Configuration du client PPPoE sur pare-feu Cisco Secure PIX Firewall

Contenu

Introduction

Ce document décrit comment configurer le client PPP (Point-to-Point Protocol) sur Ethernet (PPPoE) sur le pare-feu Cisco Secure PIX Firewall. PIX OS version 6.2 introduit cette fonction et est ciblé pour le PIX bas de gamme (501/506).

Le protocole PPPoE combine deux normes largement acceptées, Ethernet et PPP, afin de fournir une méthode authentifiée d'attribution d'adresses IP aux systèmes clients. Les clients PPPoE sont généralement des ordinateurs personnels connectés à un FAI via une connexion à large bande distante, telle que DSL ou service câblé. Les FAI déploient le protocole PPPoE car il prend en charge l'accès haut débit à large bande à l'aide de leur infrastructure d'accès à distance existante et parce qu'il est plus facile à utiliser pour les clients. PIX Firewall version 6.2 introduit la fonctionnalité de client PPPoE. Cela permet aux utilisateurs des petits bureaux et bureaux à domicile (SOHO) du pare-feu PIX de se connecter aux FAI à l'aide de modems DSL.

Actuellement, seule l'interface externe du PIX prend en charge cette fonction. Une fois que la configuration est également sur l'interface externe, il y a encapsulation de tout le trafic avec des en-têtes PPPoE/PPP. Le mécanisme d'authentification par défaut pour PPPoE est le protocole PAP (Password Authentication Protocol).

PPPoE fournit une méthode standard d'utilisation des méthodes d'authentification du protocole PPP sur un réseau Ethernet. Lorsqu'il est utilisé par les FAI, le protocole PPPoE autorise

l’attribution authentifiée d’adresses IP. Dans ce type d'implémentation, le client et le serveur PPPoE sont interconnectés par des protocoles de pontage de couche 2 qui s'exécutent sur une DSL ou une autre connexion haut débit.

L'utilisateur peut configurer manuellement le protocole CHAP (Challenge Handshake Authentication Protocol) ou MS-CHAP. PIX OS versions 6.2 et 6.3 ne prennent pas en charge le protocole L2TP (Layer 2 Tunneling Protocol) et le protocole PPTP (Point-to-Point Tunneling Protocol) avec PPPoE.

PPPoE se compose de deux phases principales :

- Phase de découverte active : au cours de cette phase, le client PPPoE localise un serveur PPPoE, appelé concentrateur d'accès. Au cours de cette phase, un ID de session est attribué et la couche PPPoE est établie.
- Phase de session PPP : au cours de cette phase, les options PPP sont négociées et l’authentification est effectuée. Une fois la configuration de la liaison terminée, le protocole PPPoE fonctionne comme une méthode d’encapsulation de couche 2, permettant le transfert de données sur la liaison PPP dans les en-têtes PPPoE.

Lors de l'initialisation du système, le client PPPoE établit une session avec le CA en échangeant une série de paquets. Une fois la session établie, une liaison PPP est configurée, qui inclut l'authentification à l'aide du protocole PAP (Password Authentication). Une fois la session PPP établie, chaque paquet est encapsulé dans les en-têtes PPPoE et PPP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- PIX 501 avec PIX OS version 6.3(4)
- Routeur Cisco 1721 avec logiciel Cisco IOS® Version 12.3(10) configuré en tant que serveur PPPoE

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

Cette section vous présente les informations que vous pouvez utiliser pour configurer les fonctionnalités décrites dans ce document.

Remarque : Afin de trouver des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commandes (clients enregistrés uniquement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes.

- Routeur Cisco 1721 en tant que serveur PPPoE
- PIX (501 ou 506) en tant que client PPPoE

Au cours de ce TP, un routeur Cisco 1721 agit comme serveur PPPoE. Vous n'en avez pas besoin dans votre bureau à domicile ou à distance, car votre FAI héberge le serveur PPPoE.

Routeur Cisco 1721 en tant que serveur 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 ou 506) en tant que 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 pppoex request dialout
pppoe

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

!--- Define authentication protocol. vpdn group pppoex
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#
```

Vérification

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show ip address outside pppoe** : affiche les informations de configuration du client PPPoE actuel.
- **show vpdn tunnel pppoe** : affiche les informations de tunnel pour le type de tunnel spécifique.
- **show vpdn session pppoe** : affiche l'état des sessions PPPoE.
- **show vpdn pppinterface** - Affiche la valeur d'identification de l'interface du tunnel PPPoE. Une interface virtuelle PPP est créée pour chaque tunnel PPPoE.
- **show vpdn group** : affiche le groupe défini pour le tunnel PPPoE.
- **show vpdn username** : affiche les informations de nom d'utilisateur local.

Voici le résultat de la commande **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
```

Voici le résultat de la commande **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
```

Voici le résultat de la commande **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
```

Voici le résultat de la commande **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
```

Voici le résultat de la commande **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
```

Voici le résultat de la commande **show vpdn username** :

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Informations de dépannage

Il s'agit d'exemples de débogages provenant de configurations incorrectes courantes sur le PIX. Activez ces débogages.

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

- Échec de l'authentification (par exemple, nom d'utilisateur/mot de passe incorrect).

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

PPP pap recv authen nak: 41757468656e7469636174696f6e206661696c757265
PPP PAP authentication failed
Rcvd Link Control Protocol pkt, Action code is: Termination Request,
len is: 0
```

- Le protocole d'authentification n'est pas valide (par exemple, PAP/CHAP mal configuré).

```
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
```

- Le serveur PPPoE ne répond pas, réessayez toutes les 30 secondes.

```
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
```

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Note : Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **de débogage**.

- **debug pppoe packet** : affiche les informations sur les paquets.
- **debug pppoe error** : affiche les messages d'erreur.
- **debug pppoe event** : affiche les informations d'événement de protocole.
- **debug ppp negotiation** : vous permet de voir si un client transmet les informations de négociation PPP.
- **debug ppp io** : affiche les informations de paquet pour l'interface virtuelle PPP PPTP.
- **debug ppp upap** - Affiche l'authentification PAP.
- **debug ppp error** - Affiche les messages d'erreur de l'interface virtuelle PPP PPTP.
- **debug ppp chap** : affiche des informations sur le passage de l'authentification par un client.

Utilisez ces commandes afin d'activer le débogage pour le 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
```

Ce résultat montre des commandes de débogage supplémentaires pour le 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
00000000000000000000000000

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
00000000000000000000000

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
00000000000000000000000

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: ff03c023010100100563697363 6f05636973636f

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210a00000859d9f6360000000000000000000000000000000000000000
00000000000000000000000

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:
ff03c0230201000500000000000000000000000000000000000000000000000000
00000000000000000000000

PPP upap rcvd authen ack:
ff03c023020100050000000000000000000000000000000000000000000000000000000000000000000000000000
00000
PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210101000a0306ac15301e000000000000000000000000000000000000
00000000000000000000000

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:
ff0380210301000a03060b0b0b020000000000000000000000000000000000
00000000000000000000000

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
00000000000000000000000

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:
ff0380210202000a03060b0b0b020000000000000000000000000000000000
00000000000000000000000

Rcvd IP Control Protocol pkt, Action code is: Config ACK, len is: 6
Pkt dump: 03060b0b0b02
IPCP Option: Config IP, IP = 11.11.11.1

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff03c0210902000c59d9f6360159937b000000000000000000000000000000
00000000000000000000000

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
00000000000000000000000
```

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

Débogage lorsque vous utilisez la commande ppp ms-chap pour l'authentification

Lorsque vous configurez l'authentification MS-CHAP PPP, cette ligne est la seule modification dont vous avez besoin dans le PIX (tous les autres restent identiques).

La commande **vpdn group pppoex ppp authentication pap** passe à **vpdn group pppoex ppp authentication mschap**.

Activez le débogage pour la nouvelle méthode d'authentification.

```
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:
ff03c02101010013010405d40305c22380050659f4cf2500000000000000
00000000000000000000000000

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:
 ff03c0210201000a05063ff50e1800000000000000000000000000000000000000
00000000000000000000000000

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:
ff03c2230103001508bfe11df6d8fb52433336343020202020000000000
```

```
00000000000000000000000000

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:
ff03c0210a00000859f4cf250000000000000000000000000000000000000000000000
00000000000000000000000000

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:
ff03c223030300040000000000000000000000000000000000000000000000000000
00000000000000000000000000

PPP rcvd, ifc = 0, pppdev: 1, len: 42, data:
ff0380210101000a0306ac15301e000000000000000000000000000000000000000000
00000000000000000000000000

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:
ff0380210301000a03060b0b0b020000000000000000000000000000000000000000
00000000000000000000000000

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:
ff0380210202000a03060b0b0b020000000000000000000000000000000000000000
00000000000000000000000000

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:
ff03c0210901000c59f4cf2501592b7e000000000000000000000000000000000000000000
00000000000000000000000000
```

```
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:
ff03c0210a01000859f4cf250000000000000000000000000000000000000000
00000000000000000000000000

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

Caveats connus dans PIX OS versions 6.2 et 6.3

- Si la route par défaut est déjà configurée, PIX n'établit pas le protocole PPPoE, car il ne peut pas remplacer la route par défaut existante par la route par défaut fournie par le protocole PPPoE. Si vous souhaitez utiliser la route par défaut à partir du serveur (option **setroute**), l'utilisateur doit effacer la route par défaut sur la configuration.
- Vous définissez un nom d'utilisateur et un serveur PPPoE uniquement.

Caveats connus dans PIX OS version 6.3

- Lorsque vous activez PPPoE et OSPF (Open Shortest Path First) et que la **mémoire en écriture** s'exécute après la récupération d'une adresse IP , la route par défaut téléchargée via PPPoE ou DHCP est enregistrée dans la configuration. La solution de contournement consiste à exécuter **la mémoire en écriture** avant le téléchargement de l'adresse à partir du serveur PPPoE.
- L'option de **segment** PPPoE, que vous utilisez pour générer une route par défaut, n'est pas compatible avec le protocole de routage dynamique OSPF sur le pare-feu PIX. La route par défaut générée par PPPoE est supprimée de la table de routage lorsque l'instruction « network » est configurée dans le processus OSPF. La solution de contournement consiste à utiliser des routes statiques.

Informations connexes

- Page de support PIX
- Référence des commandes PIX
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems