Hoe de Cisco VPN-client instellen op PIX met AES

Inhoud

Inleiding

Deze voorbeeldconfiguratie toont hoe u een externe VPN-verbinding van een Cisco VPN-client naar een PIX-firewall kunt instellen met Advanced Encryption Standard (AES) voor encryptie. Dit voorbeeld gebruikt Cisco Easy VPN om het beveiligde kanaal in te stellen en de PIX-firewall wordt ingesteld als een Easy VPN-server.

In Cisco Secure PIX-softwarerelease 6.3 en hoger wordt de nieuwe internationale coderingsstandaard AES ondersteund voor het beveiligen van VPN-verbindingen van site-to-site en externe toegang. Dit is naast de Data Encryption Standard (DES) en 3DES-encryptie-algoritmen. De PIX Firewall ondersteunt AES sleutelformaten van 128, 192 en 256 bits.

De VPN-client ondersteunt AES als een encryptie-algoritme vanaf Cisco VPN-clientrelease 3.6.1. De VPN-client ondersteunt alleen sleutelformaten van 128 bits en 256 bits.

Voorwaarden

Vereisten

Deze voorbeeldconfiguratie gaat ervan uit dat de PIX volledig operationeel is en met de benodigde opdrachten is geconfigureerd om verkeer te verwerken volgens het beveiligingsbeleid van de organisatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-softwarerelease 6.3(1)S**N.B.:** Deze instelling is getest op PIX-softwarerelease 6.3(1) en zal naar verwachting aan alle latere releases werken.
- Cisco VPN-clientversie 4.0.3(A)**Opmerking:** Deze instelling is getest op VPN-clientversie 4.0.3(A), maar werkt op eerdere releases terug naar 3.6.1 en tot de huidige release.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Remote Access VPN's voldoen aan de vereisten van de mobiele medewerkers om zich veilig aan te sluiten op het netwerk van de organisatie. Mobiele gebruikers kunnen een beveiligde verbinding opzetten met behulp van de VPN-clientsoftware die op hun pc's is geïnstalleerd. De VPN-client initieert een verbinding met een centraal siteapparaat dat is geconfigureerd om deze verzoeken te aanvaarden. In dit voorbeeld, is het centrale plaatsapparaat een PIX Firewall die als een Makkelijk VPN server wordt geconfigureerd en dynamische crypto kaarten gebruikt.

Cisco Easy VPN vereenvoudigt de implementatie van VPN door configuratie en beheer van VPN's eenvoudig te maken. Het bestaat uit de Cisco Easy VPN Server en de Cisco Easy VPN Remote. Minimale configuratie is vereist op de Easy VPN-afstandsbediening. Met de Easy VPN-afstandsbediening wordt een verbinding gestart. Als verificatie geslaagd is, drukt de Easy VPN Server de VPN-configuratie naar beneden. Meer informatie over het configureren van een PIX-firewall als een Easy VPN-server is beschikbaar bij Afstandstoegang van VPN beheren.

Dynamische crypto kaarten worden gebruikt voor de configuratie van IPsec wanneer sommige parameters die nodig zijn om het VPN in te stellen niet kunnen worden voorgeprogrammeerd, zoals het geval is met mobiele gebruikers die dynamisch toegewezen IP-adressen verkrijgen. De dynamische crypto map fungeert als een sjabloon en de ontbrekende parameters worden bepaald tijdens IPsec-onderhandeling. Meer informatie over dynamische crypto kaarten is beschikbaar bij Dynamic Crypto Maps.

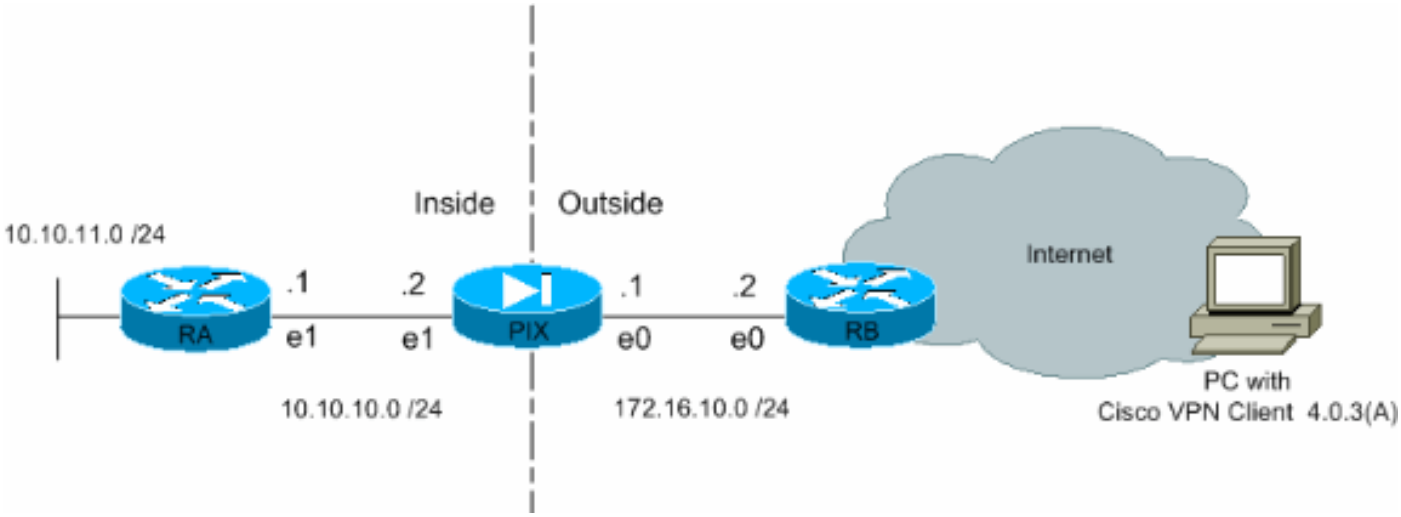
Configuraties

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



PIX configureren

De configuratie die nodig is in de PIX-firewall wordt in deze uitvoer weergegeven. De configuratie is alleen voor 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
```

Opmerking: In deze instelling wordt aangeraden om geen es-192 op te geven terwijl u de transformatie of het ISAKMP-beleid instelt. VPN-clients ondersteunen AES-192 niet voor codering.

Opmerking: Bij eerdere versies waren de opdrachten voor de configuratie van de IKE-modus **nodig**, **zoals de configuratie van de client** en **het adres voor de configuratie van de client**. Maar met nieuwere versies (3.x en hoger) zijn deze opdrachten niet langer nodig. Meervoudige

adrespools kunnen nu worden gespecificeerd met de opdracht **Adres-pool van vpngroup**.

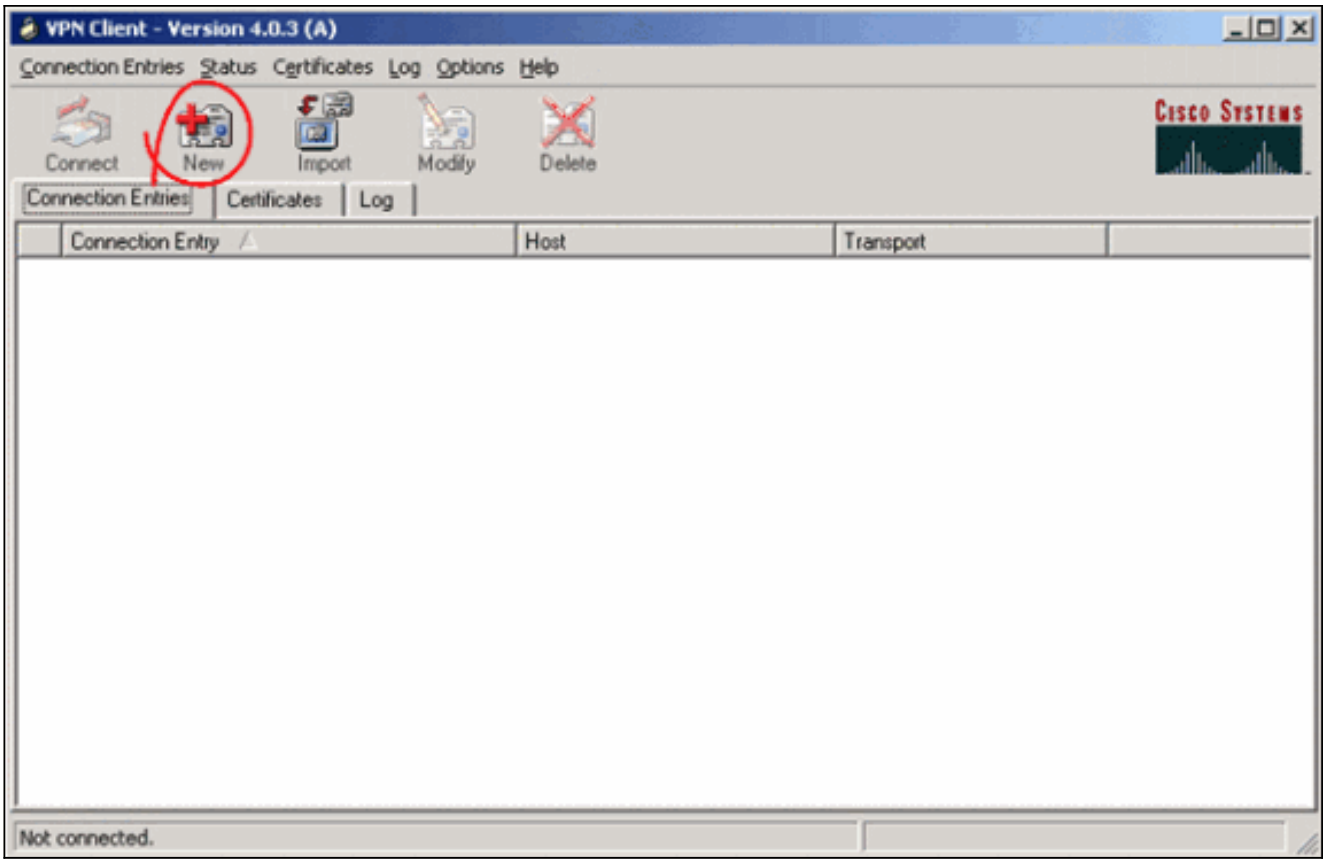
Opmerking: VPN-groepsnamen zijn hoofdlettergevoelig. Dit betekent dat gebruikersverificatie mislukt als de groepsnaam die in de PIX gespecificeerd is en de groepsnaam op de VPN-client verschillend is in termen van letters (hoofdletters of kleine letters).

Opmerking: Wanneer u bijvoorbeeld de groepsnaam als **GroupMarketing** in één apparaat invoert en **groupmarketing** in een ander apparaat, werkt het apparaat niet.

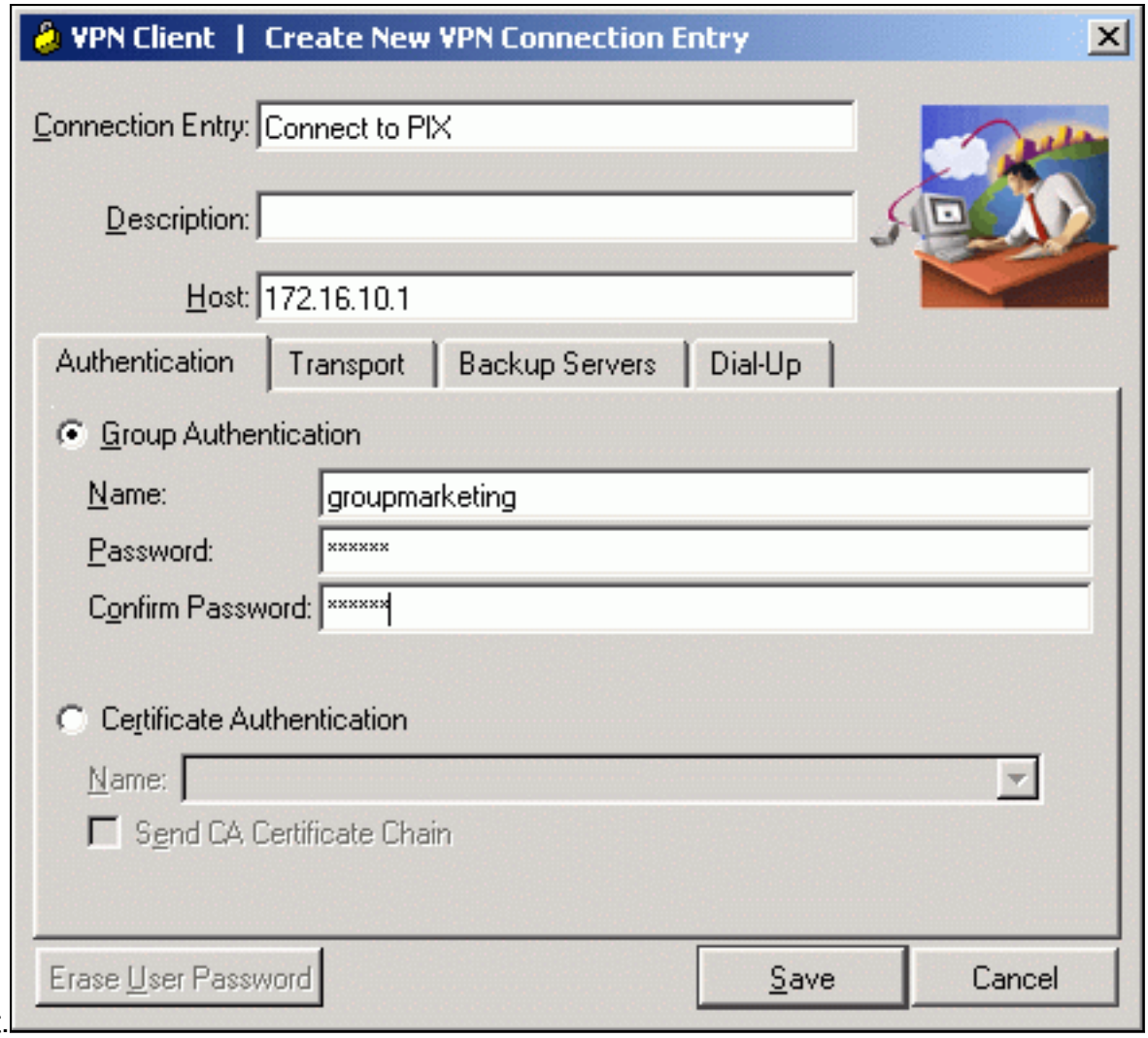
VPN-client configureren

Nadat u de VPN-client op de pc hebt geïnstalleerd, maakt u een nieuwe verbinding zoals in deze stappen:

1. Start de VPN-clienttoepassing en klik op **Nieuw** om een nieuwe verbinding te maken.

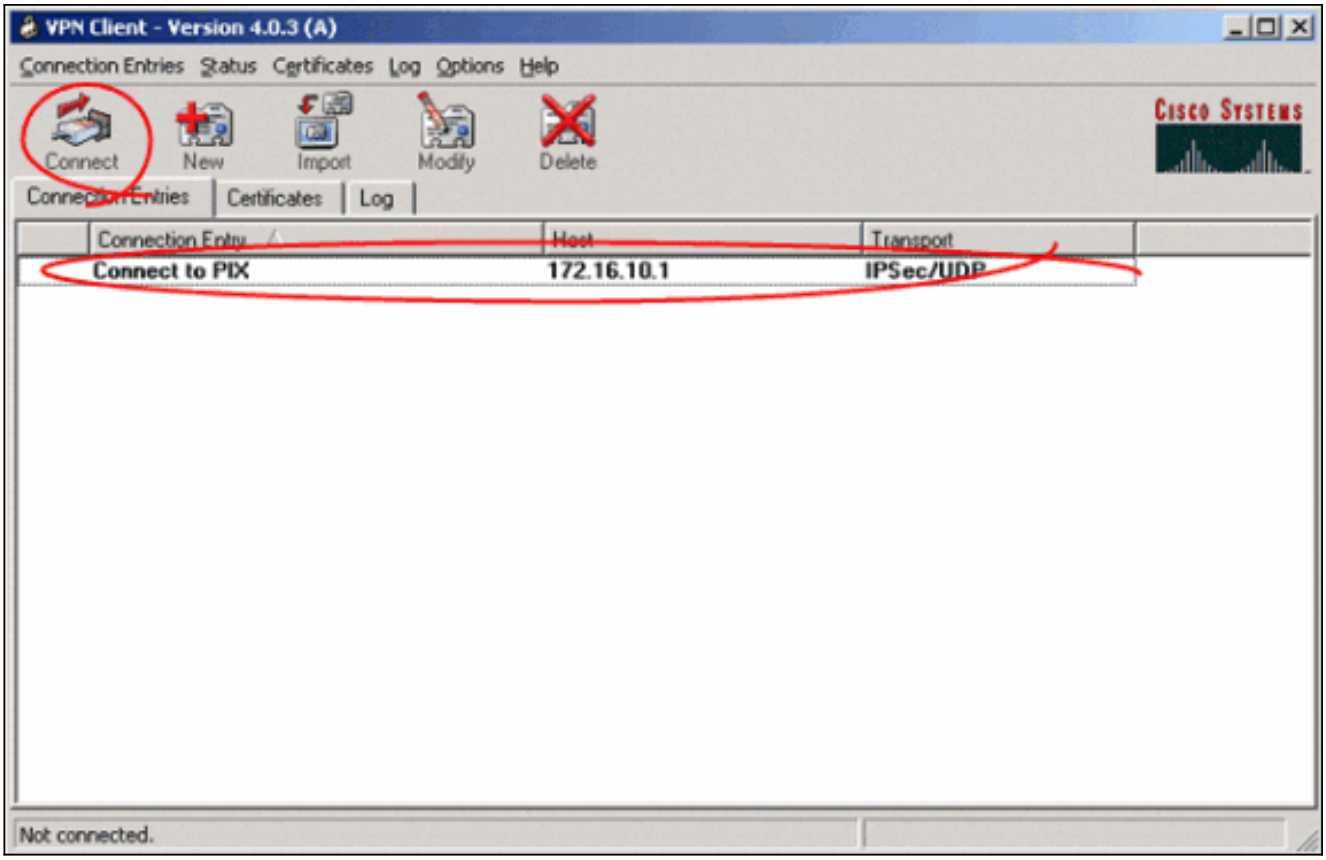


2. Een nieuw dialoogvenster met de naam VPN-client | Nieuwe VPN-verbinding maken verschijnt. Geef configuratieinformatie op voor de nieuwe verbinding.Wijzig in het veld Toegang van de verbinding een naam aan de nieuwe ingang toe die wordt gemaakt.Typ in het veld Host het IP-adres van de openbare interface van de PIX.Selecteer het tabblad Verificatie en type vervolgens de groepsnaam en het wachtwoord (twee keer - voor bevestiging). Dit moet overeenkomen met de informatie die in de PIX is ingevoerd met behulp van de opdracht **Wachtwoord** voor **vpngroup**.Klik op **Opslaan** om de ingevoerde informatie op te slaan. De nieuwe verbinding wordt nu



gemaakt.

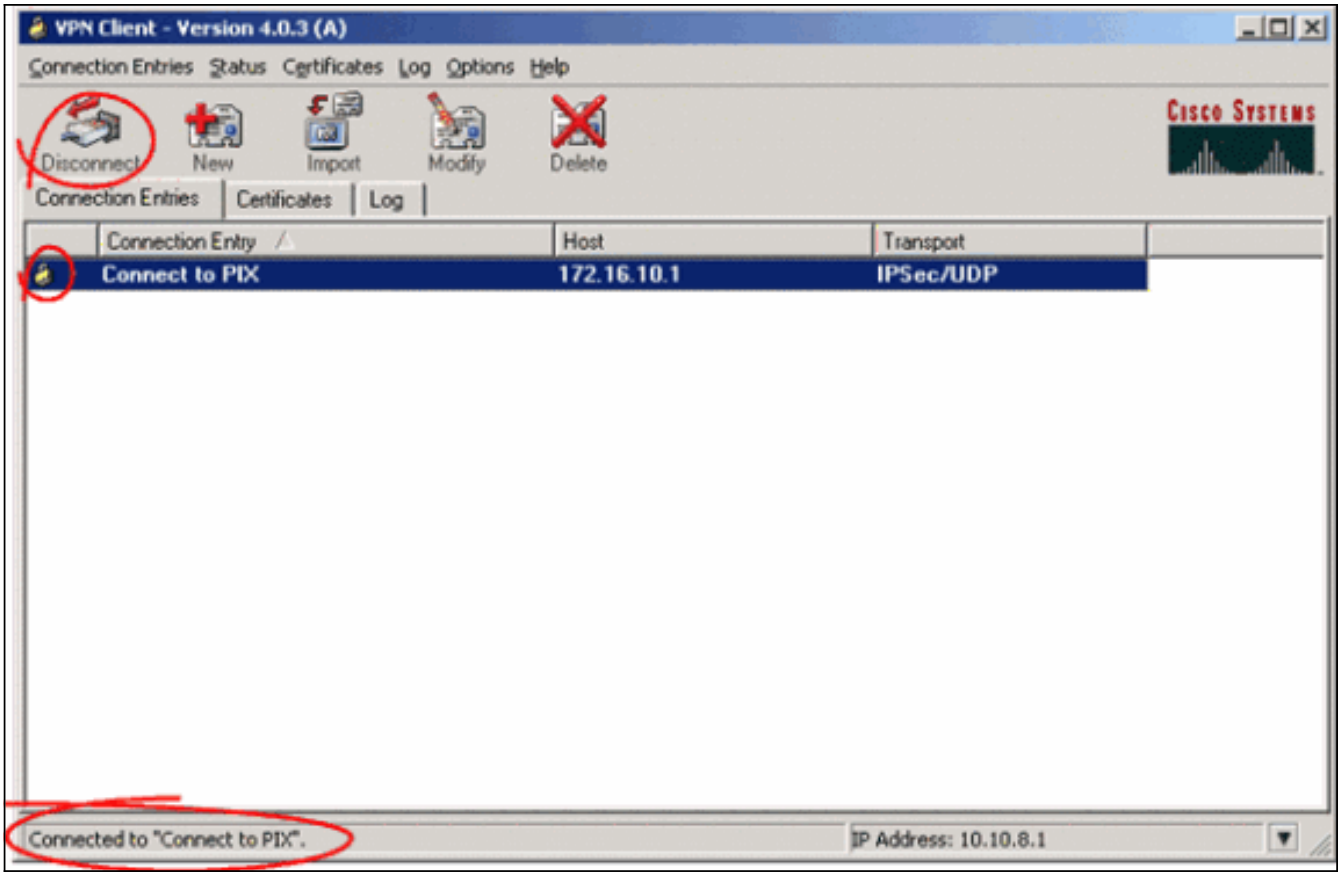
3. Als u met de nieuwe ingang van de verbinding naar de poort wilt verbinden, selecteert u de ingang van de verbinding door er eenmaal op te klikken en vervolgens op het pictogram **Connect** te klikken. Een dubbelklik op de verbindingsingang heeft hetzelfde effect.



Verifiëren

Op de VPN-client wordt een verbinding naar de externe gateway aangemaakt die met succes is ingesteld:

- Er verschijnt een geel pictogram voor een gesloten slot tegen de actieve verbinding.
- Het pictogram Connect in de werkbalk (naast het tabblad Connection Entries) verandert in Koppelen.
- De statusregel aan het eind van het venster toont de status als "Verbonden met" gevolgd door de naam van de verbindingsingang.



N.B.: standaard minimaliseert de VPN-client, zodra de verbinding is gemaakt, tot een pictogram van gesloten vergrendeling in het systeemvak, in de rechterbenedenhoek van de taakbalk van Windows. Dubbelklik op het pictogram van de gesloten vergrendeling om het VPN-clientvenster opnieuw zichtbaar te maken.

In de PIX Firewall kunnen deze opdrachten worden gebruikt om de status van de ingestelde verbindingen te controleren.

N.B.: Bepaalde **show** opdrachten worden ondersteund door de Output Tolk Tool (alleen geregistreerde klanten), waardoor u een analyse van **show** opdrachtoutput kunt bekijken.

- **tonen crypto ipsec sa**-Toont alle huidige IPsec SAs op de PIX. Daarnaast wordt het IP-adres van de externe peer, het toegewezen IP-adres, het plaatselijke IP-adres en de interface en de toegepaste crypto-map weergegeven.

```
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:
```

- **toon crypto isakmp sa** - toont de status van ISAKMP SA gebouwd tussen peers.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Deze debug opdrachten kunnen helpen bij het oplossen van problemen met de VPN-instellingen.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten afgeeft.

- **debug van crypto isakmp**-shows the ISAKMP SA die gebouwd is en de eigenschappen van IPsec die onderhandeld worden. Tijdens de onderhandelingen met ISAKMP SA kan de PIX verschillende voorstellen onmogelijk als "niet acceptabel" afwijzen voordat ze één aanvaarden. Zodra de ISAKMP SA is overeengekomen, worden de IPsec eigenschappen onderhandeld. En nogmaals, verschillende voorstellen kunnen mogelijk worden verworpen voordat ze worden aanvaard, zoals wordt aangetoond in deze **debug-**productie.

```
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 van crypto ipsec**-displays bij IPsec SA-onderhandelingen.

```
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
```

Dankzij de configuraties in dit document kan de VPN-client met succes verbinding maken met de centrale site PIX met AES. Het wordt soms waargenomen dat, alhoewel de VPN-tunnel succesvol is ingesteld, gebruikers geen gemeenschappelijke taken kunnen uitvoeren zoals het ping van netwerkbronnen, het inschakelen van het domein of het bladeren van netwerkbuurten. Meer informatie over het oplossen van dergelijke problemen is beschikbaar in de netwerkbuurt van Microsoft Network na het instellen van een VPN-tunnelband met de Cisco VPN-client.

Gerelateerde informatie

- Advanced Encryption Standard (AES)
- Een Inleiding aan IP Security (IPSec) encryptie
- IP-beveiligingsprobleemoplossing - Oplossingen begrijpen en gebruiken van debug-opdrachten
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- PIX-ondersteuningspagina
- Cisco VPN-clientondersteuningspagina
- PIX-opdracht
- Technische ondersteuning en documentatie – Cisco Systems