Como configurar o Cisco VPN Client ao PIX com AES

Índice

Introdução

Este exemplo de configuração mostra como configurar uma conexão VPN de acesso remoto de um Cisco VPN Client para um firewall PIX, usando o padrão AES para criptografia. Este exemplo usa o Cisco Easy VPN para instalar o canal seguro e o PIX Firewall é configurado como um servidor Easy VPN.

No Software Release 6.3 e Mais Recente do firewall PIX segura Cisco, o padrão de codificação internacional novo AES é apoiado fixando a site para site e as conexões VPN de acesso remoto. Isto é além do que o Data Encryption Standard (DES) e os algoritmos de criptografia 3DES. O PIX Firewall apoia tamanhos chaves AES dos bit 128, 192, e 256.

O cliente VPN apoia o AES como um algoritmo de criptografia que começa com liberação de Cisco VPN Client 3.6.1. O cliente VPN apoia tamanhos chaves dos bit 128 e dos bit 256 somente.

Pré-requisitos

Requisitos

Esta configuração de exemplo supõe que o PIX é plenamente operacional e configurado com os comandos necessários a fim segurar o tráfego conforme a política de segurança da organização.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software PIX Versão 6.3(1)**Nota:** Esta instalação foi testada no PIX Software Release 6.3(1) e é esperada trabalhar em tudo mais tarde liberações.
- Versão Cliente VPN Cisco 4.0.3(A)**Nota:** Esta instalação foi testada na versão 4.0.3(A) mas nos trabalhos do cliente VPN em versões anterior de volta a 3.6.1 e até a versão atual.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Os VPNs de Acesso Remoto atendem ao requisito de força de trabalho móvel para conectar com segurança a rede da organização. Os usuários móveis podem estabelecer uma conexão segura usando o software do cliente VPN instalado em seus PC. O cliente VPN inicia uma conexão a um dispositivo da instalação central configurado para aceitar estes pedidos. Neste exemplo, o dispositivo da instalação central é um PIX Firewall configurado como um Easy VPN Server que usa mapas cripto dinâmico.

O Cisco Easy VPN simplifica a distribuição VPN fazendo a configuração e o Gerenciamento dos VPN fáceis. Consiste no server do Cisco Easy VPN e no telecontrole do Cisco Easy VPN. A configuração mínima é exigida no Easy VPN Remote. O Easy VPN Remote inicia uma conexão. Se a autenticação é bem sucedida, o Easy VPN Server abaixa-lhe a configuração de VPN para. Mais informação em como configurar um PIX Firewall como um Easy VPN Server está disponível em controlar o Acesso remoto VPN.

Os mapas cripto dinâmico são usados para a configuração IPSec quando alguns parâmetros exigidos para estabelecer o VPN não podem ser predeterminados, como é o caso com os usuários móveis que obtêm dinamicamente endereços IP atribuídos. O mapa cripto dinâmico atua como um molde e os parâmetros faltantes são determinados durante a negociação de IPSec. Mais informações sobre mapas de criptografia dinâmicos estão disponíveis em Mapas de Criptografia Dinâmicos.

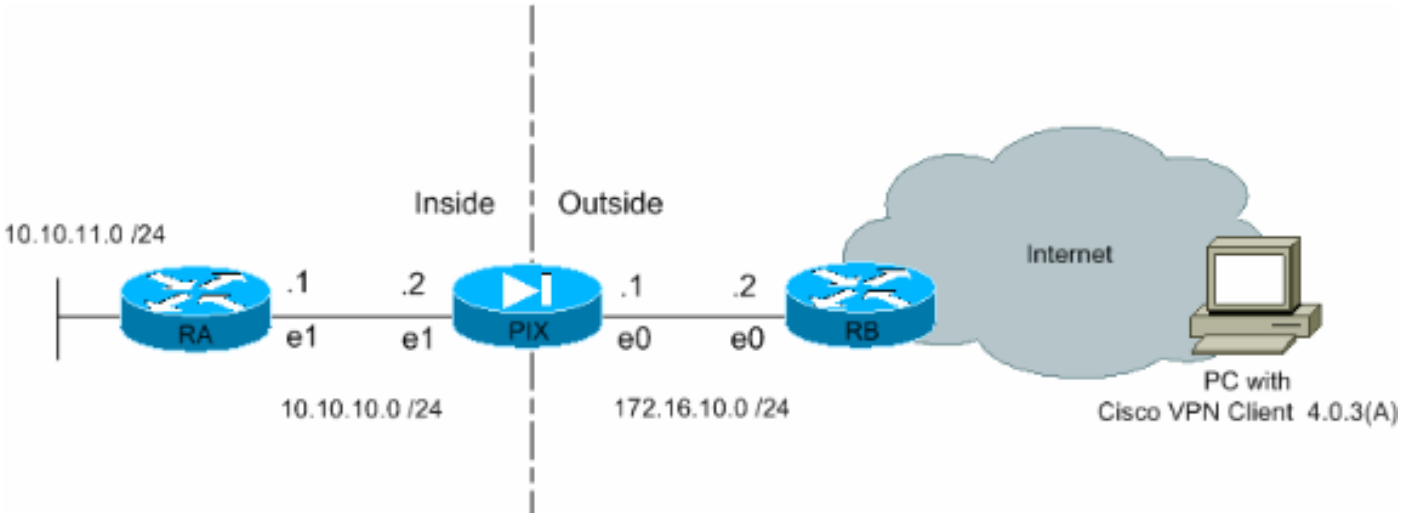
Configurações

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configure o PIX

A configuração necessária no PIX Firewall é mostrada nesta saída. A configuração é para o VPN somente.

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
```

Nota: Nesta instalação, recomenda-se que você não especificar o aes-192 quando você configurar o grupo da transformação ou a política de ISAKMP. Os clientes VPN não apoiam o aes-192 para a criptografia.

Nota: Com versões anterior, os comandos isakmp client configuration address-pool e crypto map client-configuration address da configuração de modo IKE foram exigidos. Entretanto, com

versões mais novas (3.x e mais recente), esses comandos não são mais necessários. Agora, é possível especificar vários conjuntos de endereços usando o comando vpngroup address-pool.

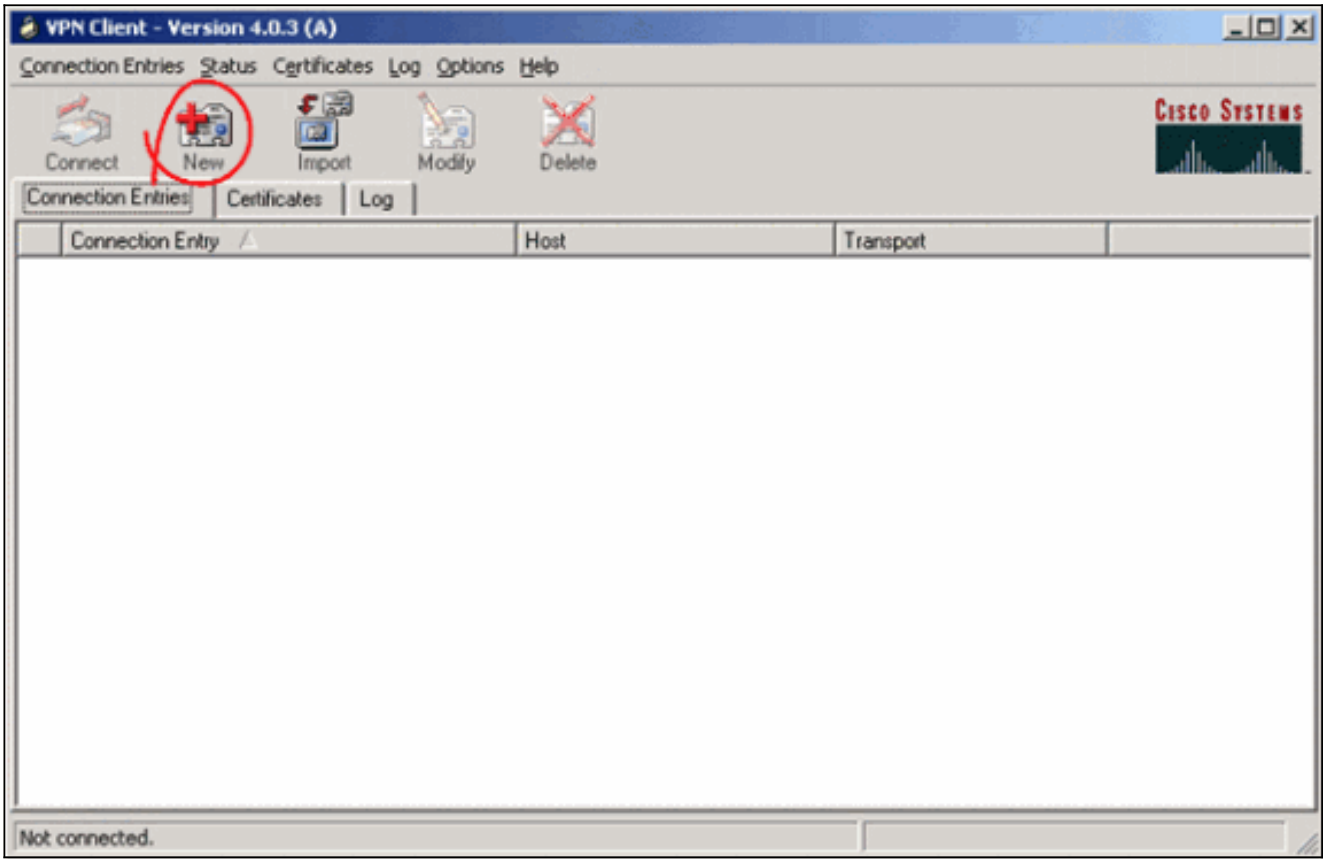
Nota: Os nomes do grupo VPN são diferenciando maiúsculas e minúsculas. Isto significa que a autenticação de usuário falha se o nome do grupo especificado no PIX e o nome do grupo no cliente VPN são diferentes em termos do caso de letra (parte superior ou caixa baixa).

Nota: Por exemplo, quando você dá entrada com o nome do grupo como **GroupMarketing em** um dispositivo e **groupmarketing em um** outro dispositivo, o dispositivo não funciona.

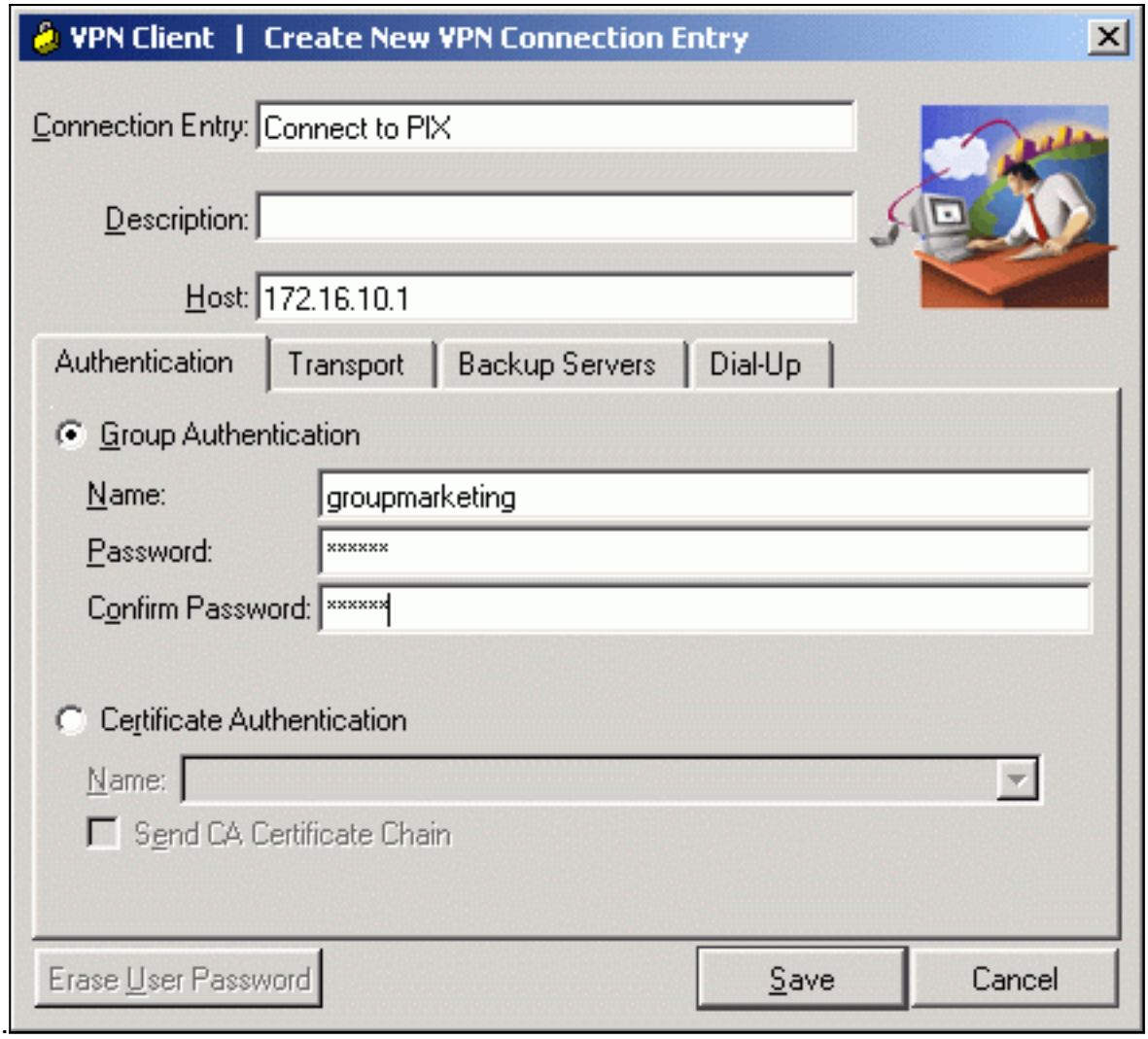
Configurar o VPN Client

Depois que você instala o cliente VPN no PC, crie uma nova conexão segundo as indicações destas etapas:

1. Inicie o aplicativo VPN Client e clique em Novo para criar uma nova entrada de conexão.

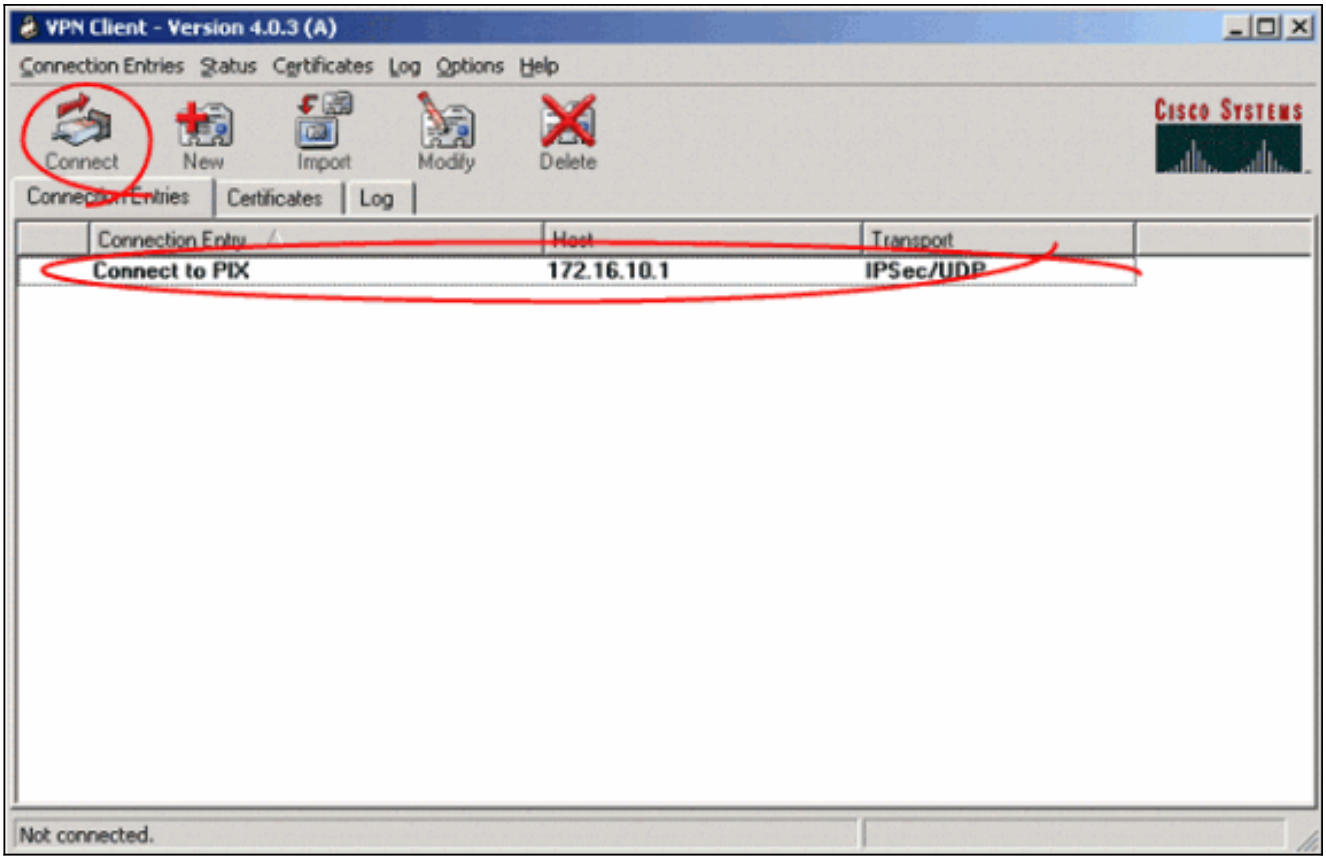


2. Uma caixa de diálogo nova intitulou o cliente VPN | Crie a entrada nova da conexão de VPN aparece. Insira as informações de configuração para a nova conexão.No campo de entrada de conexão, atribua um nome à entrada nova que é criada.No campo Host, digite o endereço IP da interface pública do PIX.Selecione a aba da autenticação, e datilografe então o nome do grupo e a senha (duas vezes - para a confirmação). Isto precisa de combinar a informação incorporada no PIX usando o **comando vpngroup password**.Clique em Save para salvar as informações inseridas. A nova conexão é criada



agora.

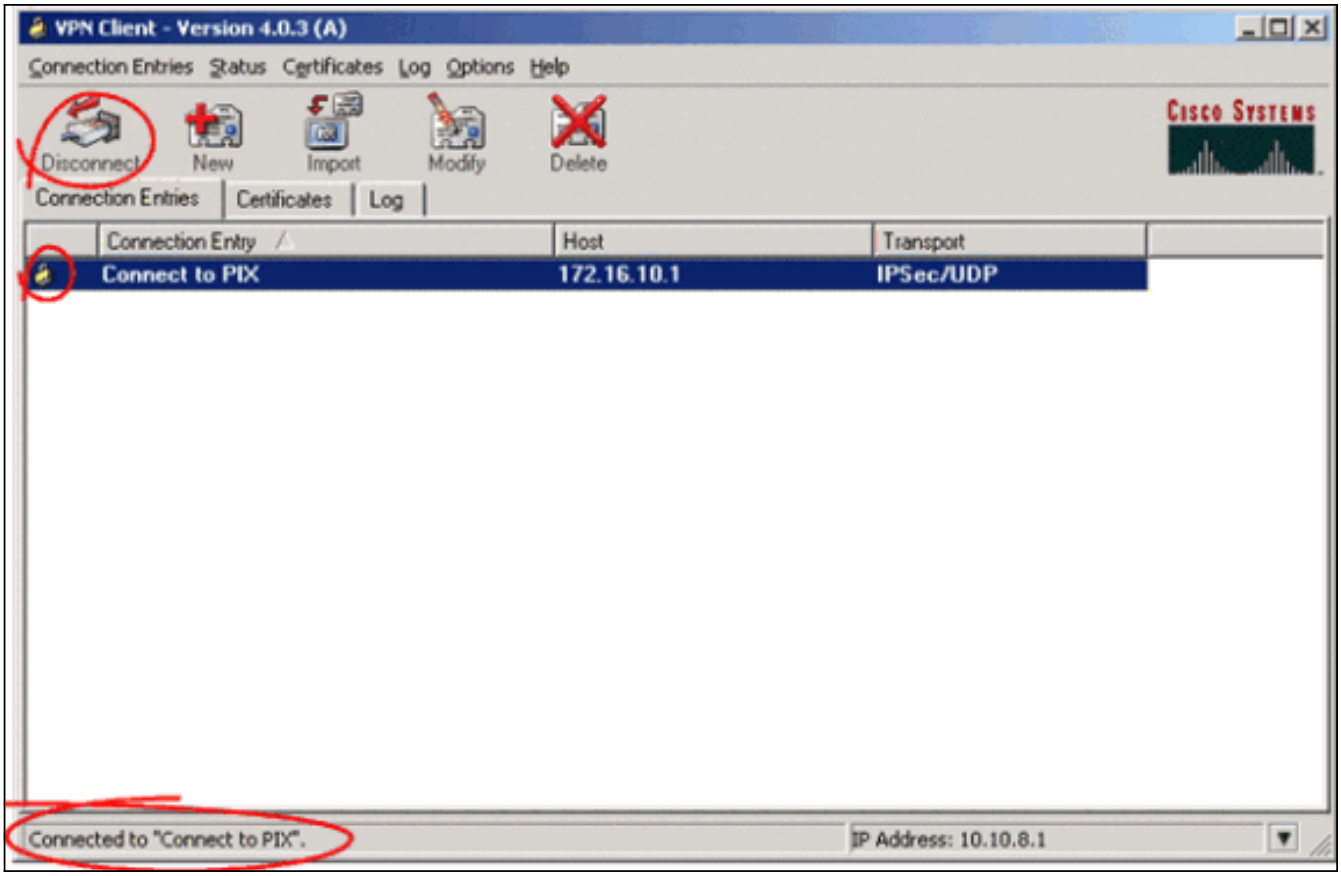
3. A fim conectar ao gateway usando a entrada da nova conexão, selecione a entrada de conexão clicando sobre a uma vez e clique então o ícone da **conexão**. Um duplo-clique na entrada da conexão tem o mesmo
efeito.



Verificar

No cliente VPN, uma conexão estabelecida ao gateway remoto é indicada com sucesso por estes artigos:

- Um ícone de cadeado fechado amarelo aparece na entrada de conexão ativa.
- O ícone da conexão na barra de ferramentas (ao lado da aba das entradas de conexão) muda para desligar.
- A linha de status na extremidade do indicador mostra o estado como “conectado” ao seguido pelo nome de entrada de
  conexão.



Nota: Por padrão, uma vez estabelecida a conexão, o VPN Client é minimizado como ícone de cadeado fechado na bandeja do sistema, no canto inferior direito da barra de tarefas do Windows. Fazer duplo clique o ícone de bloqueio fechado a fim fazer outra vez o indicador do cliente VPN visível.

No PIX Firewall, estes **comandos show** podem ser usados para verificar o estado das conexões estabelecidas.

Nota: A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **mostre IPsec cripto sa** — Mostra todo o sas de IPSec atual no PIX. Além disso, a saída exibe o endereço IP real do peer remoto, o endereço IP atribuído, a interface e o endereço IP local e o cripto mapa aplicado.

```
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:
```

- **mostre isakmp cripto sa** — Mostra o estado ISAKMP SA construído entre pares.

```
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
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Estes comandos debug podem ajudar em problemas do Troubleshooting com a instalação VPN.

Nota: Consulte Informações Importantes sobre Comandos de Debugação antes de usar comandos **debug**.

- **isakmp do debug crypto** — Mostra ISAKMP SA que é construído e os atributos do IPsec que são negociados. Durante a negociação ISAKMP SA, o PIX pode possivelmente rejeitar diversas propostas enquanto " não aceitável " antes que aceitar um. Uma vez que ISAKMP SA é concordado, os atributos do IPsec estão negociados. Mais uma vez, diversas propostas podem possivelmente ser rejeitadas antes que uma esteja aceitado, segundo as indicações deste **resultado do debug**.

```
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.

- **IPsec do debug crypto** — Indica a informação em negociações IPsec SA.

```
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.
```

Com as configurações mostradas neste original, o cliente VPN pode conectar com sucesso à instalação central PIX usando o AES. Observa-se às vezes que embora o túnel VPN seja estabelecido com sucesso, os usuários não podem executar tarefas comuns tais como recursos de rede do sibilo, entrar ao domínio, ou consultar a vizinhança de rede. Mais informação em pesquisar defeitos tais problemas está disponível na vizinhança de rede Microsoft do Troubleshooting após ter estabelecido um túnel VPN com o Cisco VPN Client.

Informações Relacionadas

- Advanced Encryption Standard (AES)
- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)
- Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Página de suporte do PIX
- Página de Suporte do Cisco VPN Client
- Referências de comando PIX
- Suporte Técnico e Documentação - Cisco Systems