명령의 출력입니다.

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

다음은 show vpdn group 명령의 출력입니다.

501(config)#show vpdn group

vpdn group pppoex request dialout pppoe

vpdn group pppoex localname cisco

vpdn group pppoex ppp authentication pap

다음은 show vpdn username 명령의 출력입니다.

501(config)#show vpdn username

vpdn username cisco password *****

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 정보

PIX의 일반적인 컨피그레이션 오류 샘플의 디버그입니다.이 디버그를 켜세요.

pix#show debug

debug ppp negotiation

debug pppoe packet

debug pppoe error

debug pppoe event

- 인증이 실패합니다(예: 잘못된 사용자 이름/비밀번호).

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

- 인증 프로토콜이 잘못되었습니다(예: PAP/CHAP가 잘못 구성됨).

```
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 서버가 응답하지 않습니다. 30초마다 다시 시도하십시오.

```
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

문제 해결 명령

일부 show 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

참고: 디버그 명령을 [실행하기](#) 전에 [디버그 명령](#)에 대한 중요 정보를 참조하십시오.

- debug pppoe packet - 패킷 정보를 표시합니다.
- debug pppoe error - 오류 메시지를 표시합니다.
- debug pppoe event - 프로토콜 이벤트 정보를 표시합니다.
- debug ppp negotiation - 클라이언트가 PPP 협상 정보를 통과하는지 확인할 수 있습니다.

- **debug ppp io** - PPTP PPP 가상 인터페이스에 대한 패킷 정보를 표시합니다.
- **debug ppp upap** — PAP 인증을 표시합니다.
- **debug ppp error(디버그 ppp 오류)** - PPTP PPP 가상 인터페이스 오류 메시지를 표시합니다.
- **debug ppp chap** — 클라이언트가 인증을 통과하는지 여부에 대한 정보를 표시합니다.

PPPoE 클라이언트에 대한 디버깅을 활성화하려면 다음 명령을 사용합니다.

```
!--- 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

이 출력은 PPPoE 클라이언트에 대한 추가 디버깅 명령을 보여줍니다.

```
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
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:
ff03c02102010012010405d40304c023050659d9f636

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c02101020012010405d40304c023050659d9f6360000000000000000
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:
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: ff03c021090000008609b39f5

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

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210a00000859d9f63600000000000000000000000000000000000
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
000000

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210101000a0306ac15301e0000000000000000000000000000000
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:
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:
ff03c0210a01000859d9f63600
00000000000000000000000000000000

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

인증에 ppp ms-chap 명령을 사용할 때 디버깅

PPP MS-CHAP 인증을 구성할 때 이 행은 PIX에서 필요한 유일한 변경 사항입니다(나머지는 모두 동일하게 유지).

vpdn group pppoex ppp authentication pap 명령이 vpdn group pppoex ppp authentication mschap로 변경됩니다.

새 인증 방법에 대한 디버그를 활성화합니다.

[illegible]

[illegible]

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

PIX OS 버전 6.2 및 6.3의 알려진 주의 사항

- 기본 경로가 이미 구성된 경우 PPPoE가 제공하는 기본 경로로 기존 기본 경로를 덮어쓸 수 없으므로 PIX는 PPPoE를 설정하지 않습니다. 서버에서 기본 경로를 사용하려면(**setroute** 옵션) 컨피그레이션에서 기본 경로를 지워야 합니다.
- 사용자 이름과 PPPoE 서버 하나만 정의합니다.

PIX OS 버전 6.3의 알려진 주의 사항

- PPPoE 및 OSPF(Open Shortest Path First)를 활성화하고 IP 주소를 검색한 후 **쓰기 메모리**를 수행하면 PPPoE 또는 DHCP를 통해 다운로드한 기본 경로가 컨피그레이션에 저장됩니다. 해결 방법은 주소가 PPPoE 서버에서 다운로드되기 전에 **쓰기 메모리**를 수행하는 것입니다.
- 기본 경로를 생성하는 데 사용하는 PPPoE setroute 옵션은 PIX 방화벽의 OSPF 동적 라우팅 프로토콜과 호환되지 않습니다. PPPoE가 생성하는 기본 경로는 OSPF 프로세스 아래에서 "network" 문을 구성할 때 라우팅 테이블에서 제거됩니다. 해결 방법은 고정 경로를 사용하는 것입니다.

관련 정보

- [PIX 지원 페이지](#)
- [PIX 명령 참조](#)
- [RFC\(Request for Comments\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)