Begrijp en gebruik debug commando's om IPsec problemen op te lossen

Inhoud

Inleiding

Dit document beschrijft gezamenlijke debugopdrachten voor het oplossen van IPsec-problemen op zowel de Cisco IOS®software als PIX/ASA.

Achtergrondinformatie

Raadpleeg de oplossingen voor probleemoplossing van meest gebruikelijke L2L- en externe IPsec VPN-toegang voor informatie over de meest gebruikelijke oplossingen voor IPsec VPN-problemen.

Het bevat een controlelijst van gebruikelijke procedures die u kunt proberen voordat u een verbinding kunt oplossen en technische ondersteuning van Cisco kunt bellen.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat u IPsec hebt geconfigureerd. Raadpleeg IPsec-onderhandeling/IKE-protocollen voor meer informatie.

Gebruikte componenten

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

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

- **Cisco IOS®-software**IPsec-functieset.56i—Geeft één signaal aan **Data Encryption Standard (DES)** functie (op Cisco IOS®-softwarerelease 11.2 en hoger).k2—Geeft drie DES-functies aan (op Cisco IOS®-softwarerelease 12.0 en hoger). Triple-DES is beschikbaar op Cisco 2600 Series en hoger.
- **PIX**—V5.0 en hoger, waarvoor een enkele of drievoudige DES-licentiesleutel nodig is om te kunnen activeren.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Cisco IOS®-softwaredebugs

De onderwerpen in deze sectie beschrijven de debug-opdrachten voor Cisco IOS®-software. Raadpleeg IPsec-onderhandeling/IKE-protocollen voor meer informatie.

show crypto isakmp sa

Deze opdracht toont de **Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)** gebouwd tussen peers.

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

crypto ipsec tonen

Deze opdracht toont IPsec SA's die tussen peers zijn gebouwd. De versleutelde tunnel is gebouwd tussen 10.1.0.1 en 10.1.0.2 voor verkeer dat tussen netwerken 10.1.0.0 en 10.1.1.0 loopt.

Je ziet de twee **Encapsulating Security Payload (ESP)** SA's inkomende en uitgaande gebouwd. De Kop van de authentificatie (AH) wordt niet gebruikt aangezien er geen AH SAs zijn.

Deze output toont een voorbeeld van **show crypto ipsec sa** uit.

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 10.1.0.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
    #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound esp sas:
      spi: 0x136A010F(325714191)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4608000/52)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
inbound pcp sas:
```

```
outbound esp sas:
   spi: 0x3D3(979)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4608000/52)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

toon crypto motorverbinding actief

Deze opdracht toont elke fase 2 SA gebouwd en de hoeveelheid verkeer verzonden.

Omdat fase 2 **Security Associations (SAs)** zijn unidirectioneel, elke SA toont verkeer in slechts één richting (encrypties zijn uitgaand, decrypties zijn inbound).

debug crypto isakmp

Deze output toont een voorbeeld van **debug crypto isakmp** uit.

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
encryption DES-CBC
      hash SHA
default group 2
auth pre-share
life type in seconds
life duration (basic) of 240
atts are acceptable. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipsec

Deze opdracht toont de bron en bestemming van IPsec-tunnelendpoints. **Src_proxy** en **dest_proxy** zijn de client subnetten.

Twee **sa created** -berichten worden in elke richting met één bericht weergegeven. (Er worden vier berichten weergegeven als u ESP en AH uitvoert.)

Deze output toont een voorbeeld van **debug crypto ipsec** uit.

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
```

```
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.2, dest= 10.1.0.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Voorbeeldfoutmeldingen

Deze voorbeelden van foutmeldingen werden gegenereerd uit de hier genoemde **debug**-opdrachten:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

Replay-controle is mislukt

Deze output toont een voorbeeld van **Replay Check Failed** fout:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

Deze fout is het resultaat van een herschikking in transmissiemedia (vooral als er parallelle paden bestaan) of ongelijke paden van pakket die binnen Cisco IOS® worden verwerkt voor grote versus kleine pakketten plus onder belasting.

Verander de transformatie-reeks om dit weer te geven. Het **reply check** wordt alleen gezien als **transform-set esp-md5-hmac** is ingeschakeld. Schakel deze foutmelding uit om deze te surfen **esp-md5-hmac** en alleen versleutelen.

Raadpleeg de Cisco-bug IDCdp19680 (alleen geregistreerde klanten).

QM FSM-fout

De IPsec L2L VPN-tunnel komt niet op de PIX-firewall of ASA en de QM FSM-foutmelding wordt weergegeven.

Een mogelijke reden zijn de proxy-identiteiten, zoals ongewoon verkeer, **Access Control List (ACL),** of crypto ACL, niet op beide einden aanpassen.

Controleer de configuratie op beide apparaten en zorg ervoor dat de crypto ACL's overeenkomen.

Een andere mogelijke oorzaak is een wanverhouding van de transformatie vastgestelde parameters. Controleer dat aan beide uiteinden VPN-gateways dezelfde transformatie gebruiken die is ingesteld met exact dezelfde parameters.

Ongeldig lokaal adres

Deze output toont een voorbeeld van de foutmelding:

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

Deze foutmelding wordt toegeschreven aan een van de twee veelvoorkomende problemen:

- Het **crypto map map-name local-address interface-id** het bevel veroorzaakt de router om een onjuist adres als identiteit te gebruiken omdat het de router dwingt om een gespecificeerd adres te gebruiken.
- **Crypto map** wordt toegepast op de verkeerde interface of helemaal niet toegepast. Controleer de configuratie om er zeker van te zijn dat de crypto-kaart wordt toegepast op de juiste interface.

IKE-bericht van X.X.X.X is niet gecontroleerd of is beschadigd

Deze **debug-**fout verschijnt als de vooraf gedeelde toetsen op de peers niet overeenkomen. Om dit probleem op te lossen, controleert u aan beide zijden de vooraf gedeelde toetsen.

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

Proces van hoofdmodus mislukt met peer

Dit is een voorbeeld van **Main Mode** (Het stuurprogramma van de VPN-client heeft een fout aangetroffen.) getoond. Het falen van de hoofdmodus duidt erop dat het beleid van fase 1 niet aan beide zijden overeenkomt.

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

Een opdracht **show crypto isakmp** toont aan dat ISAKMP SA in **MM_NO_STATE**. Dit betekent ook dat de hoofdmodus is mislukt.

```
dst      src        state     conn-id     slot
10.1.1.2  10.1.1.1   MM_NO_STATE    1           0
```

Controleer dat het fase 1-beleid op beide peers is ingesteld en controleer of alle kenmerken overeenkomen.

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

Proxy-identiteiten niet ondersteund

Dit bericht verschijnt in debugs als de toegangslijst voor IPsec verkeer niet overeenkomt.

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

De toegangslijsten op elke peer moeten elkaar weerspiegelen (alle ingangen moeten omkeerbaar zijn). Dit voorbeeld illustreert dit punt.

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

Transformeer voorstel niet ondersteund

Dit bericht wordt weergegeven als fase 2 (IPsec) niet aan beide zijden overeenkomt. Dit komt het meest voor als er een wanverhouding of een incompatibiliteit in de transformatieset is.

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

Controleer of de ingestelde transformatie aan beide zijden overeenkomt:

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
```

```
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

Geen toetsen en geen toetsen met Remote peer

Dit bericht geeft aan dat het peer-adres dat op de router is geconfigureerd, onjuist is of is gewijzigd. Controleer of het peer-adres correct is en of het adres kan worden bereikt.

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

Peeradres X.X.X.X niet gevonden

Deze foutmelding wordt normaal weergegeven bij de **VPN 3000 Concentrator** (Het stuurprogramma van de VPN-client heeft een fout aangetroffen.) getoond **Message: No proposal chosen(14)**. Dit komt doordat de verbindingen host-to-host zijn.

De routerconfiguratie heeft de IPsec-voorstellen in een volgorde waarin het voorstel dat voor de router is gekozen, overeenkomt met de toegangslijst, maar niet met de peer.

De toegangslijst heeft een groter netwerk dat de host bevat die verkeer doorsnijdt. Om dit te verbeteren, doe het routervoorstel voor deze concentrator-aan-router verbinding eerst in lijn.

Dit maakt het mogelijk om eerst de specifieke host aan te passen.

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

IPsec-pakket heeft ongeldige SPI

Deze output is een voorbeeld van de foutmelding:

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

Het ontvangen IPsec-pakket specificeert een **Security Parameters Index (SPI)** die niet in de **Security Associations Database (SADB)**. Dit kan een tijdelijke aandoening zijn als gevolg van:

- Lichte verschillen in de veroudering van **Security Sssociations (SAs)** tussen de IPsec-peers
- De lokale CTF's zijn goedgekeurd
- Onjuiste pakketten verzonden door de IPsec-peer

Dit is mogelijk een aanval.

Aanbevolen actie: de peer erkent mogelijk niet dat de lokale SA's zijn gezuiverd. Als er een nieuwe verbinding vanaf de lokale router tot stand wordt gebracht, kunnen de twee peers

vervolgens met succes opnieuw tot stand worden gebracht.

Als het probleem zich anders gedurende een korte periode voordoet, probeert u een nieuwe verbinding tot stand te brengen of neemt u contact op met de beheerder van die peer.

IPSEC(initialize_sas): Ongeldige proxy-ID's

De fout **21:57:57: IPSEC(initialize_sas): invalid proxy IDs** geeft aan dat de ontvangen proxy-identiteit niet overeenkomt met de ingestelde proxy-identiteit volgens de toegangslijst.

Controleer de uitvoer van de **debug**-opdracht om er zeker van te zijn dat beide opdrachten overeenkomen.

In de **debug** opdrachtoutput van het voorstelverzoek komt de toegangslijst 103 permissie ip 10.1.1.0 0.0.0.255 10.1.0.0 0.0.0.25 niet overeen.

De toegangslijst is netwerkspecifiek voor het ene uiteinde en hostspecifiek voor het andere.

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

Gereserveerd niet op payload 5

Dit betekent dat de ISAKMP-toetsen niet overeenkomen. Rekey/reset om de nauwkeurigheid te garanderen.

Het aangeboden algoritme komt niet overeen met beleid

Als het ingestelde ISAKMP-beleid niet overeenkomt met het voorgestelde beleid door de externe peer, probeert de router het standaardbeleid van 65535.

Als dat ook niet overeenkomt, mislukt ISAKMP-onderhandeling.

Een gebruiker ontvangt de **Hash algorithm offered does not match policy!** of **Encryption algorithm offered does not match policy!** foutenmelding op de routers.

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Hash algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
=RouterB=
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 65535 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
```

```
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
ISAKMP (0:1): no offers accepted!
ISAKMP (0:1): phase 1 SA not acceptable!
```

HMAC-verificatie mislukt

Deze foutmelding wordt gerapporteerd wanneer de verificatie van de **Hash Message Authentication Code** IPsec-pakket. Dit gebeurt gewoonlijk wanneer het pakket op enige manier wordt beschadigd.

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

Als u af en toe deze foutmelding tegenkomt, kunt u deze negeren. Als dit echter vaker gebeurt, moet u de bron van de corruptie van het pakket onderzoeken. Dit kan te wijten zijn aan een defect in de cryptoversneller.

Remote peer reageert niet

Deze foutmelding wordt aangetroffen wanneer er een mismatch is met de transformatieset. Zorg ervoor dat de aangepaste transformatiesets op beide peers zijn geconfigureerd.

Alle IPSec SA-voorstellen onaanvaardbaar bevonden

Deze foutmelding treedt op wanneer de parameters van fase 2 IPSec niet goed zijn afgestemd op de lokale en externe locaties.

Om dit probleem op te lossen, specificeert u dezelfde parameters in de transformatieset, zodat deze overeenkomen en succesvolle VPN-instellingen worden ingesteld.

Packet-encryptie/decryptie-fout

Deze output is een voorbeeld van de foutmelding:

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

Deze foutmelding is mogelijk het gevolg van een van de volgende redenen:

- Fragmentation — Fragmented crypto pakketten zijn processwitched, wat de snel-switched pakketten dwingt om naar de VPN kaart voor de proces-switched pakketten worden verzonden.

Als genoeg snel-switched pakketten voor de processwitched pakketten worden verwerkt, wordt het ESP- of AH-volgnummer voor het processwitched pakket verouderd, en wanneer het pakket

bij de VPN-kaart aankomt, is het volgnummer buiten het replay-venster.

Dit veroorzaakt ofwel de AH of ESP volgnummer fouten (respectievelijk 4615 en 4612), afhankelijk van welke inkapseling u gebruikt.

- Vertelbare cacheingangen — Een ander voorbeeld waarin dit mogelijk zou kunnen gebeuren is wanneer een snel-switch cacheingang verbaal wordt en het eerste pakket met een cachemisk procesgeschakeld wordt.

Voorwendselen

1. Schakel elk type verificatie uit op de 3DES-transformatieset en gebruik ESP-DES/3DES. Hierdoor wordt verificatie/beveiliging tegen terugspelen effectief uitgeschakeld, waardoor pakketfouten met betrekking tot ongeordend (gemengd) IPsec-verkeer worden voorkomen **%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.**
2. Een oplossing die van toepassing is op de hier genoemde reden is het instellen van de **Maximum Transmission Unit (MTU)** grootte van inkomende stromen tot minder dan 1400 bytes. Voer deze opdracht in om de maximale grootte van de transmissie-eenheid (MTU) van inkomende stromen in te stellen op minder dan 1400 bytes:
   ```
   ip tcp adjust-mss 1300
   ```
3. Schakel de AIM-kaart uit.
4. Schakel Fast/CEF uit door de routerinterfaces in te schakelen. Om snelle omschakeling te verwijderen, gebruik deze bevelen op de wijze van de interfaceconfiguratie:
   ```
   no ip route-cache
   ```

Fout bij ontvangen van pakketten vanwege ESP-reeks mislukt

Hier volgt een voorbeeld van de foutmelding:

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

Deze foutmelding geeft doorgaans een van de volgende mogelijke omstandigheden aan:

- De versleutelde IPsec-pakketten worden door de versleutelingsrouter doorgestuurd omdat het QoS-mechanisme verkeerd is geconfigureerd.
- De IPsec-pakketten die door de decrypting-router worden ontvangen, zijn defect als gevolg van een pakketherschikking op een intermediair apparaat.
- Het ontvangen IPsec-pakket is gefragmenteerd en moet opnieuw worden geassembleerd voor verificatie en decryptie van verificatie.

Tijdelijke oplossing

1. Schakel QoS uit voor het IPsec-verkeer op de coderende of tussenliggende routers.
2. IPsec-pre-fragmentatie op de versleutelingsrouter inschakelen.
   ```
   Router(config-if)#crypto ipsec fragmentation before-encryption
   ```
3. Stel de MTU-waarde in op een grootte die niet hoeft te worden gefragmenteerd.
   ```
   Router(config)#interface type [slot_#/]port_#


   Router(config-if)#ip mtu MTU_size_in_bytes
   ```

4. Upgrade het Cisco IOS®-image naar het meest recente beschikbare stabiele image in die trein.

Als de grootte MTU op om het even welke router wordt veranderd, alle tunnels die op die interface worden geëindigd worden afgebroken.

Plan deze tijdelijke oplossing tijdens een geplande uitvaltijd.

Fout bij pogingen om VPN-tunnel op 7600 Series router tot stand te brengen

Deze fout wordt ontvangen wanneer u probeert om een VPN-tunnel te creëren op 7600 Series routers:

```
crypto_engine_select_crypto_engine: can't handle any more
```

Deze fout komt voor omdat de softwarecodering niet op 7600 reeksrouter wordt ondersteund. 7600 Series routers ondersteunen IPsec-tunnelbeëindiging zonder IPsec SPA-hardware niet. VPN wordt alleen ondersteund met een IPSEC-SPA kaart in 7600 routers.

PIX-debugs

show crypto isakmp sa

Deze opdracht toont de ISAKMP SA tussen peers.

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

In de manier waarop crypto isakmp output wordt uitgevoerd, moet de staat altijd **QM_IDLE** zijn. Als de staat **MM_KEY_EXCH** is, betekent dit dat de geconfigureerde vooraf gedeelde sleutel niet correct is of dat de peer IP-adressen verschillen.

```
PIX(config)#show crypto isakmp sa
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

U kunt dit corrigeren wanneer u het juiste IP-adres of de vooraf gedeelde sleutel configureert.

crypto ipsec tonen

Deze opdracht toont IPsec SA's die tussen peers zijn gebouwd. Een versleutelde tunnel wordt gebouwd tussen 10.1.0.1 en 10.1.0.2 voor verkeer dat tussen netwerken 10.1.0.0 en 10.1.1.0 loopt.

Je ziet de twee ESP SA's inbound en outbound. AH wordt niet gebruikt omdat er geen AH SA's zijn.

Een voorbeeld van de **show crypto ipsec sa** Het bevel wordt getoond in deze output.

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.0.2/255.255.255.255/0/0)
   current_peer: 10.2.1.1
   dynamic allocated peer ip: 10.1.0.2
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #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.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound esp sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

Deze opdracht geeft debug-informatie over IPsec-verbindingen weer en toont de eerste reeks kenmerken die worden ontkend vanwege incompatibiliteit aan beide uiteinden.

De tweede poging om 3DES aan te passen (om 3DES in plaats van DES en te proberen) **Secure Hash Algorithm (SHA)** is aanvaardbaar, en ISAKMP SA wordt gebouwd.

Dit debug is ook van een inbelclient die een IP-adres (10.32.8.1) uit een lokale pool accepteert. Zodra ISAKMP SA is gebouwd, worden de IPsec-kenmerken besproken en aanvaardbaar bevonden.

PIX stelt vervolgens de IPsec SA's in zoals hier te zien is. Deze output toont een voorbeeld van **debug crypto isakmp** uit.

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
```

```
ISAKMP:      auth pre-share
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

Deze opdracht geeft **debug**-informatie over IPsec-verbindingen weer.

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from  10.1.0.2  to  10.1.0.1
           (proxy 10.32.8.1 to  10.1.0.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  10.1.0.1  to  10.1.0.2
```

```
          (proxy 10.1.0.1 to 10.32.8.1)
        has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
          got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

Veelvoorkomende clientproblemen bij router-naar-VPN

Onvermogen om subnetten buiten de VPN-tunnel te benaderen: Split-tunnel

Deze output van de voorbeeldrouterconfiguratie toont hoe een gesplitste tunnel voor de VPN-verbindingen moet worden ingeschakeld.

Het **split tunnel** opdracht is gekoppeld aan de groep zoals deze in de **crypto isakmp client configuration group hw-client-groupname** uit.

Hierdoor kan de **Cisco VPN Client** om de router te gebruiken om toegang te krijgen tot een extra subnetverbinding die geen deel uitmaakt van de VPN-tunnel.

Dit gebeurt zonder compromissen in de beveiliging van de IPsec-verbinding. De tunnel is gevormd op het 192.0.2.18 netwerk.

Verkeerstromen niet versleuteld naar apparaten die niet in het **access list 150** opdracht, zoals internet.

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool
 acl 150
!
!
access-list 150 permit ip 192.0.2.18 0.0.0.127 any
!
```

Gemeenschappelijke PIX-to-VPN clientproblemen

De onderwerpen in deze sectie behandelen gemeenschappelijke problemen die u tegenkomt wanneer u PIX aan IPsec met behulp van VPN-client 3.x vormt. De voorbeeldconfiguraties voor de PIX zijn gebaseerd op versie 6.x.

Het verkeer stroomt niet nadat de tunnel tot stand is gebracht: Kan niet binnen het netwerk achter PIX pingen

Dit is een veel voorkomend probleem bij routing. Zorg ervoor dat de PIX een route heeft voor netwerken die zich binnen bevinden en niet rechtstreeks verbonden zijn met hetzelfde subnetje.

Ook, moet het binnennetwerk een route terug naar PIX voor de adressen in de pool van het cliëntadres hebben.

Deze output toont een voorbeeld.

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on
the inside.

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1

 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client
for the IPsec session.

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then
the router needs to have route !--- for 10.1.2.0/24 network with next hop as the PIX inside
interface !.

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

Nadat de tunnel omhoog is, kan de gebruiker niet Internet doorbladeren: Split-tunnel

De meest voorkomende reden voor dit probleem is dat, met de IPsec-tunnel van de VPN-client naar PIX, al het verkeer door de tunnel naar de PIX-firewall wordt verzonden.

De functionaliteit PIX staat niet toe dat verkeer wordt teruggestuurd naar de interface waar het werd ontvangen. Daarom werkt het verkeer dat voor het internet is bestemd niet.

Om dit probleem op te lossen, gebruikt u de **split tunnel** uit. Het idee achter deze oplossing is dat slechts één specifiek verkeer door de tunnel stuurt en de rest van het verkeer rechtstreeks naar het internet gaat, niet door de tunnel.

```
vpngroup vpn3000 split-tunnel 90
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

Het **vpngroup vpn3000 split-tunnel 90** opdracht maakt de gesplitste tunnel mogelijk met **access-list number 90**.

Het **access-list number 90** De opdracht definieert welke verkeersstromen door de tunnel gaan, de rest van die verkeersstromen wordt ontkend aan het eind van de toegangslijst.

De toegangslijst moet hetzelfde zijn om te weigeren **Network Address Translation (NAT)** op PIX.

Nadat de tunnel omhoog is, werken bepaalde toepassingen niet: MTU-aanpassing op client

Nadat de tunnel tot stand is gebracht, kunt u, hoewel u de machines op het netwerk achter de PIX-firewall kunt pingen, bepaalde toepassingen zoals Microsoft niet gebruiken **Outlook**.

Een veel voorkomend probleem is de maximale overdrachteenheid (MTU) van de pakketten. De IPsec-header kan maximaal 50 tot 60 bytes bevatten, wat wordt toegevoegd aan het oorspronkelijke pakket.

Als de grootte van het pakket meer dan 1500 wordt (de standaardinstelling voor het internet), moeten de apparaten het fragmenteren. Nadat de IPsec-header is toegevoegd, blijft de grootte onder 1496, wat het maximum is voor IPsec.

Het **show interface** het bevel toont MTU van die bepaalde interface op de routers die of op de routers in uw eigen gebouw toegankelijk zijn.

Om de MTU van het gehele pad van bron naar bestemming te bepalen, worden de datagrammen van verschillende groottes met de **Do Not Fragment (DF)** bit zo ingesteld dat, als het datagram verzonden is meer dan de MTU, deze foutmelding wordt teruggestuurd naar de bron:

```
frag. needed and DF set
```

Deze output toont een voorbeeld van hoe de MTU van het pad tussen de hosts met IP-adressen 10.1.1.2 en 172.16.1.56 te vinden is.

```
Router#debug ip icmp
ICMP packet debugging is on


!--- Perform an extended ping.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1550
Timeout in seconds [2]:


!--- Make sure you enter y for extended commands.

Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:


!--- Set the DF bit as shown.


Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
```

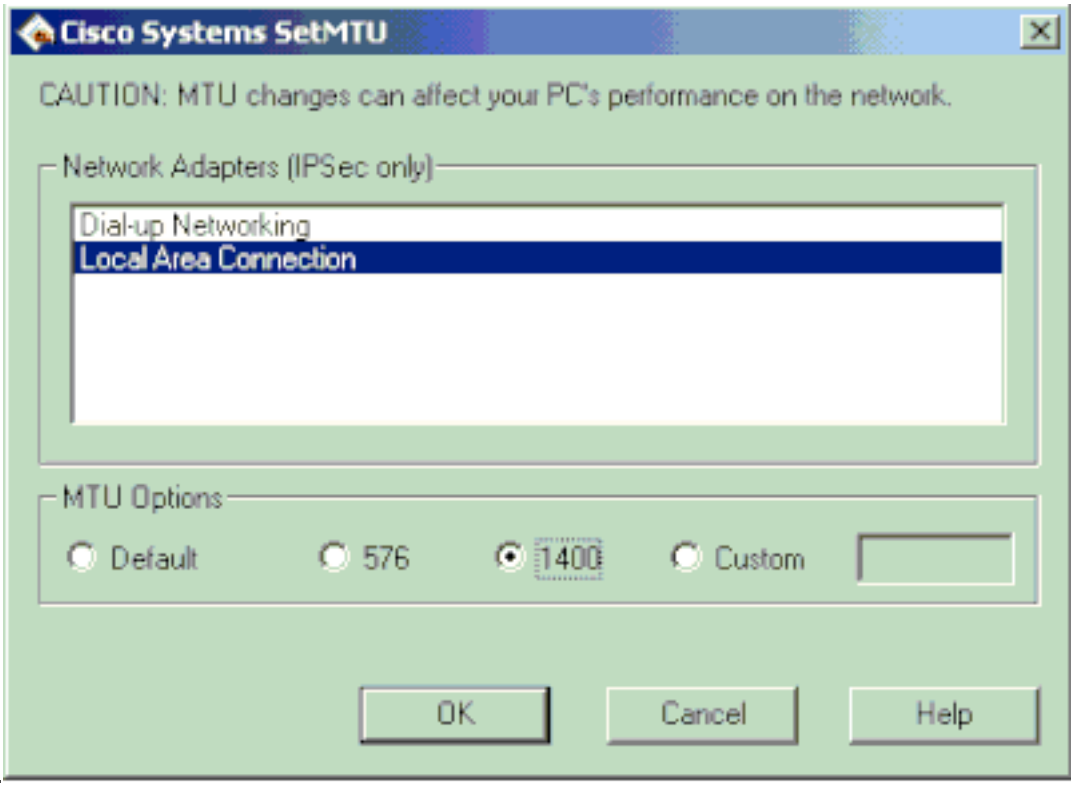
```
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

De VPN-client wordt geleverd met een MTU-hulpprogramma waarmee de gebruiker MTU kan aanpassen voor de Cisco VPN-client.

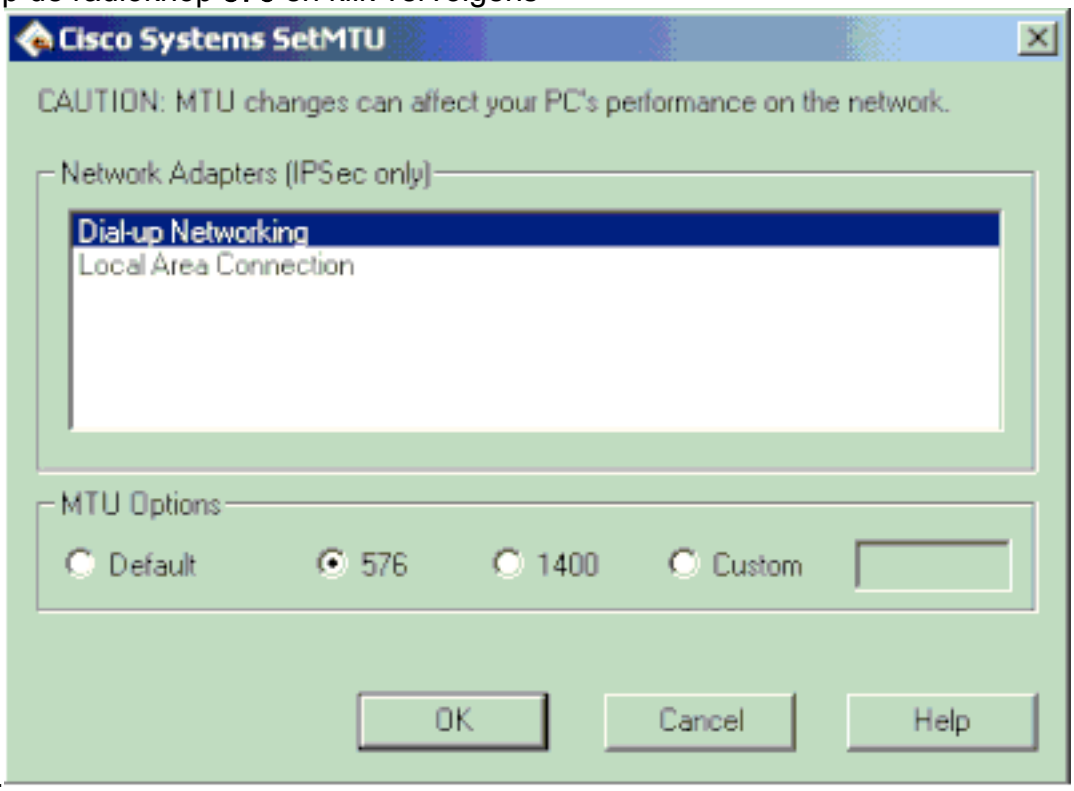
In het geval van gebruikers van PPP over Ethernet (PPPoE)-clients past u MTU aan voor de PPPoE-adapter.

Voltooi deze stappen om het hulpprogramma MTU aan te passen voor de VPN-client.

1. Kiezen **Start > Programs > Cisco System VPN Client > Set MTU**.
2. Kiezen **Local Area Connection**, en klik vervolgens op de radioknop 1400.



3. Klik **OK**.
4. Herhaal stap 1 en selecteer **Dial-up Networking**.
5. Klik op de radioknop **576** en klik vervolgens



op**OK**.

De sysopt-opdracht missen

Gebruik de **sysopt connection permit-ipsec** opdracht in IPsec-configuraties op de PIX om IPsec-verkeer door de PIX-firewall te laten lopen zonder controle van **conduit** of **access-list** opdrachtverklaringen.

Standaard moet elke inkomende sessie expliciet worden toegestaan door een **conduit** of **access-list** opdrachtverklaring. Met IPsec beveiligd verkeer kan de controle van de secundaire toegangslijst redundant zijn.

Gebruik de optie **sysopt connection permit-ipsec** uit.

Controleer toegangscontrolelijsten (ACL's)

In een typische IPsec VPN-configuratie worden twee toegangslijsten gebruikt.

Eén toegangslijst wordt gebruikt om verkeer bestemd voor de VPN-tunnel uit te sluiten van het NAT-proces.

De andere toegangslijst bepaalt welk verkeer moet worden versleuteld. Dit omvat een crypto ACL in een LAN-to-LAN installatie of een split-tunnel ACL in een configuratie voor externe toegang.

Wanneer deze ACL's onjuist zijn geconfigureerd of gemist, loopt verkeer mogelijk slechts in één richting over de VPN-tunnel, of is het helemaal niet over de tunnel verzonden.

Zorg ervoor dat u alle toegangslijsten heeft geconfigureerd die nodig zijn om uw IPsec VPN-configuratie te voltooien en dat voor deze toegangslijsten het juiste verkeer is gedefinieerd.

Deze lijst bevat items die moeten worden gecontroleerd wanneer u vermoedt dat een ACL de oorzaak is van problemen met uw IPsec VPN.

- Zorg ervoor dat het juiste verkeer is opgegeven voor uw NAT-uitzondering en crypto-ACL's.
- Als u meerdere VPN-tunnels en crypto-ACL's heeft, moet u ervoor zorgen dat deze ACL's elkaar niet overlappen.
- Gebruik ACL's niet twee keer. Gebruik ook twee verschillende toegangslijsten als hetzelfde verkeer wordt opgegeven voor uw ACL voor NAT-uitzonderingen en crypto-ACL.
- Zorg ervoor dat uw apparaat is geconfigureerd om de ACL voor NAT-uitzonderingen te gebruiken. Dat wil zeggen, gebruik de **route-map** bevel op de router; de **nat (0)** opdracht op de PIX of ASA. Een ACL voor NAT-uitzonderingen is vereist voor zowel LAN-to-LAN als externe toegang-configuraties.

Raadpleeg het gedeelte Verifiëren dat ACL's de juiste sectie zijn in de meest gebruikelijke oplossingen voor probleemoplossing van L2L en IPsec VPN voor externe toegang om meer te weten te komen over het verifiëren van de ACL-verklaringen.

Gerelateerde informatie

- Pagina voor IPsec-onderhandeling/IKE-protocolondersteuning
- Pagina met PIX-ondersteuning
- TechNotes
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.