

Configurazione del client PPPoE su un firewall Cisco Secure PIX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni sulla risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Avvertenze note in PIX OS versione 6.2 e 6.3](#)

[Avvertenze note in PIX OS versione 6.3](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare il client PPP (Point-to-Point Protocol) over Ethernet (PPPoE) su Cisco Secure PIX Firewall. PIX OS versione 6.2 introduce questa funzione ed è destinato ai PIX di fascia bassa (501/506).

La tecnologia PPPoE combina due standard ampiamente accettati, Ethernet e PPP, per fornire un metodo autenticato di assegnazione di indirizzi IP ai sistemi client. I client PPPoE sono in genere personal computer connessi a un ISP tramite una connessione a banda larga remota, ad esempio DSL o un servizio via cavo. Gli ISP implementano il protocollo PPPoE perché supporta l'accesso a banda larga ad alta velocità utilizzando l'infrastruttura di accesso remoto esistente e perché è più facile da utilizzare per i clienti. PIX Firewall versione 6.2 introduce la funzionalità client PPPoE. Ciò consente agli utenti di piccoli uffici e privati (SOHO) del firewall PIX di connettersi agli ISP utilizzando modem DSL.

Attualmente, solo l'interfaccia esterna del PIX supporta questa funzione. Se la configurazione si trova anche sull'interfaccia esterna, il traffico viene incapsulato con le intestazioni PPPoE/PPP. Il meccanismo di autenticazione predefinito per PPPoE è il protocollo PAP (Password Authentication Protocol).

Il protocollo PPPoE costituisce un metodo standard per l'utilizzo dei metodi di autenticazione del protocollo PPP su una rete Ethernet. Se utilizzato dagli ISP, il protocollo PPPoE consente

l'assegnazione autenticata di indirizzi IP. In questo tipo di implementazione, il client e il server PPPoE sono interconnessi da protocolli di bridging di layer 2 eseguiti su una connessione DSL o altra connessione a banda larga.

L'utente ha la possibilità di configurare manualmente il protocollo CHAP (Challenge Handshake Authentication Protocol) o MS-CHAP. I sistemi operativi PIX versione 6.2 e 6.3 non supportano il protocollo L2TP (Layer 2 Tunneling Protocol) e il protocollo PPTP (Point-to-Point Tunneling Protocol) con PPPoE.

Il PPPoE è costituito da due fasi principali:

- Fase di rilevamento attivo: in questa fase, il client PPPoE individua un server PPPoE, denominato concentratore di accesso. Durante questa fase, viene assegnato un ID sessione e viene stabilito il livello PPPoE.
- Fase di sessione PPP: in questa fase, le opzioni PPP vengono negoziate e viene eseguita l'autenticazione. Una volta completata la configurazione del collegamento, il protocollo PPPoE funziona come metodo di incapsulamento di layer 2, consentendo il trasferimento dei dati sul collegamento PPP all'interno delle intestazioni PPPoE.

Al momento dell'inizializzazione del sistema, il client PPPoE stabilisce una sessione con l'ACL scambiando una serie di pacchetti. Una volta stabilita la sessione, viene impostato un collegamento PPP, che include l'autenticazione tramite il protocollo PAP (Password Authentication). Una volta stabilita la sessione PPP, ogni pacchetto viene incapsulato nelle intestazioni PPPoE e PPP.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PIX 501 con PIX OS versione 6.3(4)
- Router Cisco 1721 con software Cisco IOS® versione 12.3(10) configurato come server PPPoE

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.](#)

Configurazione

In questa sezione vengono presentate le informazioni che è possibile utilizzare per configurare le funzionalità descritte nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni.

- [Cisco 1721 Router come server PPPoE](#)
- [PIX \(501 o 506 \) come client PPPoE](#)

In questo test di laboratorio, un router Cisco 1721 opera come server PPPoE. Questa operazione non è necessaria nell'ufficio di casa/remoto poiché l'ISP ospita il server PPPoE.

Cisco 1721 Router come server 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-Templat1
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) come client 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:e136533e23231c5bbbbf4088cee75a5a
: end
[OK]
pix501#

```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show ip address outside pppoe**: visualizza le informazioni correnti sulla configurazione del client PPPoE.
- **show vpdn tunnel pppoe**: visualizza le informazioni del tunnel per il tipo di tunnel specifico.
- **show vpdn session pppoe**: visualizza lo stato delle sessioni PPPoE.
- **show vpdn pppinterface**: visualizza il valore di identificazione dell'interfaccia del tunnel PPPoE. Per ogni tunnel PPPoE viene creata un'interfaccia virtuale PPP.
- **show vpdn group**: visualizza il gruppo definito per il tunnel PPPoE.
- **show vpdn username**: visualizza le informazioni sul nome utente locale.

Di seguito viene riportato l'output 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

Di seguito viene riportato l'output 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
```

Di seguito viene riportato l'output 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
```

Di seguito viene riportato l'output 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
```

Di seguito viene riportato l'output 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
```

Di seguito viene riportato l'output del comando **show vpdn username**:

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

[Risoluzione dei problemi](#)

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

[Informazioni sulla risoluzione dei problemi](#)

Di seguito vengono riportati alcuni esempi di debug relativi a configurazioni errate comuni sul PIX.
Attiva questi debug.

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

- Autenticazione non riuscita (ad esempio, nome utente/password non validi).

```
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
```

- Protocollo di autenticazione non valido (ad esempio, PAP/CHAP non configurato correttamente).

```
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
```

- Il server PPPoE non risponde. Riprovare ogni 30 secondi.

```
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

Comandi per la risoluzione dei problemi

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

- **debug pppoe packet:** visualizza le informazioni sul pacchetto.
- **debug pppoe error:** visualizza i messaggi di errore.
- **debug pppoe event:** visualizza le informazioni sull'evento del protocollo.
- **debug ppp negotiation:** consente di verificare se un client supera le informazioni di negoziazione PPP.
- **debug ppp io:** visualizza le informazioni sul pacchetto per l'interfaccia virtuale PPTP PPP.
- **debug ppp upap:** visualizza l'autenticazione PAP.
- **debug ppp error:** visualizza i messaggi di errore dell'interfaccia virtuale PPTP PPP.
- **debug ppp chap:** visualizza informazioni sul passaggio dell'autenticazione da parte di un client.

Utilizzare questi comandi per abilitare il debug per il client 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

In questo output vengono visualizzati comandi di debug aggiuntivi per il client 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
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:
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:
ff03c02302010005000
00000000000000000000000000000000

PPP upap rcvd authen ack:
ff03c0230201000500
00000

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

ff0380210101000a0306ac15301e000
0000000000000000000000000000

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:
ff0380210301000a03060b0b0b0200
0000000000000000000000000000

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:
ff03c0210901000c59d9f636015995a1000000000000000000000000000000000000
0000000000000000000000000000

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:
ff0380210202000a03060b0b0b0200000000000000000000000000000000000000
0000000000000000000000000000

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:
ff03c0210902000c59d9f6360159937b000000000000000000000000000000000000
0000000000000000000000000000

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

Debug quando si utilizza il comando ppp ms-chap per l'autenticazione

Quando si configura l'autenticazione PPP MS-CHAP, questa riga è l'unica modifica necessaria nel PIX (tutte le altre rimangono invariate).

il comando `vpdn group pppoex ppp authentication pap` viene modificato in `vpdn group pppoex ppp authentication mschap`.

Abilitare il debug per il nuovo metodo di autenticazione.

```
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:
ff03c0210201000a05063ff50e180000000000000000000000000000000000
00000000000000000000000000000000

Rcvd Link Control Protocol pkt, Action code is: Config ACK, len is: 6
Pkt dump: 05063ff50e18

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:
ff03c0210901000c59f4cf2501592b7e00000000000000000000000000000000
00000000000000000000000000000000

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:
ff03c0210a01000859f4cf2500
00000000000000000000000000000000

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

[Avvertenze note in PIX OS versione 6.2 e 6.3](#)

- Se la route predefinita è già configurata, il PIX non la stabilisce in quanto non può sovrascrivere la route predefinita esistente con quella fornita dal PPPoE. Se si desidera utilizzare il percorso predefinito dal server (opzione **setroute**), è necessario cancellare il percorso predefinito nella configurazione.
- Il nome utente e un solo server PPPoE vengono definiti.

[Avvertenze note in PIX OS versione 6.3](#)

- Quando si abilita PPPoE e Open Shortest Path First (OSPF) e la **memoria di scrittura** viene eseguita dopo il recupero di un indirizzo IP, la route predefinita scaricata tramite PPPoE o DHCP viene salvata nella configurazione. Per risolvere il problema, è necessario eseguire la **scrittura** della **memoria** prima che l'indirizzo venga scaricato dal server PPPoE.
- L'opzione PPPoE **setroute**, utilizzata per generare una route predefinita, non è compatibile con il protocollo di routing dinamico OSPF sul firewall PIX. La route predefinita generata dal PPPoE viene rimossa dalla tabella di routing quando l'istruzione "network" viene configurata nel processo OSPF. Per risolvere il problema, è possibile utilizzare route statiche.

[Informazioni correlate](#)

- [Pagina di supporto PIX](#)
- [Informazioni di riferimento sui comandi PIX](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)