

# IPSec - Connexion entre un pare-feu PIX et un client VPN Cisco avec caractères génériques, clés pré-partagées, mode configuration avec authentification étendue

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Échantillon de debug PIX](#)

[Debugs avec le client vpn 4.x](#)

[Debugs avec le client vpn 1.1](#)

[Informations connexes](#)

## Introduction

Cet exemple de configuration explique comment connecter un client vpn à un Pare-feu PIX utilisant des masques, le mode-config, la commande d'**autorisation-ipsec de connexion de sysopt**, et l'authentification étendue (Xauth).

Afin de voir le TACACS+ et la configuration RADIUS pour PIX 6.3 et plus tard, référez-vous à [TACACS+ et à RAYON exemple pour PIX 6.3 et PIX/ASA 7.x configuration](#).

Le client VPN prend en charge le Norme AES (Advanced Encryption Standard) comme algorithme de chiffrement dans la version 3.6.1 et ultérieures de Client VPN Cisco et avec le Pare-feu 6.3 PIX. Le client vpn prend en charge des tailles de clé de 128 bits et de 256 bits seulement. Pour plus d'informations sur la façon configurer AES, référez-vous à [comment configurer le Client VPN Cisco à PIX avec AES](#).

Référez-vous à [PIX/ASA 7.x et Client VPN Cisco 4.x pour Windows avec l'exemple de configuration d'authentification de RAYON du Microsoft Windows 2003 IAS](#) pour installer la

connexion VPN d'Accès à distance entre un Client VPN Cisco (4.x pour Windows) et l'appliance 7.x de Sécurité de gamme 500 PIX utilisant un serveur de RAYON du Service d'authentification Internet de Microsoft Windows 2003 (IAS).

Consultez [Exemple de configuration d'IPsec entre un concentrateur VPN 3000 et un client VPN 4.x pour Windows à l'aide de RADIUS pour l'authentification et la comptabilisation des utilisateurs](#) pour établir un tunnel IPsec entre un concentrateur Cisco VPN 3000 et un Client VPN Cisco 4.x pour Windows utilisant RADIUS pour la vérification de l'ID de l'utilisateur et la gestion des comptes.

Consultez [Configuration d'IPSec entre un routeur Cisco IOS et un client VPN Cisco 4.x pour Windows à l'aide de RADIUS pour l'authentification d'utilisateur](#) pour configurer une connexion entre un routeur et le Client VPN Cisco 4.x utilisant RADIUS pour la vérification de l'ID de l'utilisateur.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

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

- Client VPN Cisco 4.x. Ce produit a avancé des caractéristiques VPN, à la différence du Cisco Secure VPN Client 1.x.
- Version 6.3(3) du Pare-feu 515E PIX.

**Note:** La technologie de cryptage est sujette à des contrôles d'exportation. Il est de votre responsabilité de connaître la loi concernant l'exportation de la technologie de cryptage. Le pour en savoir plus, se rapportent au [site Web d'administration du bureau d'exportation](#) . [Si vous avez n'importe quelles questions concernant le contrôle d'exportation, envoyez s'il vous plaît un email à \[export@cisco.com\]\(mailto:export@cisco.com\)](#).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

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

## Informations générales

La commande d'**autorisation-ipsec de connexion de sysopt** permet implicitement n'importe quel paquet qui provient un tunnel d'IPsec pour sauter vérifier d'une **liste d'accès**, d'un **conduit**, ou d'un

ordre associé d'**access-group** pour des connexions d'IPsec. Le Xauth authentifie l'utilisateur d'IPsec à un serveur externe TACACS+ ou de RAYON. En plus de la clé pré-partagée de caractère d'ambiguïté, l'utilisateur doit fournir un nom d'utilisateur/mot de passe.

Un utilisateur avec un client vpn reçoit une adresse IP de leur ISP. Ceci est remplacé par une adresse IP du groupe d'adresse IP sur le PIX. L'utilisateur a accès à tout sur l'intérieur du Pare-feu, y compris des réseaux. Les utilisateurs qui n'exécutent pas le client vpn peuvent se connecter seulement au web server utilisant l'adresse fournie extérieure par l'affectation statique.

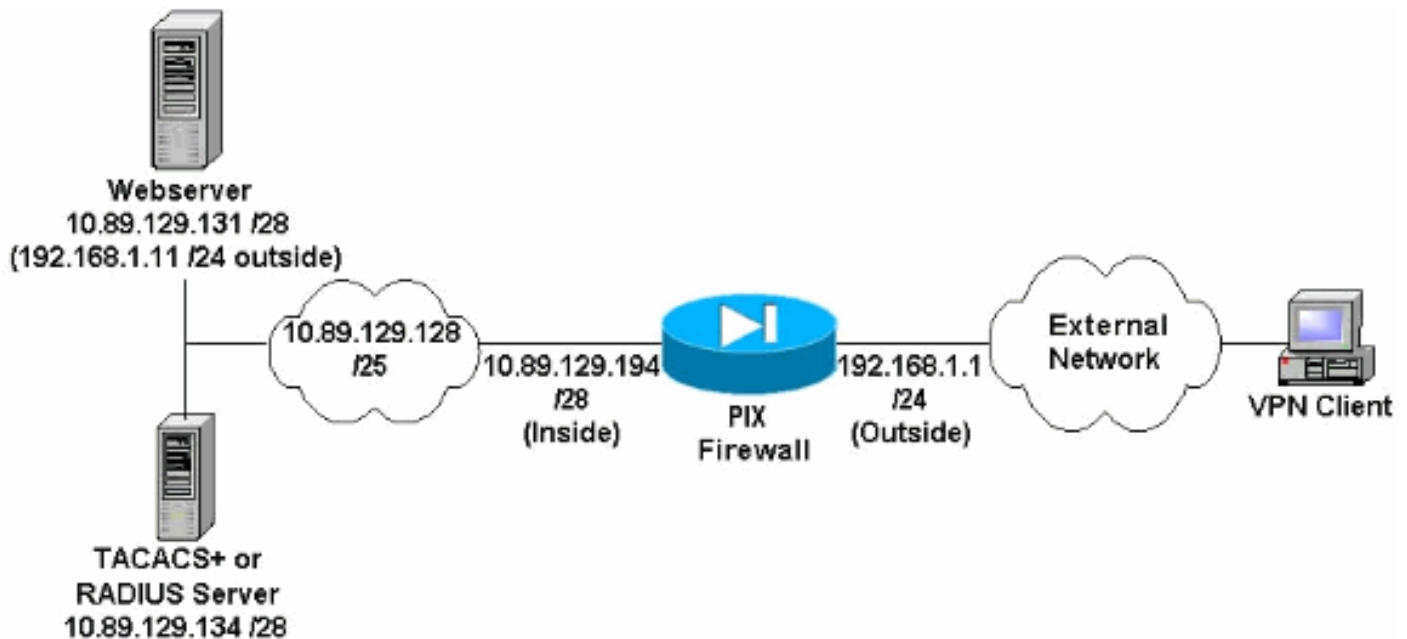
## Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Note:** Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :



## Remarques sur les diagrammes de réseau

- Des hôtes d'Internet qui accèdent au web server utilisant l'adresse IP globale 192.168.1.1 sont authentifiés même si une connexion VPN n'est pas établie. Ce trafic n'est pas chiffré.
- Les clients vpn peuvent accéder à tous les hôtes sur le réseau intérieur (10.89.129.128 /25) une fois que leur tunnel d'IPsec est établi. Tout le trafic du client vpn au Pare-feu PIX est chiffré. Sans tunnel d'IPsec, ils peuvent seulement accéder au web server par l'intermédiaire de son adresse IP globale mais sont toujours exigés pour authentifier.
- Les clients vpn proviennent l'Internet et leurs adresses IP ne sont pas connues à l'avance.

## Configurations

Ce document utilise les configurations suivantes.

- [Configuration PIX 6.3\(3\)](#)
- [Configuration du client vpn 4.0.5](#)
- [Configuration du client vpn 3.5](#)
- [Configuration du client vpn 1.1](#)

### Configuration PIX 6.3(3)

```
pixfirewall#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 100full
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
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
!--- Do not use Network Address Translation (NAT) for
inside-to-pool !--- traffic. This should not go through
NAT. access-list 101 permit ip 10.89.129.128
255.255.255.240 10.89.129.192 255.255.255.240 !---
Permits Internet Control Message Protocol (ICMP) !---
Transmission Control Protocol (TCP) and User Datagram
Protocol (UDP) !--- traffic from any host on the
Internet (non-VPN) to the web server. access-list 120
permit icmp any host 10.89.129.131 access-list 120
permit tcp any host 10.89.129.131 access-list 120 permit
udp any host 10.89.129.131 pager lines 24 mtu outside
1500 mtu inside 1500 ip address outside 192.168.1.1
255.255.255.0 ip address inside 10.89.129.194
255.255.255.240 ip audit info action alarm ip audit
attack action alarm !--- Specifies the inside IP address
range to be assigned !--- to the VPN Clients. ip local
pool VPNpool 10.89.129.200-10.89.129.204 no failover
failover timeout 0:00:00 failover poll 15 no failover ip
address outside no failover ip address inside pdm
history enable arp timeout 14400 !--- Defines a pool of
global addresses to be used by NAT. global (outside) 1
192.168.1.6-192.168.1.10 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--- Specifies which
outside IP address to apply to the web server. static
(inside,outside) 192.168.1.11 10.89.129.131 netmask
255.255.255.255 0 0 !--- Apply ACL 120 to the outside
interface in the inbound direction. access-group 120 in
```

```

interface outside !--- Defines a default route for the
PIX. route outside 0.0.0.0 0.0.0.0 192.168.1.3 1 !---
Defines a route for traffic within the PIX's !--- subnet
to reach other inside hosts. route inside 10.89.129.128
255.255.255.128 10.89.129.193 1 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
RADIUS protocol radius aaa-server LOCAL protocol local
!--- Authentication, authorization, and accounting (AAA)
statements !--- for authentication. !--- Use either of
these statements to define the protocol of the group
AuthInbound. !--- You cannot use both.
aaa-server AuthInbound protocol tacacs+

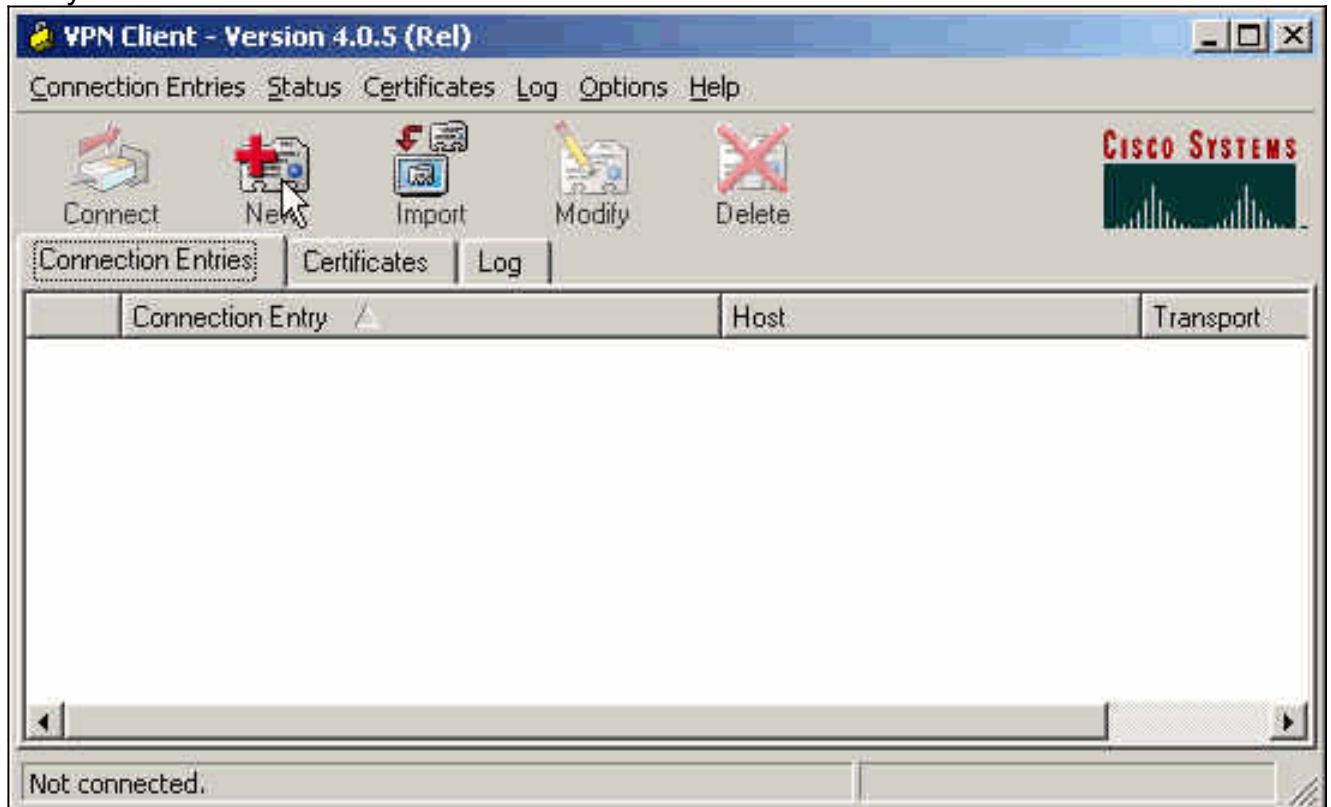
!--- OR aaa-server AuthInbound protocol radius !---
After you define the protocol of the group AuthInbound,
define !--- a server of the same type. !--- In this case
we specify the TACACS+ server and key of "secretkey".
aaa-server AuthInbound (inside) host 10.89.129.134
secretkey timeout 10 !--- Authenticate HTTP, FTP, and
Telnet traffic to the web server. aaa authentication
include http outside 10.89.129.131 255.255.255.255
0.0.0.0 0.0.0.0 AuthInbound aaa authentication include
ftp outside 10.89.129.131 255.255.255.255 0.0.0.0
0.0.0.0 AuthInbound aaa authentication include telnet
outside 10.89.129.131 255.255.255.255 0.0.0.0 0.0.0.0
AuthInbound no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- Trust IPsec traffic
and avoid going through ACLs/NAT. sysopt connection
permit-ipsec !--- IPsec and dynamic map configuration.
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap !---
Assign IP address for VPN 1.1 Clients. crypto map mymap
client configuration address initiate crypto map mymap
client configuration address respond !--- Use the AAA
server for authentication (AuthInbound). crypto map
mymap client authentication AuthInbound !--- Apply the
IPsec/AAA/ISAKMP configuration to the outside interface.
crypto map mymap interface outside isakmp enable outside
!--- Pre-shared key for VPN 1.1 Clients. isakmp key
***** address 0.0.0.0 netmask 0.0.0.0 isakmp identity
address !--- Assign address from "VPNpool" pool for VPN
1.1 Clients. isakmp client configuration address-pool
local VPNpool outside !--- ISAKMP configuration for VPN
Client 3.x/4.x. isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 2 isakmp policy 10
lifetime 86400 !--- ISAKMP configuration for VPN Client
1.x. isakmp policy 20 authentication pre-share isakmp
policy 20 encryption des isakmp policy 20 hash md5
isakmp policy 20 group 1 isakmp policy 20 lifetime 86400
!--- Assign addresses from "VPNpool" for VPN Client
3.x/4.x. vpngroup vpn3000 address-pool VPNpool vpngroup
vpn3000 idle-time 1800 !--- Group password for VPN
Client 3.x/4.x (not shown in configuration). vpngroup
vpn3000 password ***** telnet timeout 5 ssh timeout 5
console timeout 0 terminal width 80
Cryptochecksum:ba54c063d94989cbd79076955dbfeefc : end
pixfirewall#

```

## [Configuration du client vpn 4.0.5](#)

Terminez-vous ces étapes pour configurer le client vpn 4.0.5.

1. Sélectionnez **Démarrer > Programmes > Client VPN Cisco Systems > Client VPN**.
2. Cliquez sur **New** pour ouvrir la fenêtre Create New VPN Connection Entry.



3. Entrez le nom de l'entrée de connexion avec une description. Entrez l'adresse IP externe du pare-feu PIX dans la zone Host. Entrez ensuite le nom du groupe VPN et le mot de passe, puis cliquez sur

**VPN Client | Create New VPN Connection Entry**

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication  Mutual Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

Name:

Send CA Certificate Chain

Erase User Password | **Save** | Cancel

Save.

4. De la fenêtre principale de client vpn, cliquez sur en fonction la connexion que vous voudriez au clic d'utiliser-et le bouton **Connect**.

**VPN Client - Version 4.0.5 (Rel)**

Connection Entries | Status | Certificates | Log | Options | Help

Connect | New | Import | Modify | Delete

Connection Entries | Certificates | Log

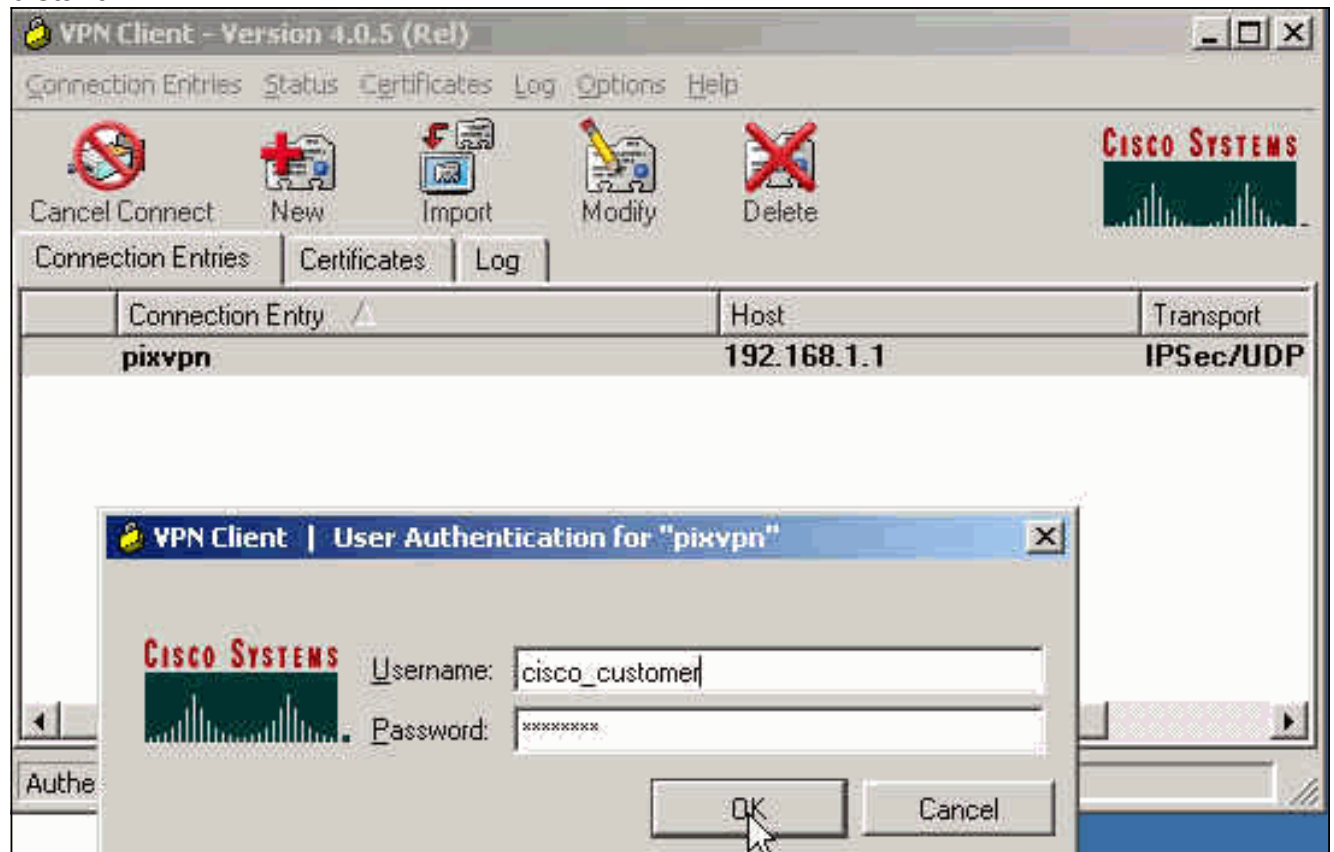
Connection Entry	Host	Transport
<b>pixvpn</b>	<b>192.168.1.1</b>	<b>IPSec/UDP</b>

Not connected.

5. Lorsque vous y êtes invité, saisissez le nom d'utilisateur et le mot de passe pour Xauth et



cliquez sur **OK** pour vous connecter au réseau distant.



### [Configuration du client vpn 3.5](#)

Terminez-vous ces étapes pour configurer la configuration du client vpn 3.5.

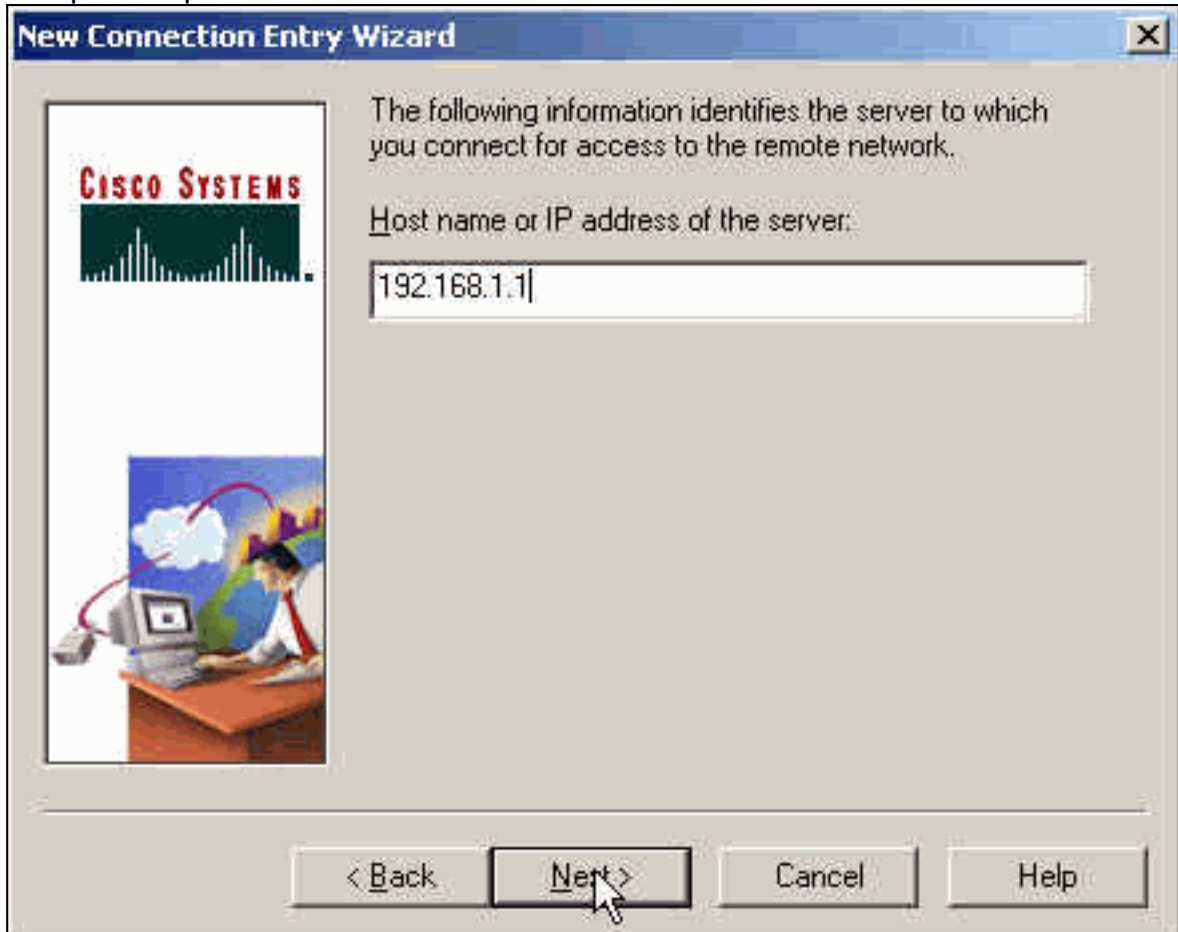
1. Sélectionnez le **début > les programmes > le client vpn de Cisco Systems > le numéroteur VPN.**
2. Cliquez sur **New** pour lancer le nouvel assistant d'entrée de connexion.
3. Écrivez le nom de votre nouvelle entrée de connexion et cliquez sur





Next.

4. Écrivez le nom d'hôte ou l'adresse IP du serveur qui est utilisé pour se connecter au serveur distant et pour cliquer sur



Next.

5. Le Group Access Information choisi et entrent le nom et le mot de passe qui est utilisé pour

authentifier votre accès au serveur distant. Cliquez sur **Next**



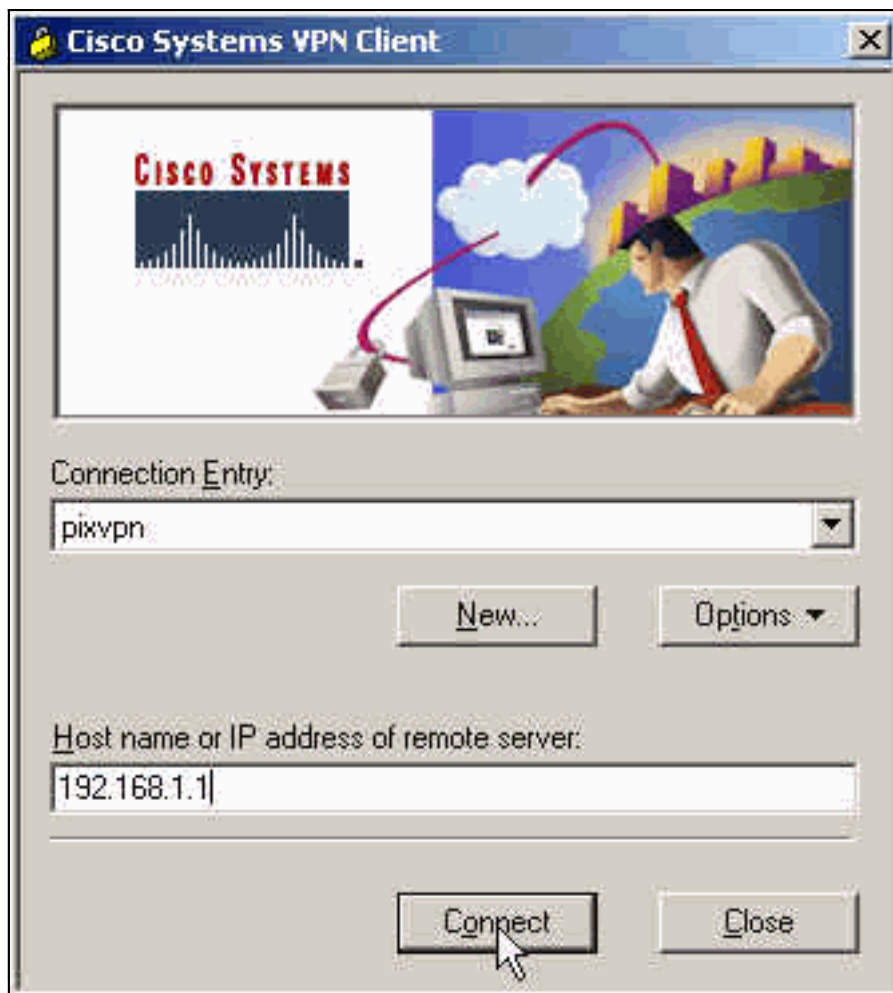
(Suivant).

6. Cliquez sur Finish pour sauvegarder la nouvelle



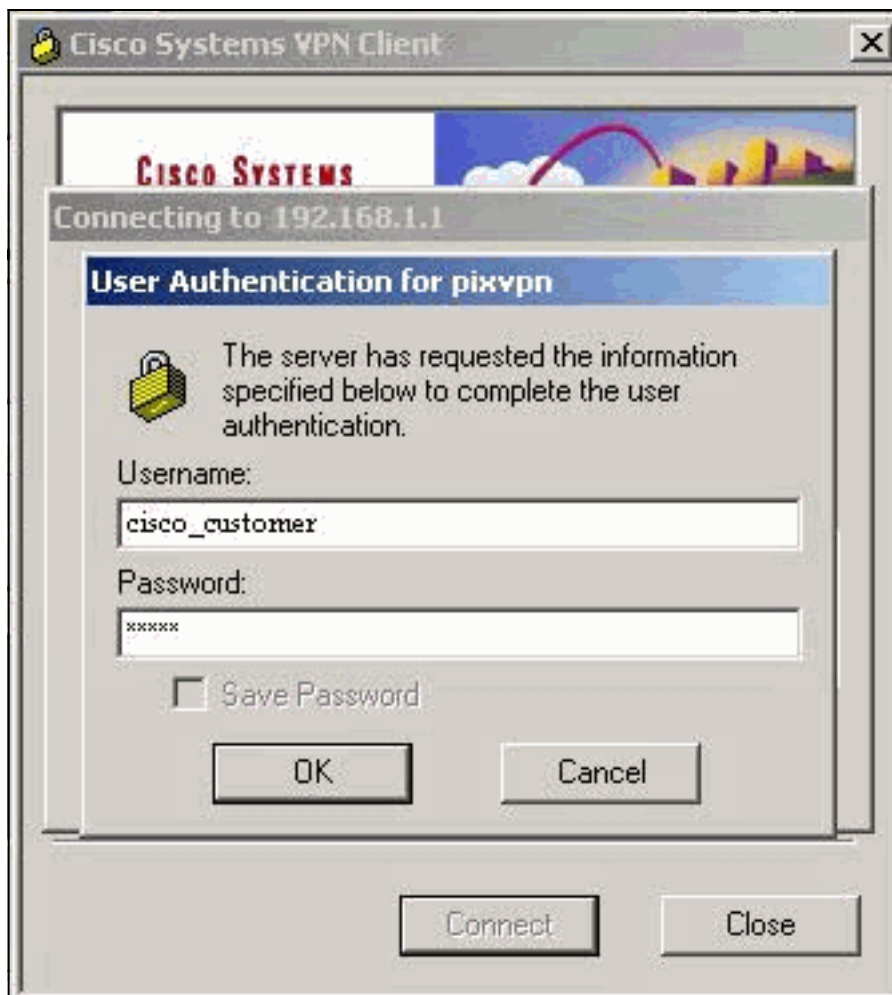
entrée.

7. Sélectionnez l'entrée de connexion dans le numéroteur et le clic **se**



connectent.

8. Lorsque vous y êtes invité, saisissez le nom d'utilisateur et le mot de passe pour Xauth et cliquez sur **OK** pour vous connecter au réseau



distant.

### Configuration du client vpn 1.1

```
pixfirewall#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 100full
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
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
!--- Do not use Network Address Translation (NAT) for
inside-to-pool !--- traffic. This should not go through
NAT. access-list 101 permit ip 10.89.129.128
255.255.255.240 10.89.129.192 255.255.255.240 !---
```

```

Permits Internet Control Message Protocol (ICMP) !---
Transmission Control Protocol (TCP) and User Datagram
Protocol (UDP) !--- traffic from any host on the
Internet (non-VPN) to the web server. access-list 120
permit icmp any host 10.89.129.131 access-list 120
permit tcp any host 10.89.129.131 access-list 120 permit
udp any host 10.89.129.131 pager lines 24 mtu outside
1500 mtu inside 1500 ip address outside 192.168.1.1
255.255.255.0 ip address inside 10.89.129.194
255.255.255.240 ip audit info action alarm ip audit
attack action alarm !--- Specifies the inside IP address
range to be assigned !--- to the VPN Clients. ip local
pool VPNpool 10.89.129.200-10.89.129.204 no failover
failover timeout 0:00:00 failover poll 15 no failover ip
address outside no failover ip address inside pdm
history enable arp timeout 14400 !--- Defines a pool of
global addresses to be used by NAT. global (outside) 1
192.168.1.6-192.168.1.10 nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--- Specifies which
outside IP address to apply to the web server. static
(inside,outside) 192.168.1.11 10.89.129.131 netmask
255.255.255.255 0 0 !--- Apply ACL 120 to the outside
interface in the inbound direction. access-group 120 in
interface outside !--- Defines a default route for the
PIX. route outside 0.0.0.0 0.0.0.0 192.168.1.3 1 !---
Defines a route for traffic within the PIX's !--- subnet
to reach other inside hosts. route inside 10.89.129.128
255.255.255.128 10.89.129.193 1 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
RADIUS protocol radius aaa-server LOCAL protocol local
!--- Authentication, authorization, and accounting (AAA)
statements !--- for authentication. !--- Use either of
these statements to define the protocol of the group
AuthInbound. !--- You cannot use both.
aaa-server AuthInbound protocol tacacs+

!--- OR aaa-server AuthInbound protocol radius !---
After you define the protocol of the group AuthInbound,
define !--- a server of the same type. !--- In this case
we specify the TACACS+ server and key of "secretkey".
aaa-server AuthInbound (inside) host 10.89.129.134
secretkey timeout 10 !--- Authenticate HTTP, FTP, and
Telnet traffic to the web server. aaa authentication
include http outside 10.89.129.131 255.255.255.255
0.0.0.0 0.0.0.0 AuthInbound aaa authentication include
ftp outside 10.89.129.131 255.255.255.255 0.0.0.0
0.0.0.0 AuthInbound aaa authentication include telnet
outside 10.89.129.131 255.255.255.255 0.0.0.0 0.0.0.0
AuthInbound no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- Trust IPsec traffic
and avoid going through ACLs/NAT. sysopt connection
permit-ipsec !--- IPsec and dynamic map configuration.
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap !---
Assign IP address for VPN 1.1 Clients. crypto map mymap
client configuration address initiate crypto map mymap
client configuration address respond !--- Use the AAA
server for authentication (AuthInbound). crypto map
mymap client authentication AuthInbound !--- Apply the

```



```

IPsec/AAA/ISAKMP configuration to the outside interface.
crypto map mymap interface outside isakmp enable outside
!--- Pre-shared key for VPN 1.1 Clients. isakmp key
***** address 0.0.0.0 netmask 0.0.0.0 isakmp identity
address !--- Assign address from "VPNpool" pool for VPN
1.1 Clients. isakmp client configuration address-pool
local VPNpool outside !--- ISAKMP configuration for VPN
Client 3.x/4.x. isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 2 isakmp policy 10
lifetime 86400 !--- ISAKMP configuration for VPN Client
1.x. isakmp policy 20 authentication pre-share isakmp
policy 20 encryption des isakmp policy 20 hash md5
isakmp policy 20 group 1 isakmp policy 20 lifetime 86400
!--- Assign addresses from "VPNpool" for VPN Client
3.x/4.x. vpngroup vpn3000 address-pool VPNpool vpngroup
vpn3000 idle-time 1800 !--- Group password for VPN
Client 3.x/4.x (not shown in configuration). vpngroup
vpn3000 password ***** telnet timeout 5 ssh timeout 5
console timeout 0 terminal width 80
Cryptochecksum:ba54c063d94989cbd79076955dbfeefc : end
pixfirewall#

```

## [Ajoutez la gestion des comptes](#)

La syntaxe de la commande d'ajouter la comptabilité est :

```
aaa accounting include acctg_service inbound|outbound l_ip l_mask [f_ip f_mask] server_tag
```

Par exemple, dans la configuration PIX, cette commande est ajoutée :

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

**Note:** La commande d'autorisation-ipsec de connexion de sysopt, pas la commande pl-compatible d'ipsec de sysopt, est nécessaire pour que la comptabilité de Xauth fonctionne. La comptabilité de Xauth ne fonctionne pas avec seulement la commande pl-compatible d'ipsec de sysopt. La comptabilité de Xauth est valide pour des connexions TCP, pas l'ICMP ou l'UDP.

Cette sortie est un exemple des enregistrements des comptes TACACS+ :

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

## [Vérifiez](#)

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .



**Note:** Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Permettez au visualiseur Cisco Secure de log afin de voir que le côté client met au point.

- **debug crypto ipsec** — Utilisé pour voir les négociations IPSEcs de la phase 2.
- **debug crypto isakmp** — Utilisé pour voir les négociations ISAKMP de la phase 1.

## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. L'exemple de sortie Debug est également affiché.

### Dépannage des commandes

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

**Note:** Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug crypto engine** — Utilisé pour mettre au point le processus de moteur de chiffrement.

### Échantillon de debug PIX

```
pixfirewall#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
  tx      Off
  rx      Off
  open    Off
  cable   Off
  txdmp   Off
  rxdmp   Off
  ifc     Off
  rxip    Off
  txip    Off
  get     Off
  put     Off
  verify  Off
  switch  Off
  fail    Off
  fmsg    Off
```

### Debugs avec le client vpn 4.x

```
pixfirewall#
crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1
VPN Peer: ISAKMP: Added new peer: ip:192.168.1.2
Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:192.168.1.2 Ref cnt incremented
```

to:1 Total VPN Peers:1

OAK\_AG exchange

ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy

ISAKMP: encryption 3DES-CBC

ISAKMP: hash SHA

ISAKMP: default group 2

ISAKMP: extended auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are not acceptable. Next payload is 3

ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy

ISAKMP: encryption 3DES-CBC

ISAKMP: hash MD5

ISAKMP: default group 2

ISAKMP: extended auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are not acceptable. Next payload is 3

ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy

ISAKMP: encryption 3DES-CBC

ISAKMP: hash SHA

ISAKMP: default group 2

ISAKMP: auth pre-shared

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are not acceptable. Next payload is 3

ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy

ISAKMP: encryption 3DES-CBC

ISAKMP: hash MD5

ISAKMP: default group 2

ISAKMP: auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are not acceptable. Next payload is 3

ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy

ISAKMP: encryption DES-CBC

ISAKMP: hash SHA

ISAKMP: default group 2

ISAKMP: extended auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are not acceptable. Next payload is 3

ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy

**ISAKMP: encryption DES-CBC**

**ISAKMP: hash MD5**

**ISAKMP: default group 2**

**ISAKMP: extended auth pre-share**

**ISAKMP: life type in seconds**

**ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b**

**ISAKMP (0): atts are acceptable. Next payload is 3**

*!--- Attributes offered by the VPN Client are accepted by the PIX.* ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to a Unity client ISAKMP (0): ID payload next-payload: 10 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0) : Total payload length: 12 return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_AG exchange ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1 spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL\_CONTACT IPSEC(key\_engine): got a queue event... IPSEC(key\_engine\_delete\_sas): rec'd delete notify from ISAKMP IPSEC(key\_engine\_delete\_sas): delete all SAs shared with 192.168.1.2 ISAKMP (0): SA has been authenticated return status is IKMP\_NO\_ERROR ISAKMP/xauth: request

attribute XAUTH\_TYPE ISAKMP/xauth: request attribute XAUTH\_USER\_NAME ISAKMP/xauth: request  
attribute XAUTH\_USER\_PASSWORD ISAKMP (0:0): initiating peer config to 192.168.1.2. ID =  
1623347510 (0x60c25136) crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1  
ISAKMP\_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2.  
message ID = 84 ISAKMP: Config payload CFG\_REPLY return status is IKMP\_ERR\_NO\_RETRANS ISAKMP  
(0:0): initiating peer config to 192.168.1.2. ID = 2620656926 (0x9c340d1e)  
crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP\_TRANSACTION exchange  
ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 60 ISAKMP: Config  
payload CFG\_ACK return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2,  
dest 192.168.1.1 ISAKMP\_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from  
192.168.1.2. message ID = 0 ISAKMP: Config payload CFG\_REQUEST ISAKMP (0:0): checking request:  
ISAKMP: attribute IP4\_ADDRESS (1) ISAKMP: attribute IP4\_NETMASK (2) ISAKMP: attribute IP4\_DNS  
(3) ISAKMP: attribute IP4\_NBNS (4) ISAKMP: attribute ADDRESS\_EXPIRY (5) Unsupported Attr: 5  
ISAKMP: attribute APPLICATION\_VERSION (7) Unsupported Attr: 7 ISAKMP: attribute UNKNOWN (28672)  
Unsupported Attr: 28672 ISAKMP: attribute UNKNOWN (28673) Unsupported Attr: 28673 ISAKMP:  
attribute UNKNOWN (28674) ISAKMP: attribute UNKNOWN (28676) ISAKMP: attribute UNKNOWN (28679)  
Unsupported Attr: 28679 ISAKMP: attribute UNKNOWN (28680) Unsupported Attr: 28680 ISAKMP:  
attribute UNKNOWN (28677) Unsupported Attr: 28677 ISAKMP (0:0): responding to peer config from  
192.168.1.2. ID = 177917346 return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src  
192.168.1.2, dest 192.168.1.1 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_IDLE ISAKMP (0):  
processing SA payload. message ID = 942875080 ISAKMP : Checking IPsec proposal 1 ISAKMP:  
transform 1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP:  
encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b  
IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported ISAKMP  
(0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (1) ISAKMP  
: Checking IPsec proposal 2 ISAKMP: transform 1, ESP\_3DES ISAKMP: attributes in transform:  
ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA  
life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3,  
trans 3, hmac\_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP  
(0): skipping next ANDED proposal (2) ISAKMP: Checking IPsec proposal 3 ISAKMP: transform 1,  
ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1  
ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b  
IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported ISAKMP  
(0): atts not acceptable. Next payload is 0 ISAKMP: Checking IPsec proposal 4 ISAKMP: transform  
1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is  
1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b  
IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 2) not supported ISAKMP  
(0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 5 ISAKMP: transform  
1, ESP\_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is  
1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP  
(0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP: Checking IPsec proposal  
6 ISAKMP: transform 1, ESP\_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-  
SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0  
0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3, trans 2, hmac\_alg 2) not  
supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED  
proposal (6) ISAKMP : Checking IPsec proposal 7 ISAKMP: transform 1, ESP\_DES ISAKMP: attributes  
in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in  
seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are  
acceptable.IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.) dest=  
192.168.1.1, src= 192.168.1.2, dest\_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1), src\_proxy=  
10.89.129.200/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing  
NONCE payload. message ID = 942875080 ISAKMP (0): processing ID payload. message ID = 942875080  
ISAKMP (0): ID\_IPV4\_ADDR src 10.89.129.200 prot 0 port 0 ISAKMP (0): processing ID payload.  
message ID = 942875080 ISAKMP (0): ID\_IPV4\_ADDR dst 192.168.1.1 prot 0 port 0IPSEC(key\_engine):  
got a queue event... IPSEC(spi\_response): getting spi 0x64d7a518(1691854104) for SA from  
192.168.1.2 to 192.168.1.1 for prot 3 return status is IKMP\_NO\_ERROR  
crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_QM exchange  
oakley\_process\_quick\_mode: OAK\_QM\_IDLE ISAKMP (0): processing SA payload. message ID =  
3008609960 ISAKMP: Checking IPsec proposal 1 ISAKMP: transform 1, ESP\_3DES ISAKMP: attributes in  
transform: ISAKMP: authenticator is HMAC-MD5 crypto\_isakmp\_process\_block: src 192.168.1.2, dest  
192.168.1.1 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_AUTH\_AWAITmap\_alloc\_entry:  
allocating entry 2 map\_alloc\_entry: allocating entry 1ISAKMP (0): Creating IPsec SAs inbound SA  
from 192.168.1.2 to 192.168.1.1 (proxy 10.89.129.200 to 192.168.1.1) has spi 1691854104 and

```
conn_id 2 and flags 4 lifetime of 2147483 seconds outbound SA from 192.168.1.1 to 192.168.1.2
(proxy 192.168.1.1 to 10.89.129.200) has spi 1025193431 and conn_id 1 and flags 4 lifetime of
2147483 seconds IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): ,(key eng. msg.)
dest= 192.168.1.1, src= 192.168.1.2, dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), src_proxy=
10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
2147483s and 0kb, spi= 0x64d7a518(1691854104),conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,(key eng. msg.) src= 192.168.1.1, dest=192.168.1.2, src_proxy=
192.168.1.1/0.0.0.0/0/0 (type=1), dest_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP,
transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x3d1b35d7(1025193431),conn_id=
1, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:2 Total
VPN Peers:1 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1
OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 4
map_alloc_entry: allocating entry 3 ISAKMP (0): Creating IPsec SAs inbound SA from 192.168.1.2
to 192.168.1.1 (proxy 10.89.129.200 to 0.0.0.0) has spi 3415657865 and conn_id 4 and flags 4
lifetime of 2147483 seconds outbound SA from 192.168.1.1 to 192.168.1.2 (proxy 0.0.0.0 to
10.89.129.200) has spi 2383969893 and conn_id 3 and flags 4 lifetime of 2147483
secondsIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): ,(key eng. msg.) dest=
192.168.1.1, src=192.168.1.2, dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), src_proxy=
10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform=esp-des esp-md5-hmac , lifedur=
2147483s and 0kb, spi= 0xcb96cd89(3415657865),conn_id= 4, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,(key eng. msg.) src= 192.168.1.1, dest=192.168.1.2, src_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), dest_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP,
transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x8e187e65(2383969893),conn_id=
3, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:4 Total
VPN Peers:1 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:5 Total VPN Peers:1
return status is IKMP_NO_ERROR pixfirewall#show uauth
Current      Most Seen
Authenticated Users
1            1
Authen In Progress
0            1
ipsec user 'cisco_customer' at 10.89.129.200, authenticated
pixfirewall#
```

## [Debugs avec le client vpn 1.1](#)

```
pixfirewall#
crypto_isakmp_process_block: src 192.168.1.2, dest 192.168.1.1
VPN Peer: ISAKMP: Added new peer: ip:192.168.1.2
Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:192.168.1.2 Ref cnt incremented
to:1 Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
```

ISAKMP: encryption 3DES-CBC  
ISAKMP: hash SHA  
ISAKMP: default group 2  
ISAKMP: auth pre-shared  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy  
ISAKMP: encryption 3DES-CBC  
ISAKMP: hash MD5  
ISAKMP: default group 2  
ISAKMP: auth pre-share  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy  
ISAKMP: encryption DES-CBC  
ISAKMP: hash SHA  
ISAKMP: default group 2  
ISAKMP: extended auth pre-share  
ISAKMP: life type in seconds  
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b  
ISAKMP (0): atts are not acceptable. Next payload is 3  
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy  
**ISAKMP: encryption DES-CBC**  
**ISAKMP: hash MD5**  
**ISAKMP: default group 2**  
**ISAKMP: extended auth pre-share**  
**ISAKMP: life type in seconds**  
**ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b**  
**ISAKMP (0): atts are acceptable. Next payload is 3**  
*!--- Attributes offered by the VPN Client are accepted by the PIX.* ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to a Unity client ISAKMP (0): ID payload next-payload: 10 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0) : Total payload length: 12 return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_AG exchange ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1 spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL\_CONTACT IPSEC(key\_engine): got a queue event... IPSEC(key\_engine\_delete\_sas): rec'd delete notify from ISAKMP IPSEC(key\_engine\_delete\_sas): delete all SAs shared with 192.168.1.2 ISAKMP (0): SA has been authenticated return status is IKMP\_NO\_ERROR ISAKMP/xauth: request attribute XAUTH\_TYPE ISAKMP/xauth: request attribute XAUTH\_USER\_NAME ISAKMP/xauth: request attribute XAUTH\_USER\_PASSWORD ISAKMP (0:0): initiating peer config to 192.168.1.2. ID = 1623347510 (0x60c25136) crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP\_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 84 ISAKMP: Config payload CFG\_REPLY return status is IKMP\_ERR\_NO\_RETRANS ISAKMP (0:0): initiating peer config to 192.168.1.2. ID = 2620656926 (0x9c340dle) crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP\_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 60 ISAKMP: Config payload CFG\_ACK return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 ISAKMP\_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 192.168.1.2. message ID = 0 ISAKMP: Config payload CFG\_REQUEST ISAKMP (0:0): checking request: ISAKMP: attribute IP4\_ADDRESS (1) ISAKMP: attribute IP4\_NETMASK (2) ISAKMP: attribute IP4\_DNS (3) ISAKMP: attribute IP4\_NBNS (4) ISAKMP: attribute ADDRESS\_EXPIRY (5) Unsupported Attr: 5 ISAKMP: attribute APPLICATION\_VERSION (7) Unsupported Attr: 7 ISAKMP: attribute UNKNOWN (28672) Unsupported Attr: 28672 ISAKMP: attribute UNKNOWN (28673) Unsupported Attr: 28673 ISAKMP: attribute UNKNOWN (28674) ISAKMP: attribute UNKNOWN (28676) ISAKMP: attribute UNKNOWN (28679) Unsupported Attr: 28679 ISAKMP: attribute UNKNOWN (28680) Unsupported Attr: 28680 ISAKMP: attribute UNKNOWN (28677) Unsupported Attr: 28677 ISAKMP (0:0): responding to peer config from 192.168.1.2. ID = 177917346 return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_IDLE ISAKMP (0): processing SA payload. message ID = 942875080 ISAKMP : Checking IPsec proposal 1 ISAKMP:

transform 1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (1) ISAKMP : Checking IPsec proposal 2 ISAKMP: transform 1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (2) ISAKMP: Checking IPsec proposal 3 ISAKMP: transform 1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 1) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP: Checking IPsec proposal 4 ISAKMP: transform 1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3, trans 3, hmac\_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP : Checking IPsec proposal 5 ISAKMP: transform 1, ESP\_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable. ISAKMP (0): bad SPI size of 2 octets! ISAKMP: Checking IPsec proposal 6 ISAKMP: transform 1, ESP\_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-SHA ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC(validate\_proposal): transform proposal (prot 3, trans 2, hmac\_alg 2) not supported ISAKMP (0): atts not acceptable. Next payload is 0 ISAKMP (0): skipping next ANDED proposal (6) ISAKMP : Checking IPsec proposal 7 ISAKMP: transform 1, ESP\_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b ISAKMP (0): atts are acceptable.IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.) dest= 192.168.1.1, src= 192.168.1.2, dest\_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1), src\_proxy= 10.89.129.200/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 942875080 ISAKMP (0): processing ID payload. message ID = 942875080 ISAKMP (0): ID\_IPV4\_ADDR src 10.89.129.200 prot 0 port 0 ISAKMP (0): processing ID payload. message ID = 942875080 ISAKMP (0): ID\_IPV4\_ADDR dst 192.168.1.1 prot 0 port 0IPSEC(key\_engine): got a queue event... IPSEC(spi\_response): getting spi 0x64d7a518(1691854104) for SA from 192.168.1.2 to 192.168.1.1 for prot 3 return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_IDLE ISAKMP (0): processing SA payload. message ID = 3008609960 ISAKMP: Checking IPsec proposal 1 ISAKMP: transform 1, ESP\_3DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_AUTH\_AWAITmap\_alloc\_entry: allocating entry 2 map\_alloc\_entry: allocating entry 1 ISAKMP (0): Creating IPsec SAs inbound SA from 192.168.1.2 to 192.168.1.1 (proxy 10.89.129.200 to 192.168.1.1) has spi 1691854104 and conn\_id 2 and flags 4 lifetime of 2147483 seconds outbound SA from 192.168.1.1 to 192.168.1.2 (proxy 192.168.1.1 to 10.89.129.200) has spi 1025193431 and conn\_id 1 and flags 4 lifetime of 2147483 seconds IPSEC(key\_engine): got a queue event... IPSEC(initialize\_sas): ,(key eng. msg.) dest= 192.168.1.1, src= 192.168.1.2, dest\_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), src\_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x64d7a518(1691854104),conn\_id= 2, keysize= 0, flags= 0x4 IPSEC(initialize\_sas): , (key eng. msg.) src= 192.168.1.1, dest=192.168.1.2, src\_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), dest\_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x3d1b35d7(1025193431),conn\_id= 1, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block: src 192.168.1.2, dest 192.168.1.1 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_AUTH\_AWAITmap\_alloc\_entry: allocating entry 4 map\_alloc\_entry: allocating entry 3 ISAKMP (0): Creating IPsec SAs inbound SA from 192.168.1.2 to 192.168.1.1 (proxy 10.89.129.200 to 0.0.0.0) has spi 3415657865 and conn\_id 4 and flags 4 lifetime of 2147483 seconds outbound SA from 192.168.1.1 to 192.168.1.2 (proxy 0.0.0.0 to 10.89.129.200) has spi 2383969893 and conn\_id 3 and flags 4 lifetime of 2147483 secondsIPSEC(key\_engine): got a queue event... IPSEC(initialize\_sas): , (key eng. msg.) dest= 192.168.1.1, src=192.168.1.2, dest\_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), src\_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP, transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0xcb96cd89(3415657865),conn\_id= 4, keysize= 0, flags= 0x4



```
IPSEC(initialize_sas): , (key eng. msg.) src= 192.168.1.1, dest=192.168.1.2, src_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), dest_proxy= 10.89.129.200/0.0.0.0/0/0 (type=1), protocol= ESP,
transform=esp-des esp-md5-hmac , lifedur= 2147483s and 0kb, spi= 0x8e187e65(2383969893),conn_id=
3, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:4 Total
VPN Peers:1 VPN Peer: IPSEC: Peer ip:192.168.1.2 Ref cnt incremented to:5 Total VPN Peers:1
return status is IKMP_NO_ERROR pixfirewall#show uauth
Current      Most Seen
Authenticated Users
1            1
Authen In Progress
0            1
ipsec user 'cisco_customer' at 10.89.129.200, authenticated
pixfirewall#
```

## [Informations connexes](#)

- [Appliances de sécurité de la gamme PIX 500](#)
- [Références des commandes du pare-feu PIX](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Introduction à IPSec](#)
- [Établissement de la Connectivité par des Pare-feu de Cisco PIX](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)