Como configurar o Cisco VPN Client para PIX com AES

Contents

Introduction

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 Cisco Secure PIX Firewall versão 6.3 e posterior, o novo padrão de criptografia internacional AES é suportado para proteger conexões VPN de site para site e de acesso remoto. Além dos algoritmos de criptografia DES (Data Encryption Standard) e 3DES. O PIX Firewall suporta tamanhos de chave AES de 128, 192 e 256 bits.

O VPN Client suporta AES como um algoritmo de criptografia iniciando com o Cisco VPN Client versão 3.6.1. O VPN Client suporta tamanhos chave de 128 bits e 256 bits apenas.

Prerequisites

Requirements

Esta configuração de exemplo pressupõe que o PIX está totalmente operacional e configurado com os comandos necessários para tratar o tráfego de acordo com 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)**Observação:** essa configuração foi testada no software PIX versão 6.3(1) e deve funcionar em todas as versões posteriores.
- Cisco VPN Client versão 4.0.3(A)**Observação:** essa configuração foi testada no VPN Client versão 4.0.3(A), mas funciona em versões anteriores de volta à 3.6.1 e até a versão atual.

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

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 configurar uma conexão segura usando o software VPN Client instalado em seus PCs. O VPN Client inicia uma conexão com um dispositivo de site central configurado para aceitar essas solicitações. Neste exemplo, o dispositivo do site central é um PIX Firewall configurado como um servidor Easy VPN que usa mapas de criptografia dinâmicos.

O Cisco Easy VPN simplifica a implantação de VPN, facilitando a configuração e o gerenciamento de VPNs. Consiste no Cisco Easy VPN Server e no Cisco Easy VPN Remote. É necessária uma configuração mínima no Easy VPN Remote. O Easy VPN Remote inicia uma conexão. Se a autenticação for bem-sucedida, o Easy VPN Server envia a configuração da VPN para ele. Mais informações sobre como configurar um PIX Firewall como um servidor Easy VPN estão disponíveis em Managing VPN Remote Access.

Os mapas de criptografia dinâmicos são usados para a configuração de IPsec quando alguns parâmetros necessários para configurar a VPN não podem ser predeterminados, como é o caso dos usuários móveis que obtêm endereços IP atribuídos dinamicamente. O mapa de criptografia dinâmico atua como um modelo e os parâmetros ausentes são determinados durante a negociação de IPsec. Mais informações sobre mapas de criptografia dinâmicos estão disponíveis em Mapas de Criptografia Dinâmicos.

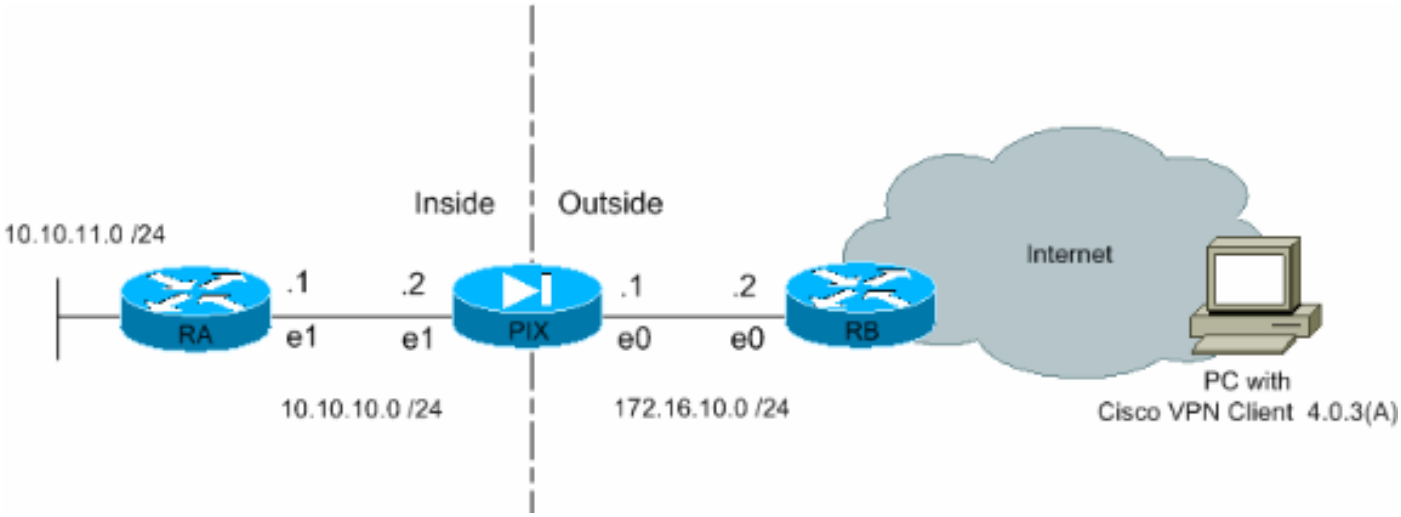
Configurações

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 somente para 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
```

Observação: nesta configuração, é recomendável não especificar aes-192 enquanto você configura o conjunto de transformação ou a política ISAKMP. Os VPN Clients não suportam aes-192 para criptografia.

Observação: com versões anteriores, os comandos IKE Mode Configuration **isakmp client configuration address-pool** e **crypto map client-configuration address** eram necessários.

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.

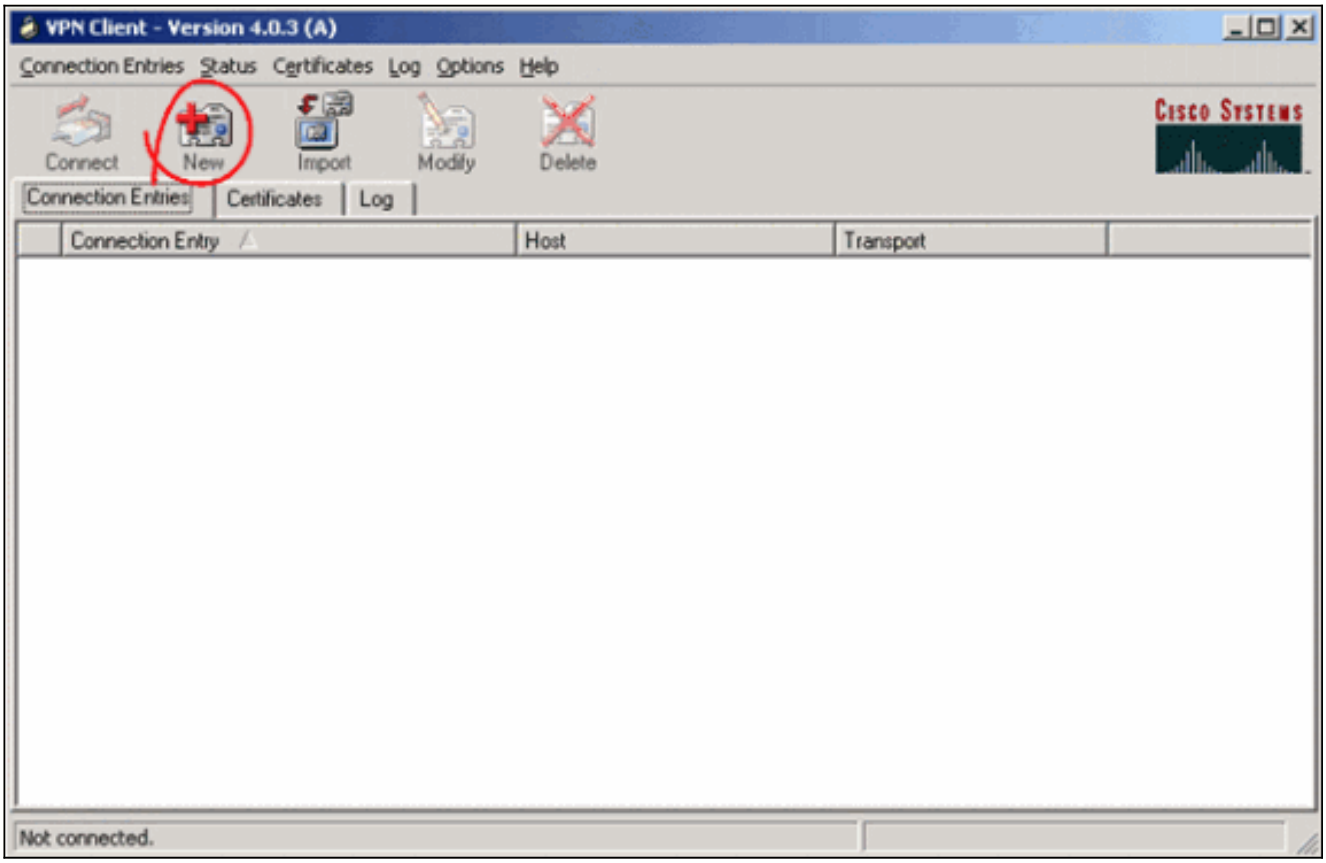
Observação: os nomes dos grupos de VPNs diferenciam maiúsculas e minúsculas. Isso significa que a autenticação do usuário falha se o nome do grupo especificado no PIX e o nome do grupo no VPN Client forem diferentes em termos de letras maiúsculas ou minúsculas.

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

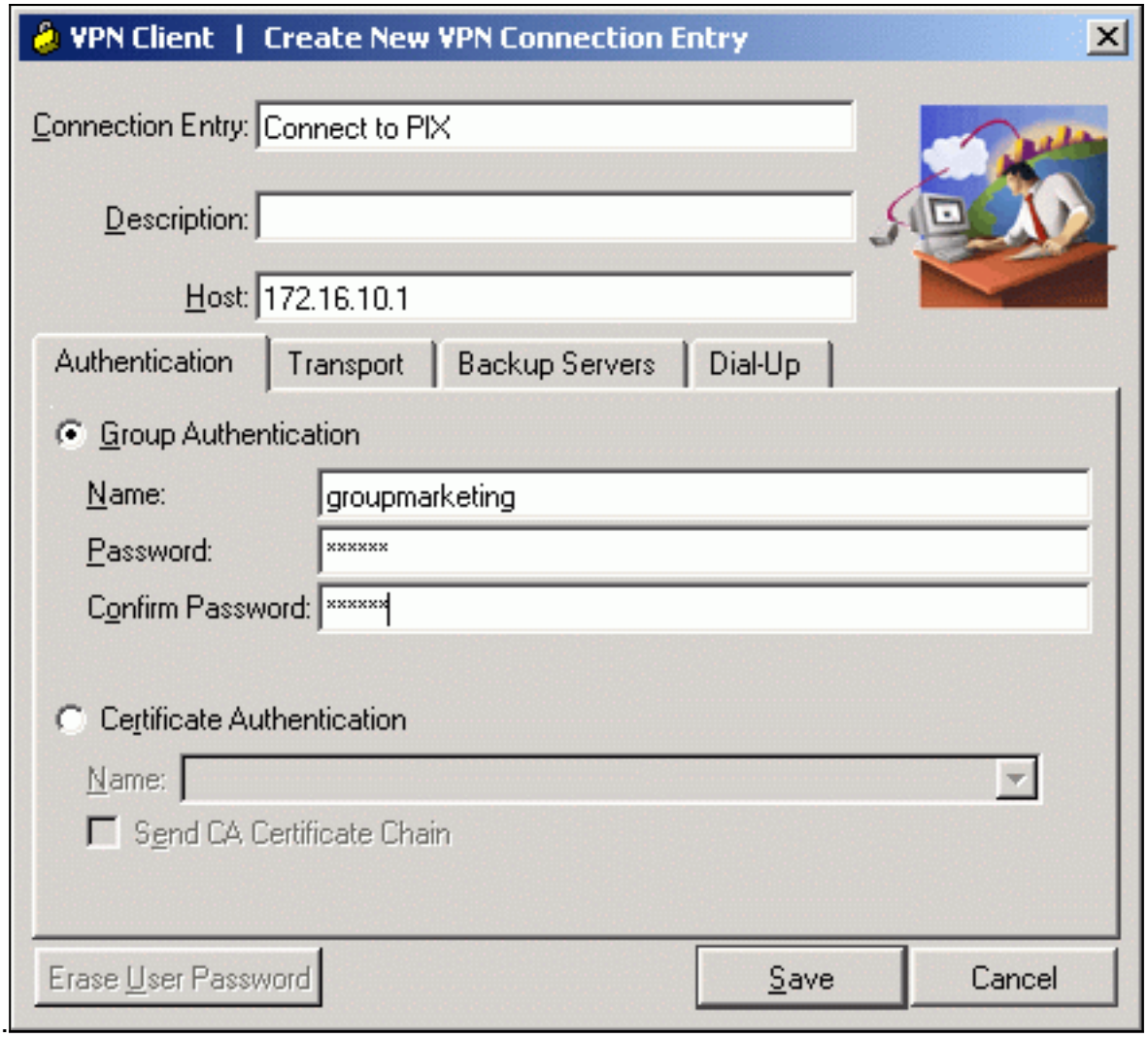
Configurar o VPN Client

Depois de instalar o VPN Client no PC, crie uma nova conexão conforme mostrado nas seguintes etapas:

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

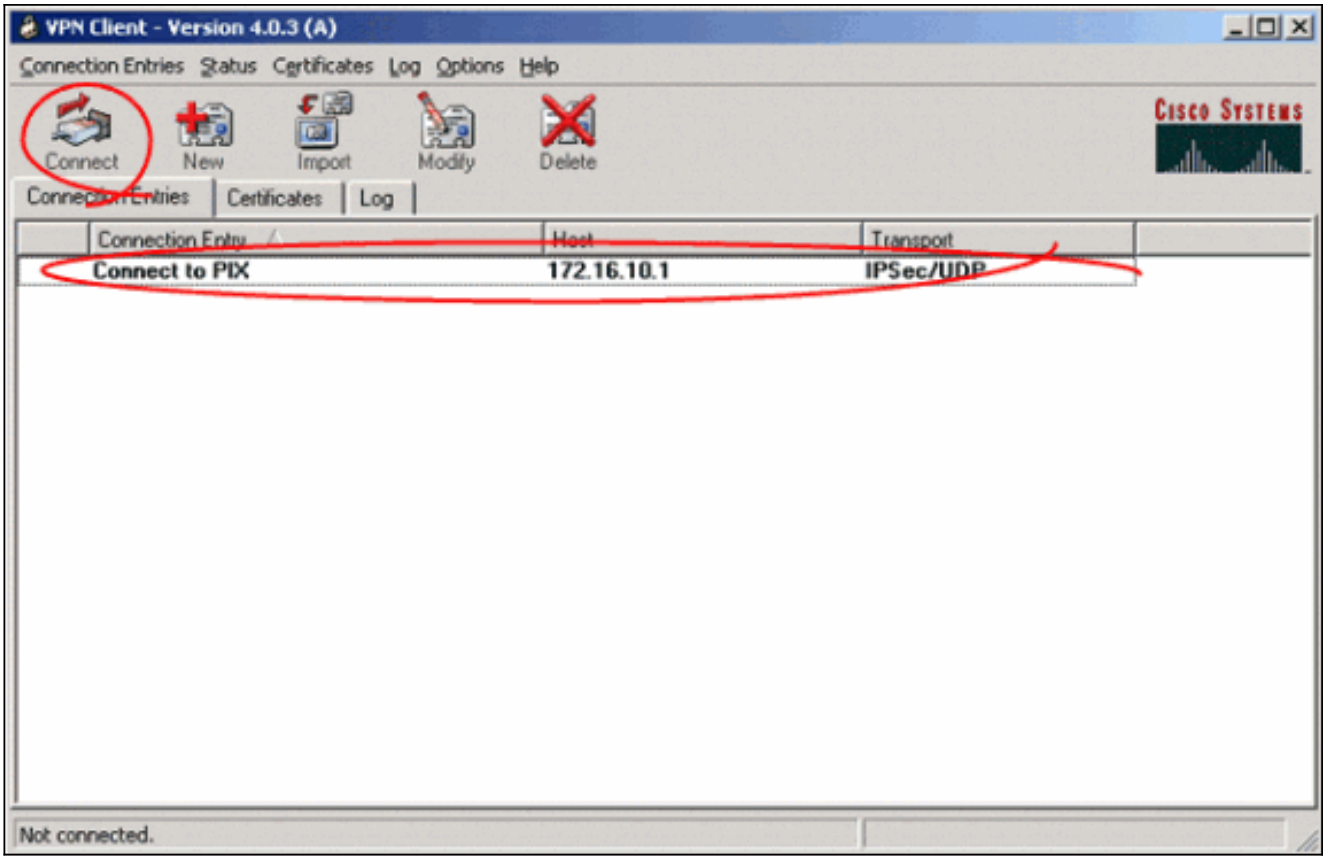


2. Uma nova caixa de diálogo intitulada Cliente VPN | Create New VPN Connection Entry (Criar nova entrada de conexão VPN) é exibido. Insira as informações de configuração para a nova conexão.No campo Entrada de conexão, atribua um nome à nova entrada criada.No campo Host, digite o endereço IP da interface pública do PIX.Selecione a guia Autenticação e digite o nome do grupo e a senha (duas vezes - para confirmação). Isso precisa corresponder às informações inseridas no PIX usando o comando **vpngroup password**.Clique em Save para salvar as informações inseridas. A nova conexão foi criada



agora.

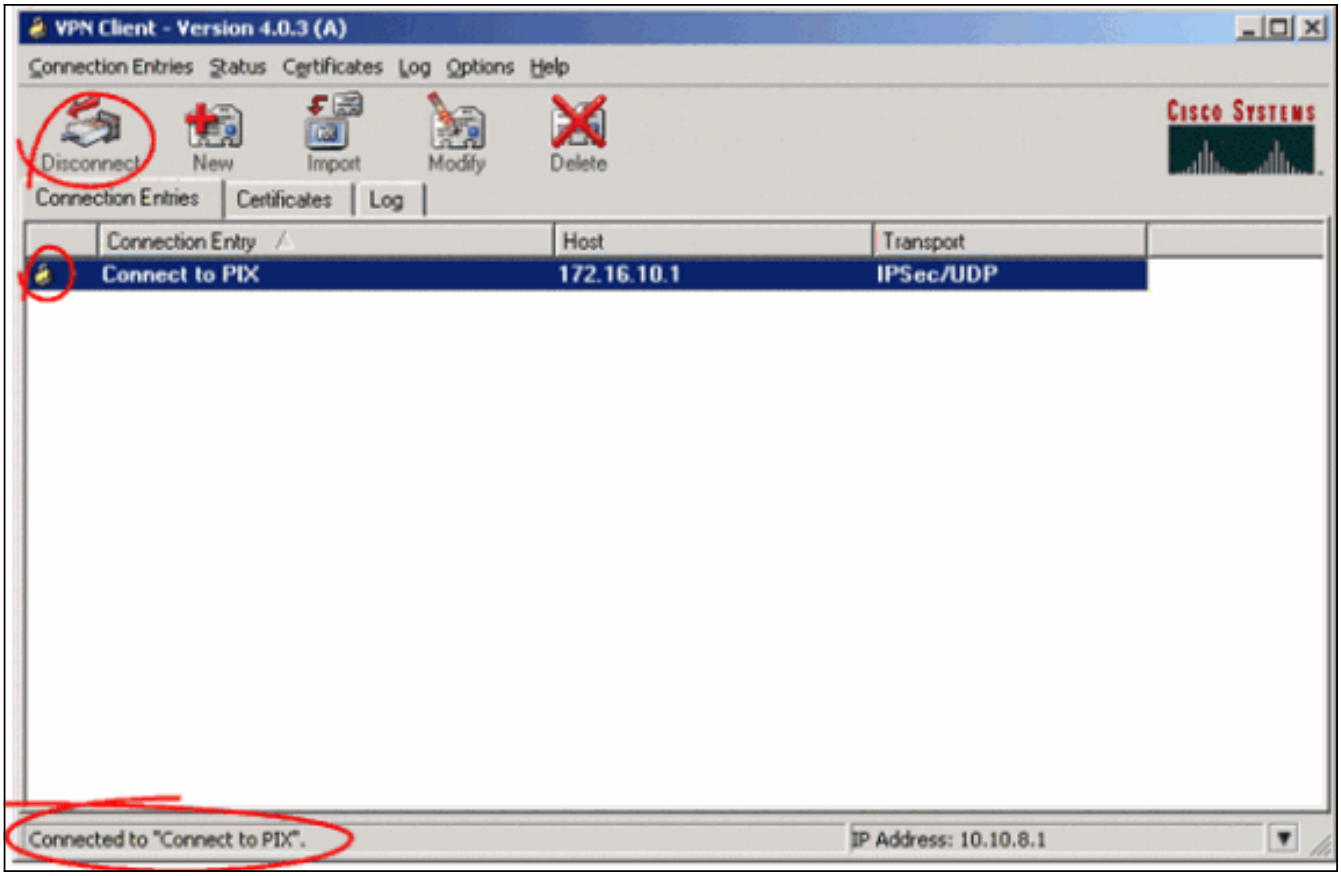
3. Para se conectar ao gateway usando a nova entrada de conexão, selecione a entrada de conexão clicando uma vez nele e clique no ícone **Connect**. Um duplo-clique na entrada da conexão tem o mesmo
efeito.



Verificar

No VPN Client, uma conexão estabelecida com êxito com o gateway remoto é indicada por estes itens:

- Um ícone de cadeado fechado amarelo aparece na entrada de conexão ativa.
- O ícone Conectar na barra de ferramentas (ao lado da guia Entradas de conexão) é alterado para Desconectar.
- A linha de status no final da janela mostra o status como "Conectado" seguido do nome da entrada da
  conexão.



Observação: por padrão, depois que a conexão é estabelecida, o VPN Client é minimizado para um ícone de cadeado fechado na bandeja do sistema, no canto inferior direito da barra de tarefas do Windows. Clique duas vezes no ícone de bloqueio para tornar a janela do VPN Client visível novamente.

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

Observação: determinados comandos **show** são suportados pela Output Interpreter Tool (somente clientes registrados) , que permite exibir uma análise da saída do comando **show**.

- **show crypto ipsec sa** — Mostra todas as SAs IPsec atuais 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:
```

- **show crypto isakmp sa** — Mostra o status da SA ISAKMP criada 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
```

Troubleshoot

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

Esses comandos debug podem auxiliar na solução de problemas com a configuração da VPN.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos debug.

- **debug crypto isakmp** — Mostra a SA ISAKMP criada e os atributos IPsec negociados. Durante a negociação SA do ISAKMP, o PIX pode descartar várias propostas como "não aceitável" antes de aceitá-las. Após o acordo sobre o ISAKMP SA, os atributos de IPSec serão negociados. Mais uma vez, várias propostas podem ser rejeitadas antes que uma seja aceita, como mostrado nesta saída **de depuração**.

```
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** — Exibe informações sobre as negociações SA do 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
```

Com as configurações mostradas neste documento, o VPN Client pode se conectar com êxito ao PIX do site central usando AES. Às vezes, observa-se que, embora o túnel VPN seja estabelecido com êxito, os usuários não podem executar tarefas comuns, como ping de recursos de rede, logon no domínio ou navegar na vizinhança da rede. Mais informações sobre a solução de problemas desse tipo estão disponíveis na Solução de problemas de vizinhança de rede da Microsoft após estabelecer 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