Comment configure le client VPN Cisco sur PIX avec AES

Contenu

Introduction

Cet exemple de configuration indique comment installer une connexion VPN d'accès à distance d'un client VPN Cisco à un pare-feu PIX, en utilisant l'Advanced Encryption Standard (AES) pour le chiffrement. Cet exemple utilise Cisco Easy VPN pour installer le canal sécurisé et le pare-feu PIX est configuré en tant que serveur Easy VPN.

Dans le logiciel Cisco Secure PIX Firewall version 6.3 et ultérieure, la nouvelle norme internationale de cryptage AES est prise en charge pour sécuriser les connexions VPN de site à site et d'accès à distance. Ceci s'ajoute aux algorithmes de chiffrement DES (Data Encryption Standard) et 3DES. Le pare-feu PIX prend en charge les tailles de clé AES de 128, 192 et 256 bits.

Le client VPN prend en charge AES en tant qu'algorithme de chiffrement commençant par Cisco VPN Client version 3.6.1. Le client VPN prend en charge des tailles de clés de 128 bits et 256 bits uniquement.

Conditions préalables

Conditions requises

Cet exemple de configuration suppose que le PIX est entièrement opérationnel et configuré avec les commandes nécessaires afin de gérer le trafic conformément à la stratégie de sécurité de

l'organisation.

Components Used

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

- Logiciel PIX version 6.3(1)**Remarque :** Cette configuration a été testée sur le logiciel PIX version 6.3(1) et devrait fonctionner sur toutes les versions ultérieures.
- Client VPN Cisco version 4.0.3(A)**Remarque :** Cette configuration a été testée sur le client VPN version 4.0.3(A) mais fonctionne sur les versions antérieures remontant à la version 3.6.1 et jusqu'à la version actuelle.

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.

Informations générales

Les VPN d'accès à distance adressent la condition requise du collaborateur mobile pour se connecter en toute sécurité au réseau de l'entreprise. Les utilisateurs mobiles peuvent configurer une connexion sécurisée à l'aide du logiciel client VPN installé sur leurs PC. Le client VPN initie une connexion au périphérique d'un site central configuré pour accepter ces requêtes. Dans cet exemple, le périphérique du site central est un pare-feu PIX configuré en tant que serveur Easy VPN qui utilise des crypto-cartes dynamiques.

Cisco Easy VPN simplifie le déploiement VPN en facilitant la configuration et la gestion des VPN. Il se compose du serveur Cisco Easy VPN Server et de Cisco Easy VPN Remote. Une configuration minimale est requise sur Easy VPN Remote. Easy VPN Remote établit une connexion. Si l'authentification réussit, Easy VPN Server descend la configuration VPN vers elle. Pour plus d'informations sur la configuration d'un pare-feu PIX en tant que serveur Easy VPN, consultez la section Gestion de l'accès à distance VPN.

Les crypto-cartes dynamiques sont utilisées pour la configuration IPsec lorsque certains paramètres requis pour configurer le VPN ne peuvent pas être prédéterminés, comme c'est le cas pour les utilisateurs mobiles qui obtiennent des adresses IP attribuées dynamiquement. La crypto-carte dynamique agit comme un modèle et les paramètres manquants sont déterminés lors de la négociation IPsec. Pour plus d'informations sur les crypto-cartes dynamiques, consultez Dynamic Crypto Maps.

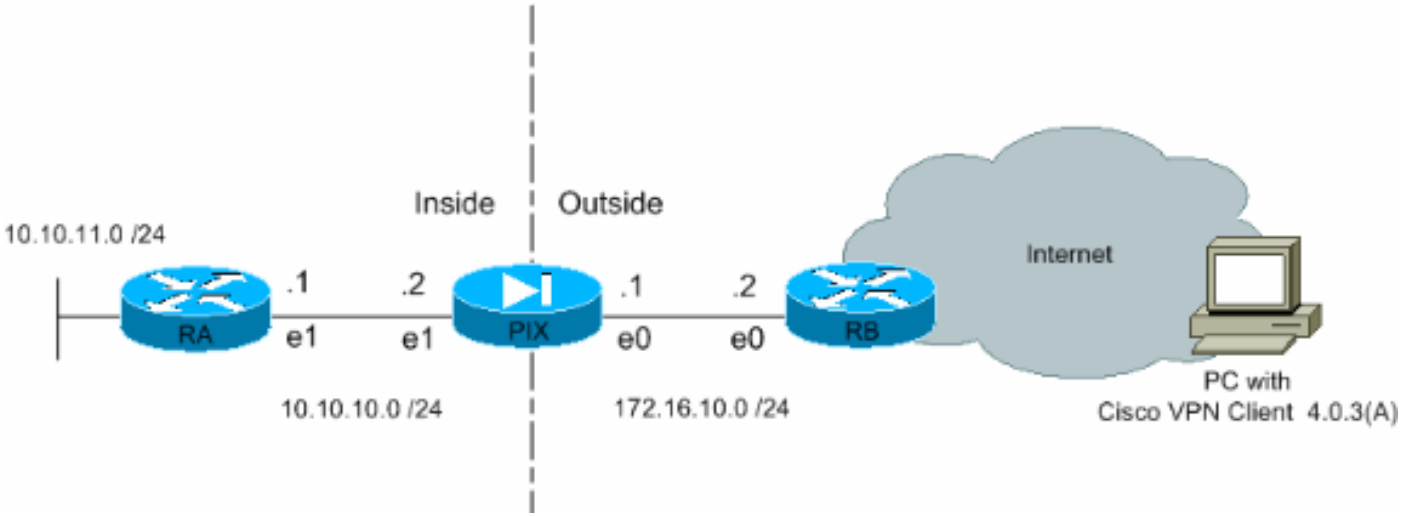
Configurations

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurer le PIX

La configuration nécessaire sur le pare-feu PIX est présentée dans ce résultat. La configuration est réservée au VPN.

PIX

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names

!--- Define the access list to enable split tunneling.
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
```

```
Define the access list to avoid network address !---
translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
255.255.255.0 access-list 102 permit ip 10.10.11.0
255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
Create a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history
enable arp timeout 14400 !--- Disable NAT for IPsec
packets. nat (inside) 0 access-list 102 route outside
0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0
255.255.255.0 10.10.10.1 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 no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Permit packet that came from an IPsec tunnel
to pass through without !--- checking them against the
configured conduits/access lists. sysopt connection
permit-ipsec !--- Define the transform set to be used
during IPsec !--- security association (SA) negotiation.
Specify AES as the encryption algorithm. crypto ipsec
transform-set trmset1 esp-aes-256 esp-sha-hmac !---
Create a dynamic crypto map entry !--- and add it to a
static crypto map. crypto dynamic-map map2 10 set
transform-set trmset1 crypto map map1 10 ipsec-isakmp
dynamic map2 !--- Bind the crypto map to the outside
interface. crypto map map1 interface outside !--- Enable
Internet Security Association and Key Management !---
Protocol (ISAKMP) negotiation on the interface on which
the IPsec !--- peer communicates with the PIX Firewall.
isakmp enable outside isakmp identity address !---
Define an ISAKMP policy to be used while !---
negotiating the ISAKMP SA. Specify !--- AES as the
encryption algorithm. The configurable AES !--- options
are aes, aes-192 and aes-256. !--- Note: AES 192 is not
supported by the VPN Client.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- Create a VPN group and configure the policy
attributes which are !--- downloaded to the Easy VPN
Clients. vpngroup groupmarketing address-pool vpnpool1
vpngroup groupmarketing dns-server 10.10.11.5 vpngroup
groupmarketing wins-server 10.10.11.5 vpngroup
groupmarketing default-domain org1.com vpngroup
groupmarketing split-tunnel 101 vpngroup groupmarketing
idle-time 1800 vpngroup groupmarketing password ********
telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421ee1c3 : end
```

Remarque : Dans cette configuration, il est recommandé de ne pas spécifier aes-192 lorsque vous configurez le jeu de transformation ou la stratégie ISAKMP. Les clients VPN ne prennent pas en charge aes-192 pour le chiffrement.

Remarque : avec les versions précédentes, les commandes de configuration du mode IKE **isakmp configuration client address-pool** et **crypto map client-configuration address** étaient requises. Cependant, avec les versions plus récentes (3.x et ultérieures), ces commandes ne sont plus nécessaires. Plusieurs pools d'adresses peuvent maintenant être spécifiés à l'aide de la commande **vpngroup address-pool**.

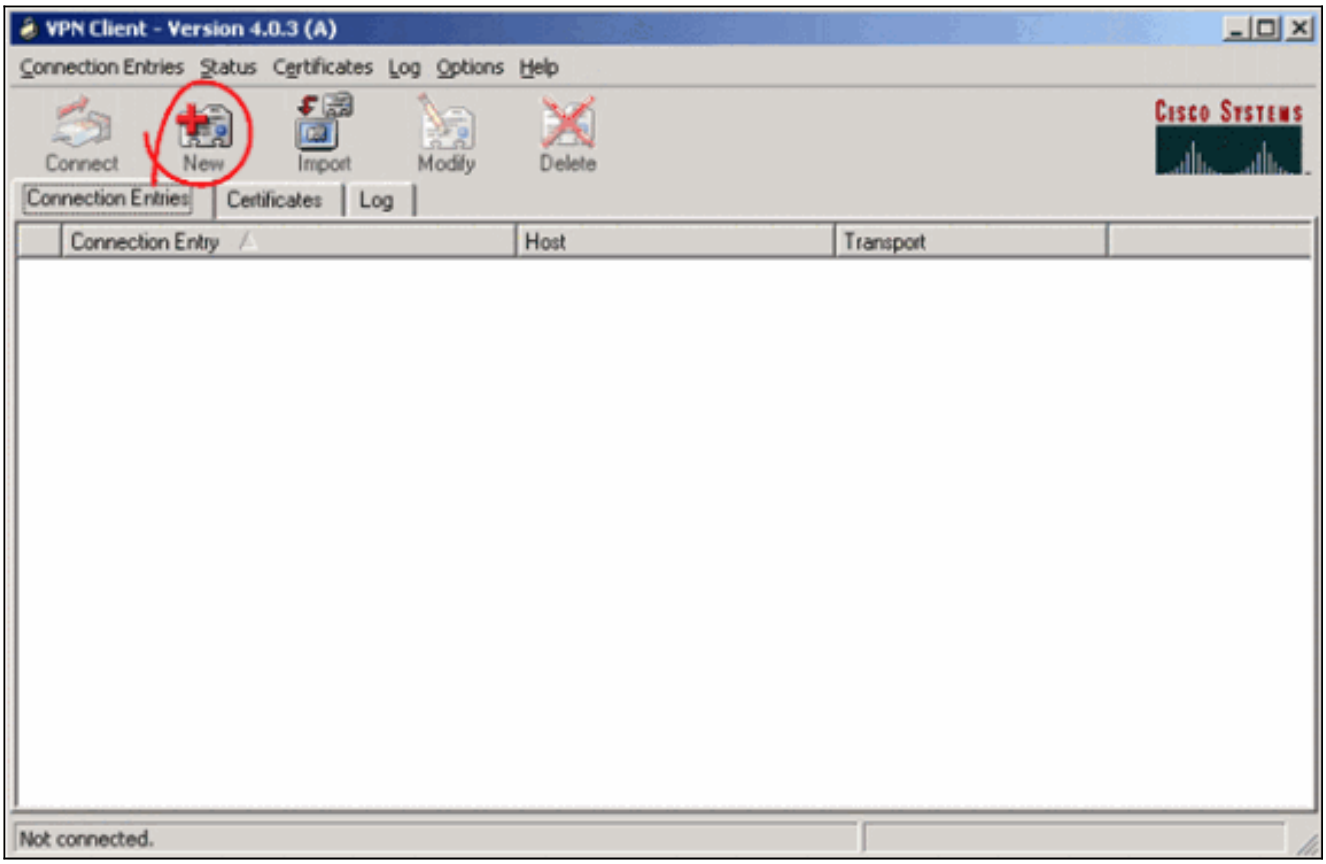
Remarque : les noms des groupes VPN sont sensibles à la casse. Cela signifie que l'authentification de l'utilisateur échoue si le nom de groupe spécifié dans le PIX et le nom de groupe sur le client VPN sont différents en termes de casse de lettre (majuscule ou minuscule).

Remarque : Par exemple, lorsque vous entrez le nom du groupe **GroupMarketing** dans un périphérique et **groupmarketing** dans un autre périphérique, le périphérique ne fonctionne pas.

Configurer le client VPN

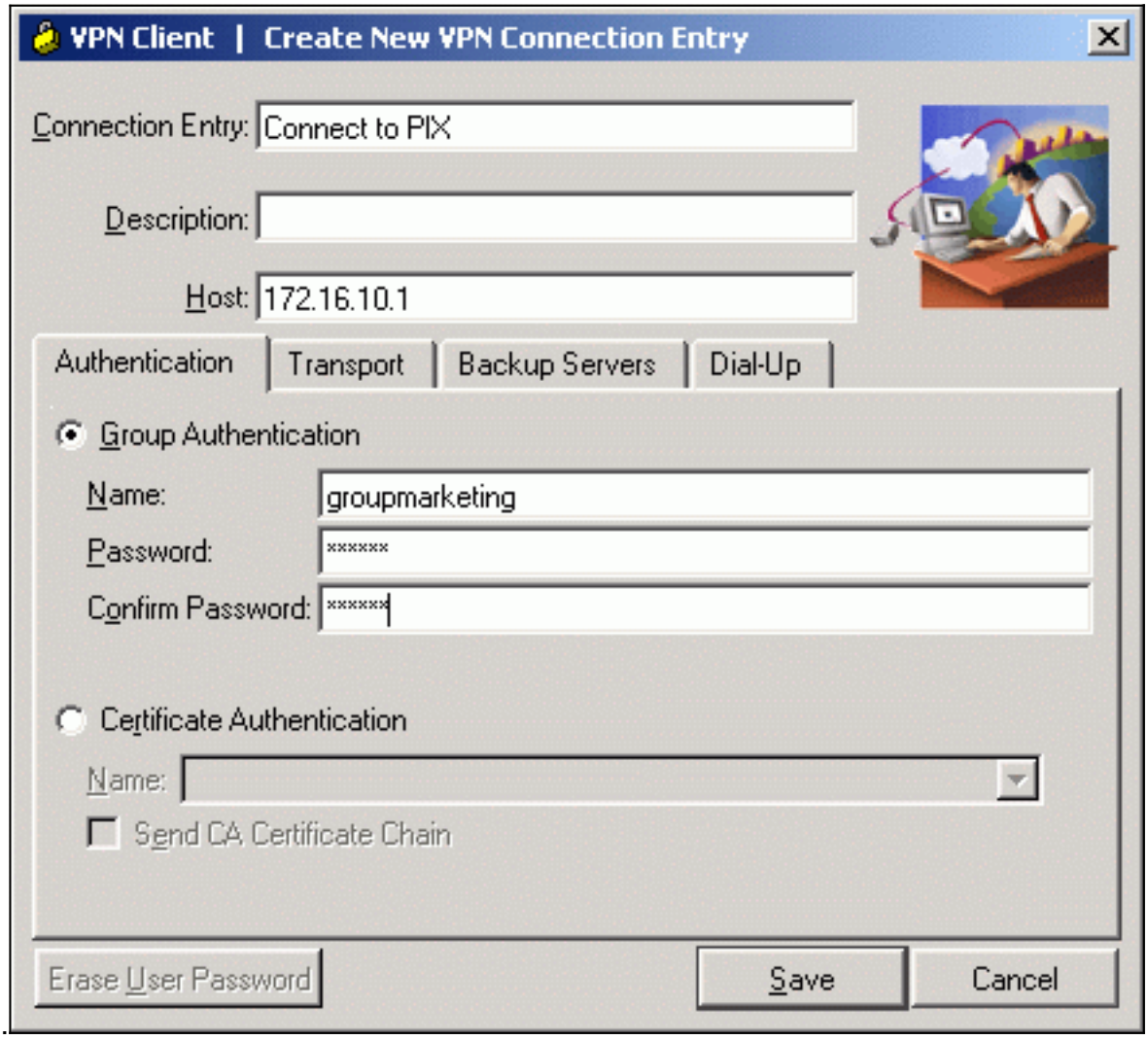
Après avoir installé le client VPN sur le PC, créez une nouvelle connexion comme indiqué dans les étapes suivantes :

1. Lancez l'application Client VPN et cliquez sur **Nouveau** pour créer une nouvelle entrée de connexion.

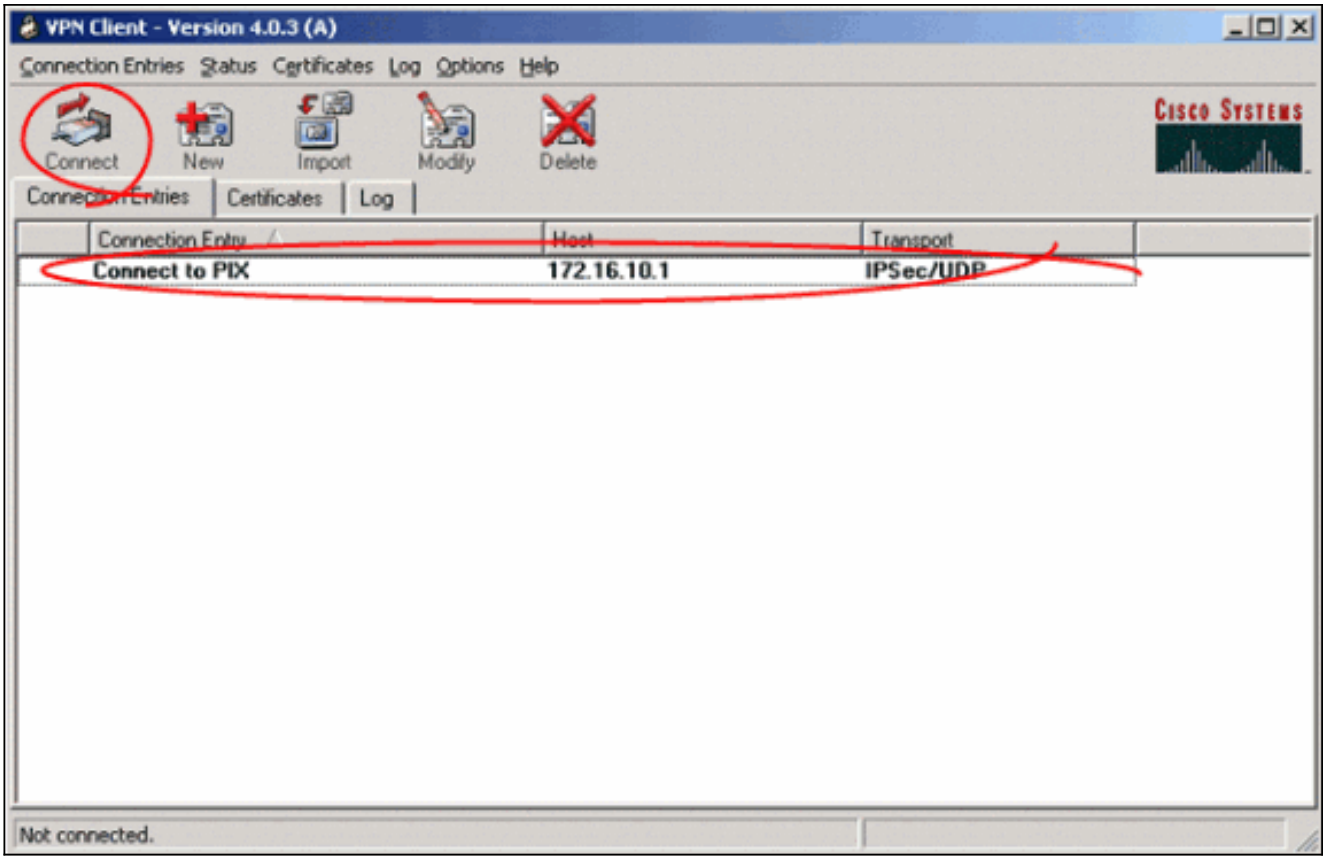


2. Une nouvelle boîte de dialogue intitulée Client VPN | Créer une entrée de connexion VPN s'affiche. Entrez les informations de configuration de la nouvelle connexion.Dans le champ Connection Entry, attribuez un nom à la nouvelle entrée créée.Dans le champ Host, saisissez l'adresse IP de l'interface publique du PIX.Sélectionnez l'onglet Authentification, puis tapez le nom et le mot de passe du groupe (deux fois - pour confirmation). Cela doit

correspondre aux informations entrées sur le PIX à l'aide de la commande **vpngroup password**.Cliquez sur **Enregistrer** pour enregistrer les informations saisies. La nouvelle connexion est maintenant créée.



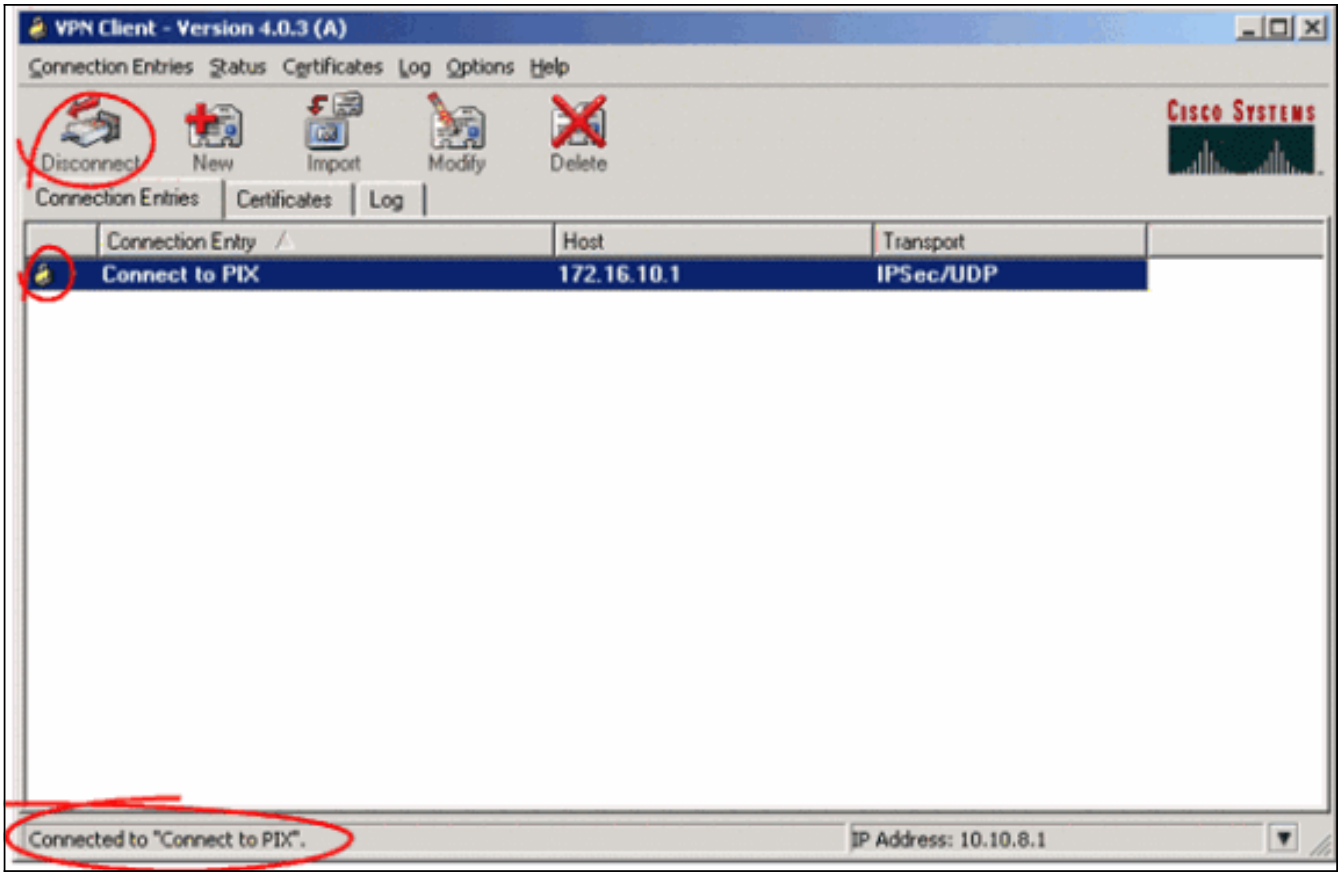
3. Afin de se connecter à la passerelle à l'aide de la nouvelle entrée de connexion, sélectionnez l'entrée de connexion en cliquant une fois dessus, puis cliquez sur l'icône **Connexion**. Un double-clic sur l'entrée de connexion a le même effet.



Vérification

Sur le client VPN, une connexion établie avec succès à la passerelle distante est indiquée par les éléments suivants :

- Une icône de verrouillage fermé jaune apparaît contre l'entrée de connexion active.
- L'icône Connect de la barre d'outils (en regard de l'onglet Connection Entries) devient Disconnect.
- La ligne d'état située à la fin de la fenêtre affiche l'état « Connecté à » suivi du nom de l'entrée de
connexion.



Remarque : Par défaut, une fois la connexion établie, le client VPN réduit à un icône de verrouillage fermé dans la barre d'état système, dans l'angle inférieur droit de la barre des tâches Windows. Double-cliquez sur l'icône de verrouillage fermé afin de rendre la fenêtre VPN Client visible à nouveau.

Sur le pare-feu PIX, ces commandes **show** peuvent être utilisées pour vérifier l'état des connexions établies.

Remarque : Certaines commandes **show** sont prises en charge par l'outil Interpréteur de sortie (clients enregistrés uniquement) , qui vous permet d'afficher une analyse de la sortie de la commande **show**.

- **show crypto ipsec sa** - Affiche toutes les SA IPsec actuelles sur le PIX. En outre, le résultat indique l'adresse IP réelle de l'homologue distant, l'adresse IP attribuée, l'adresse IP et l'interface locales, ainsi que la carte de chiffrement appliquée.

```
Pixfirewall#show crypto ipsec sa

interface: outside
    Crypto map tag: map1, local addr. 172.16.10.1

   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0)
   current_peer: 172.16.12.3:500
   dynamic allocated peer ip: 10.10.8.1

     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.12.3
```

```
path mtu 1500, ipsec overhead 64, media mtu 1500
current outbound spi: cbabd0ce

inbound esp sas:
 spi: 0x4d8a971d(1300928285)
   transform: esp-aes-256 esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2, crypto map: map1
   sa timing: remaining key lifetime (k/sec): (4607996/28685)
   IV size: 16 bytes
   replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
 spi: 0xcbabd0ce(3417034958)
   transform: esp-aes-256 esp-sha-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 1, crypto map: map1
   sa timing: remaining key lifetime (k/sec): (4608000/28676)
   IV size: 16 bytes
   replay detection support: Y


outbound ah sas:


outbound pcp sas:
```

- **show crypto isakmp sa** - Affiche l'état de la SA ISAKMP construite entre homologues.

```
Pixfirewall#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending     created
172.16.10.1      172.16.12.3    QM_IDLE         0           1
```

Dépannage

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

Ces commandes de débogage peuvent aider à résoudre les problèmes liés à la configuration du VPN.

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

- **debug crypto isakmp** - Affiche la SA ISAKMP qui est créée et les attributs IPsec qui sont négociés. Pendant la négociation ISAKMP SA, le PIX peut éventuellement rejeter plusieurs propositions comme « inacceptables » avant d'en accepter une. Une fois l'association de sécurité ISAKMP acceptée, les attributs IPsec sont négociés. Une fois de plus, plusieurs propositions peuvent être rejetées avant d'en accepter une, comme le montre ce résultat **de débogage**.

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 spt:500 dpt:500
OAK_AG exchange
```

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

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- Proposal is rejected since extended auth is not configured. ISAKMP (0): atts are not
acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- Proposal is rejected since MD5 is not specified as the hash algorithm. ISAKMP (0): atts
are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- This proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are
acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
!--- Output is suppressed. OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3348522173

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      key length is 256
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
!--- This proposal is not accepted since transform-set !--- trmset1 does not use MD5. 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_AES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      key length is 256
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
!--- This proposal is accepted since it matches !--- transform-set trmset1. ISAKMP (0): atts
are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 3
!--- Output is suppressed.
```

- **debug crypto ipsec** - Affiche des informations sur les négociations de SA IPsec.

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with     172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
        from     172.16.12.3 to     172.16.10.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4
```

Avec les configurations présentées dans ce document, le client VPN est en mesure de se connecter avec succès au PIX du site central à l'aide d'AES. Il est parfois observé que bien que le tunnel VPN soit correctement établi, les utilisateurs ne sont pas en mesure d'effectuer des tâches courantes telles que la requête ping aux ressources réseau, la connexion au domaine ou la navigation dans le voisinage du réseau. Pour plus d'informations sur le dépannage de ces problèmes, consultez Dépannage du voisinage réseau Microsoft après l'établissement d'un tunnel VPN avec le client VPN Cisco.

Informations connexes

- Standard de cryptage avancé (AES)
- Présentation du chiffrement IPSec (IP Security)
- Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage
- Page de support de la négociation IPSec/des protocoles IKE
- Page de support PIX
- Cisco VPN Client Support Page
- Référence des commandes PIX
- Support et documentation techniques - Cisco Systems