# Gangbare problemen met L2L en IPsec VPN voor externe toegang troubleshooten

## Inhoud

# Inleiding

Dit document beschrijft de meest voorkomende oplossingen voor IPsec VPN-problemen.

# Achtergrondinformatie

De oplossingen die hier worden beschreven, komen rechtstreeks uit serviceaanvragen die de technische ondersteuning van Cisco heeft opgelost.

Veel van deze oplossingen worden geïmplementeerd voorafgaand aan de diepgaande probleemoplossing van een IPsec VPN-verbinding.

Dit document bevat een samenvatting van de gebruikelijke procedures die u moet proberen voordat u een verbinding kunt oplossen.

Hoewel de configuratievoorbeelden in dit document bedoeld zijn voor gebruik op routers en security applicaties, zijn bijna al deze concepten ook van toepassing op VPN 3000 .

Raadpleeg IP Security Proubleshooting - Begrip en gebruiken van debug commando's voor een toelichting op veelvoorkomende debug commando's die worden gebruikt om IPsec-problemen op zowel de Cisco IOS®-software als op te lossen.

**Opmerking:** ASA geeft geen multicast verkeer via IPsec VPN-tunnels door.

**Waarschuwing:** Veel van de oplossingen die in dit document worden gepresenteerd, kunnen leiden tot een tijdelijk verlies van alle IPsec VPN-connectiviteit op een apparaat.

Het wordt aanbevolen dat u deze oplossingen voorzichtig en in overeenstemming met uw beleid voor wijzigingsbeheer toepast.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de IPsec VPN-configuratie op deze Cisco-apparaten aan:

- Cisco ASA 5500 Series security applicatie
- Cisco IOS®-routers

## Gebruikte componenten

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

- Cisco ASA 5500 Series security applicatie
- Cisco IOS®

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.

### Conventies

Raadpleeg Cisco Technical Tips Conventies voor meer informatie over documentconventies.

# IPsec VPN-configuratie werkt niet

### Probleem

Een recent geconfigureerde of gewijzigde IPsec VPN-oplossing werkt niet.

Een huidige IPsec VPN-configuratie werkt niet meer.

### Oplossingen

Deze sectie bevat oplossingen voor de meest gangbare problemen met IPsec VPN.

Hoewel ze niet in een bepaalde volgorde worden vermeld, kunnen deze oplossingen worden gebruikt als een checklist van items om te verifiëren of proberen voordat u zich bezighoudt met diepgaande sanering.

Al deze oplossingen zijn rechtstreeks afkomstig van TAC-serviceaanvragen en hebben vele problemen opgelost.

- NAT-Traversal inschakelen (VPN-kwestie 1)
- Connectiviteit effectief testen
- ISAKMP inschakelen
- PFS in-/uitschakelen
- Oude of bestaande security koppelingen (tunnels) wissen
- Controleer de levensduur van ISAKMP
- ISAKMP-keepalives in- of uitschakelen
- Vooraf gedeelde sleutels opnieuw invoeren of herstellen
- Vooraf gedeelde sleutel komt niet overeen
- Crypto maps verwijderen en opnieuw toepassen
- Controleer of er systeemopdrachten aanwezig zijn (alleen/ASA)
- De ISAKMP-identiteit controleren
- Time-out bij inactiviteit/sessietime-out controleren
- Controleren of ACLâ€™s correct en aan crypto map gebonden zijn
- Het ISAKMP-beleid controleren

- Controleren of de routing juist is
- Controleren of de transformatieset juist is
- Volgnummers en naam van crypto map controleren
- Controleren of het peer-IP-adres juist is
- De tunnelgroep en groepsnamen controleren
- XAUTH voor L2L-peers uitschakelen
- Uitputting van de VPN-pool
- Problemen met latentie voor VPN-clientverkeer

**Opmerking:** Sommige opdrachten in deze secties over twee regels verdeeld vanwege de benodigde ruimte.

## NAT-Traversal inschakelen (VPN-kwestie 1)

**NAT-TraUniversal** (of NAT-T) maakt het mogelijk dat VPN-verkeer door NAT- of PAT-apparaten wordt doorgegeven, zoals een Linksys SOHO-router.

Als NAT-T niet is ingeschakeld, lijken VPN-clientgebruikers vaak zonder probleem verbinding te maken met de ASA, maar ze kunnen geen toegang krijgen tot het interne netwerk achter het security apparaat.

Als u de NAT-T niet inschakelt in het NAT/PAT-apparaat, kunt u **de** aanmaak van **de reguliere vertaling** ontvangen die **voor protocol 50 src binnen:10.0.1.26 dst buiten:10.9.69.4**foutmelding in de ASA is **mislukt**.

Als u niet in staat bent om tegelijkertijd in te loggen vanaf hetzelfde IP-adres, wordt **de beveiligde VPN-verbinding lokaal beëindigd door de client. Reden 412: De externe peer reageert niet meer.**foutmelding verschijnt.

Schakel NAT-T in het head-end VPN-apparaat in om deze fout op te lossen.

**Opmerking:** met Cisco IOS®-softwarerelease 12.2(13)T en hoger wordt NAT-T standaard ingeschakeld in Cisco IOS®.

Dit is de opdracht om NAT-T in te schakelen op een Cisco security applicatie. De twintig (20) in dit voorbeeld is de keepalive-tijd (standaard).

**ASA**

<#root>

```
securityappliance(config)#
```

```
crypto isakmp nat-traversal 20
```

Om het te laten werken moeten ook de clients worden aangepast.

In Cisco VPN Client, navigeer **naar** Connection-items en **klik op Wijzigen**. Het opent een nieuw venster waar u het tabblad Transport moet kiezen.

**Klik** onder dit tabblad **op Transparent** Tunneling **inschakelen** en op **het** keuzerondje **IPSec over UDP ( NAT / PAT )**. Klik vervolgens op Opslaan en de verbinding testen.

Het is belangrijk om UDP 4500 voor NAT-T-, UDP 500- en ESP-poorten toe te staan door de configuratie van een ACL, omdat de ASA als NAT-apparaat fungeert.

Raadpleeg Een IPsec-tunnel configureren via een firewall met NAT voor meer informatie over de ACL-configuratie in ASA.

## Connectiviteit effectief testen

Idealiter wordt de VPN-verbinding getest vanaf apparaten achter de endpointapparaten die de versleuteling uitvoeren, maar veel gebruikers testen de VPN-verbinding met de opdracht op de apparaten die de versleuteling uitvoeren.

Terwijl het pingelen over het algemeen voor dit doel werkt, is het belangrijk om uw pingelen van de juiste interface te voorzien.

Als de bron onjuist is, kan het lijken dat de VPN verbinding is mislukt wanneer deze echt werkt. Dit is een voorbeeld:

Crypto-ACL op router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Crypto-ACL op router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

In deze situatie, moet aping van het binnennetwerk achter één van beide router worden afkomstig. Dit komt doordat crypto-ACL's alleen geconfigureerd zijn om verkeer met die bronadressen te versleutelen.

Apingsourced van de buiteninterfaces van één van beide router wordt niet versleuteld. Gebruik de uitgebreide opties van het pingingbevel in bevoorrechte wijze EXEC om van bron te pingelen van de binneninterface van een router:

<#root>

```
routerA#
ping
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
```

```
Source address or interface: 192.168.100.1

Type of service [0]:
Set DF bit in IP header? [no]:
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, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

Stel je voor dat de routers in dit **diagram** zijn vervangen door ASA security applicaties. **Het pingelen** dat wordt gebruikt om connectiviteit te testen kan ook van de binneninterface met het binnensleutelwoord worden afkomstig:

<#root>

```
securityappliance#

ping inside 192.168.200.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Het is niet aan te raden om de binnenkant van een security applicatie **te** benaderen met **uw ping**.

Als u **uw ping** moet **koppelen** aan de **gebruikersinterface**, moet u de beheertoegang tot die interface **inschakelen**, anders reageert het apparaat niet.

<#root>

```
securityappliance(config)#

management-access inside
```

Als er een probleem is met de connectiviteit, werkt zelfs fase één (1) van VPN niet.

Voor ASA, als de connectiviteit ontbreekt, is de output SA gelijkaardig aan dit voorbeeld, dat op een mogelijke onjuiste crypto peer configuratie en/of onjuiste ISAKMP voorstelconfiguratie wijst:

<#root>

```
Router#

show crypto isakmp sa
```

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

De status kan van **MM_wait_MSG2** tot **MM_wait_MSG5** zijn, wat de mislukking van de betrokken statusuitwisseling in **Hoofdmodus (MM)** aanduidt.

**Crypto SA** output wanneer fase 1 omhoog is is gelijkaardig aan dit voorbeeld:

<#root>

```
Router#
```

**show crypto isakmp sa**

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

## ISAKMP inschakelen

Als er geen indicatie is dat een IPsec VPN-tunnel werkt, is het mogelijk dat ISAKMP niet is ingeschakeld. Zorg ervoor dat u ISAKMP op uw apparaten heeft ingeschakeld.

Gebruik een van de volgende opdrachten om ISAKMP op uw apparaten in te schakelen:

Cisco IOS®

<#root>

```
router(config)#
```

**crypto isakmp enable**

Cisco ASA (vervangen buiten uw gewenste interface)

<#root>

```
securityappliance(config)#
```

**crypto isakmp enable outside**

Bij het inschakelen van ISAKMP op de buiteninterface kan de volgende foutmelding optreden:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

De oorzaak van de fout kan zijn dat de Cliënt achter ASA PAT aan udp haven 500 krijgt alvorens de isakmp op de interface kan worden toegelaten. Zodra de PAT-vertaling is verwijderd (clear xlate) kan ISAKMP worden ingeschakeld.

Controleer dat UDP 500 en 4500 poortnummers zijn gereserveerd voor onderhandeling van ISAKMP-verbindingen met de peer.

Wanneer ISAKMP niet op de interface is ingeschakeld, toont de VPN-client een foutbericht dat vergelijkbaar is met dit bericht:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

Om deze fout op te lossen, laat ISAKMP op de crypto interface van de VPN gateway toe.

## PFS in-/uitschakelen

Bij IPsec-onderhandelingen zorgt Perfect Forward Secrecy (PFS) ervoor dat elke nieuwe cryptografische sleutel geen verband houdt met een eerdere sleutel.

Schakel PFS op beide tunnelpeers in of uit; anders wordt de LAN-to-LAN (L2L) IPsec-tunnel niet ingesteld in de ASA/Cisco IOS®-router.

**Perfect Forward Security (PFS) is bedrijfseigen van Cisco en wordt niet ondersteund op apparaten van derden.**

**ASA:**

PFS is standaard uitgeschakeld. Als u PFS wilt inschakelen, gebruikt u de opdracht pfscommando met de opdracht Enable keyword in de configuratiemodus voor groepsbeleid. Voer het trefwoord disable in om PFS uit te schakelen.

<#root>

```
hostname(config-group-policy)#
```

**pfs {enable | disable}**

Typ het **nr**-formulier van deze opdracht om het PFS-kenmerk uit de configuratie te verwijderen.

Een groepsbeleid kan een PFS-waarde overnemen van een ander groepsbeleid. Voer het **nr**-formulier van deze opdracht in om de overdracht van een waarde te voorkomen.

<#root>

```
hostname(config-group-policy)#
```

**no pfs**

**Cisco IOS® router:**

Om te specificeren dat IPsec om PFS moet vragen wanneer nieuwe **Security Associations** worden gevraagd voor deze crypto map-ingang, gebruik **deze set** pfscommando in crypto map-configuratiemodus.

Om te specificeren dat IPsec PFS vereist wanneer het verzoeken om nieuwe **Security Associations** ontvangt, gebruik **de set** pfscommando in crypto map configuratiemodus.

Als u wilt instellen dat IPsec niet om PFS vraagt, gebruikt u de no-vorm van deze opdracht. PFS wordt standaard niet aangevraagd. Als bij deze opdracht geen groep wordt gespecificeerd, wordt standaard group1 gebruikt.

```
set pfs [group1 | group2]
no set pfs
```

Argumenten van de opdracht set pfs:

- group1: Specificeert dat IPsec de 768-bits Diffie-Hellman prime modulus-groep moet gebruiken wanneer de nieuwe Diffie-Hellman uitwisseling wordt uitgevoerd.
- group2: Specificeert dat IPsec de 1024-bits Diffie-Hellman prime modulus-groep moet gebruiken wanneer de nieuwe Diffie-Hellman uitwisseling wordt uitgevoerd.

Voorbeeld:

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

**set pfs group2**

## Oude of huidige security associaties wissen (tunnels)

Als deze foutmelding in de Cisco IOS®® router voorkomt, is het probleem dat de SA is verlopen of gewist.

Het externe tunnel-eindapparaat weet niet dat het een verlopen SA gebruikt om een pakket versturen (dat geen SA-opbouwpakket is).

Wanneer er een nieuwe SA is opgebouwd, wordt de communicatie hervat. Initieer dus het interessante verkeer door de tunnel om een nieuwe SA te maken en de tunnel opnieuw op te bouwen.

<#root>

**%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA**

Het wissen van de security koppelingen (SA's) van ISAKMP (fase I) en IPsec (fase II) is de meest simpele en vaak de beste oplossing voor IPsec VPN-problemen.

Met het wissen van security koppelingen kan een breed scala foutmeldingen en vreemd gedrag worden opgelost zonder dat troubleshooten nodig is.

Hoewel deze methode eenvoudig kan worden gebruikt in elke situatie, is het bijna altijd nodig security koppelingen te wissen na het wijzigen van een huidige IPsec VPN-configuratie.

Bovendien, hoewel het mogelijk is alleen specifieke security koppelingen te wissen, kan het gunstig zijn om alle security koppelingen op het apparaat te wissen.

Zodra de Security Associations zijn ontruimd, kan het nodig zijn om verkeer door de tunnel te sturen om ze opnieuw te vestigen.

**Waarschuwing:** Tenzij u opgeeft welke security koppelingen u wilt wissen, kunnen de onderstaande opdrachten alle security koppelingen op het apparaat wissen. Ga voorzichtig te werk als andere IPsec VPN-tunnels in gebruik zijn.

1. Bekijk security koppelingen voordat u deze verwijdert

    a. **Cisco IOS IOS®**

    <#root>

    router#

    **show crypto isakmp sa**

    router#

    **show crypto ipsec sa**

    b. **Cisco ASA security applicaties**

    <#root>

    securityappliance#

    **show crypto isakmp sa**

    securityappliance#

    **show crypto ipsec sa**

2. Wis security koppelingen. Elke opdracht kan worden ingevoerd zoals vetgedrukt weergegeven of met de opties die worden weergegeven.

    a. **Cisco IOS®**

        a. **ISAKMP (fase I)**

        <#root>

        router#

        **clear crypto isakmp**

```
?
 <0 - 32766>  connection id of SA
 <cr>
```

b. **IPsec (fase II)**

<#root>

router#

**clear crypto sa**

```
?
 counters  Reset the SA counters
 map       Clear all SAs for a given crypto map
 peer      Clear all SAs for a given crypto peer
 spi       Clear SA by SPI
 <cr>
```

b. **Cisco ASA security applicaties**

a. **ISAKMP (fase I)**

<#root>

securityappliance#

**clear crypto isakmp sa**

b. **IPsec (fase II)**

<#root>

security appliance#

**clear crypto ipsec sa**

```
?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

## Controleer de levensduur van ISAKMP

Als de gebruikers vaak van de L2L-tunnel worden losgekoppeld, kan het probleem liggen in de lagere levensduur die is geconfigureerd in de SA van ISAKMP.

Als er tijdens het ISAKMP-leven een discrepantie optreedt, kunt u de**%ASA-5-713092** ontvangen**: Group**

**= x.x.x.x, IP = x.x.x.x, Mislukking tijdens fase 1 rekey poging als gevolg van** botsingsfoutmelding in /ASA.

De standaardinstelling is 86.400 seconden of 24 uur. Over het algemeen biedt een kortere levensduur veiligere ISAKMP-onderhandelingen (tot op een zekere hoogte), maar met een kortere levensduur stelt de security applicatie sneller toekomstige IPsec security koppelingen in.

Er is een match wanneer het beleid van de twee peers dezelfde encryptie-, hash-, authenticatie- en Diffie-Hellman-parameterwaarden bevatten, en wanneer het beleid van de externe peer een levensduur specificeert die korter is dan of gelijk is aan de levensduur van het vergeleken beleid.

Bij niet-overeenkomende levensduren wordt de kortere levensduur â€“ die van de externe peer â€“ gebruikt. Als er geen aanvaardbare overeenkomst wordt gevonden, weigert de IKE de onderhandeling en wordt de IKE SA niet opgebouwd.

Specificeer de SA-levensduur. Dit voorbeeld stelt een levensduur van 4 uur (14400 seconden) in. De standaardinstelling is 86400 seconden (24 uur).

ASA

<#root>

```
hostname(config)#
```

```
isakmp policy 2 lifetime  14400
```

Cisco IOS® router

<#root>

```
R2(config)#
```

```
crypto isakmp policy 10
```

```
R2(config-isakmp)#
```

```
lifetime 86400
```

Als de maximale geconfigureerde levensduur wordt overschreden, krijgt u deze foutmelding wanneer de VPN-verbinding wordt beëindigd:

```
Secure VPN Connection terminated locally by the Client. Reden 426: Maximale ingesteld levensduur overschreden.
```

Om deze foutmelding op te lossen, stelt u de elifetimewaarde in op nul (0) om de levensduur van een IKE-beveiligingsassociatie in te stellen op infinity. VPN wordt altijd verbonden en eindigt niet.

```
hostname(config)#isakmp policy 2 lifetime 0
```

U kunt **rexauth** ook **uitschakelen in het** groepsbeleid om het probleem op te lossen.

## ISAKMP-keepalives in- of uitschakelen

Het configureren van ISAKMP-keepalives helpt het voorkomen van het sporadisch verbreken van LAN-to-LAN VPN's of VPNâ€™s voor externe toegang, met inbegrip van VPN-clients, tunnels en tunnels die na een periode van inactiviteit worden verbroken.

Deze functie stelt het tunnel-endpoint in staat de voortdurende aanwezigheid van een externe peer te monitoren en zijn eigen aanwezigheid aan die peer te melden.

Als de peer niet meer reageert, verbreekt het endpoint de verbinding.

Om ervoor te zorgen dat ISAKMP-keepalives blijven werken, moeten beide VPN-endpoints deze ondersteunen.

Configureer ISAKMP-keepalives in Cisco IOS® met deze opdracht:

<#root>

```
router(config)#
```

**crypto isakmp keepalive 15**

Gebruik deze opdrachten om ISAKMP-keepalives op de **ASA security applicaties** te configureren:

Cisco ASA voor de tunnelgroep **10.165.205.222**

<#root>

```
securityappliance(config)#
```

**tunnel-group 10.165.205.222**
**ipsec-attributes**

```
securityappliance(config-tunnel-ipsec)#
```

**isakmp keepalive**
**threshold 15 retry 10**

In sommige situaties is het nodig om deze functie uit te schakelen om een probleem op te lossen, bijvoorbeeld als de VPN-client zich achter een firewall bevindt die DPD-pakketten tegenhoudt.

Cisco ASA, voor de tunnelgroep **10.165.205.222**

Schakel IKE keepalive-verwerking uit, die standaard is ingeschakeld.

<#root>

```
securityappliance(config)#
```

**tunnel-group 10.165.205.222**
**ipsec-attributes**

```
securityappliance(config-tunnel-ipsec)#
```

```
isakmp keepalive
```

```
disable
```

**Keepalives voor Cisco VPN Client 4.x uitschakelen**

Navigeer naar**%System Root% > Program Files > Cisco Systems > VPN Client >** Profielen op de client-pc die het probleem ondervindt om IKE keepalive uit te schakelen en bewerk **het PCF-bestand**, waar van toepassing, voor de verbinding.

Verander **deForceKeepAlive=0**(standaard) **inForceKeepAlive=1**.

**Keepalives** zijn eigendom van Cisco en worden niet ondersteund door apparaten van derden.

## Vooraf gedeelde sleutels opnieuw invoeren of herstellen

In veel gevallen kan een simpele typografische fout de schuld zijn als een IPsec VPN-tunnel niet werkt. Bijvoorbeeld worden op de security applicatie de vooraf gedeelde sleutels verborgen zodra ze worden ingevoerd.

Deze verduistering maakt het onmogelijk om te zien of een sleutel onjuist is. Zorg ervoor dat u alle vooraf gedeelde sleutels op elk VPN-endpoint correct hebt ingevoerd.

Voer een sleutel opnieuw in om er zeker van te zijn dat deze correct is; dit is een eenvoudige oplossing die kan helpen bij het voorkomen van diepgaande probleemoplossing.

In VPNâ€™s voor externe toegang, controleer of de geldige groepsnaam en vooraf gedeelde sleutels zijn ingevoerd in de Cisco VPN Client.

U kunt met deze fout geconfronteerd worden als de groepsnaam of de vooraf gedeelde sleutel niet wordt aangepast tussen de VPN-client en het head-end apparaat.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
```

```
negotiator:(Navigator:2202)
```

**Waarschuwing:** Als u crypto-gerelateerde opdrachten verwijdert, zal u waarschijnlijk een of alle VPN-tunnels stopzetten. Gebruik deze opdrachten voorzichtig en raadpleeg het wijzigingsbeheerbeleid van uw organisatie voordat u cryptoopdrachten verwijdert.

Gebruik deze opdrachten om het vooraf gedeelde sleutelsleutel voor de peer**10.0.0.1** of de groep Vpngroupin Cisco IOS® te verwijderen en opnieuw in te voeren:

Cisco LAN-to-LAN VPN

<#root>

```
router(config)#
```

```
no crypto isakmp key secretkey
   address 10.0.0.1
```

```
router(config)#
```

```
crypto isakmp key secretkey
   address 10.0.0.1
```

Cisco VPN voor externe toegang

<#root>

```
router(config)#
```

```
crypto isakmp client configuration
   group vpngroup
```

```
router(config-isakmp-group)#
```

```
no key secretkey
```

```
router(config-isakmp-group)#
```

```
key secretkey
```

Gebruik deze opdrachten om de pre-shared-keysecretkey voor de peer**10.0.0.1**on/ASA security applicaties te verwijderen en opnieuw in te voeren:

Cisco 6.x

<#root>

```
(config)#
```

```
no isakmp key secretkey address 10.0.0.1
```

```
(config)#
```

```
isakmp key secretkey address 10.0.0.1
```

Cisco/ASA 7.x en hoger

<#root>

```
securityappliance(config)#
```

**tunnel-group 10.0.0.1**
**ipsec-attributes**

```
securityappliance(config-tunnel-ipsec)#
```

**no ikev1 pre-shared-key**

```
securityappliance(config-tunnel-ipsec)#
```

**ikev1**

**pre-shared-key**
**secretkey**

## Vooraf gedeelde sleutel komt niet overeen

Het initialiseren van de VPN-tunnel wordt onderbroken. Deze kwestie doet zich voor als gevolg van een onaangepaste pre-shared-key tijdens de onderhandelingen over fase I.

**HetMM_wait_MSG_6**bericht in **de manier crypto isakmp** sacommand wijst op een slecht samengekomen pre-gedeelde sleutel zoals in dit voorbeeld:

<#root>

```
ASA#
```

**show crypto isakmp sa**

```
Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :
```

**MM_WAIT_MSG_6**

Om dit probleem op te lossen, voert u de vooraf gedeelde sleutel opnieuw in beide apparaten in. De vooraf gedeelde sleutel moet uniek zijn en met elkaar overeenstemmen. Zie Vooraf gedeelde toetsen opnieuw invoeren of herstellen voor meer informatie.

## Crypto maps verwijderen en opnieuw toepassen

Wanneer u beveiligingsassociaties opheldert, en het lost geen IPsec VPN probleem op, verwijder en

opnieuw toepassen van de relevante crypto kaart om een brede verscheidenheid van problemen op te lossen die intermitterende druppels van VPN-tunnel en mislukking van sommige VPN-sites omvatten om te komen.

**Waarschuwing:** Als u een crypto-kaart verwijdert van een interface, worden alle IPsec-tunnels die aan die cryptokaart gekoppeld zijn, automatisch verwijderd. Ga voorzichtig verder met deze stappen en overweeg het wijzigingsbeheerbeleid van uw organisatie voordat u verdergaat.

Gebruik deze opdrachten om een crypto-kaart in Cisco IOS te verwijderen en te vervangen®:

Begin met het verwijderen van de crypto map van de interface. Gebruik de no-vorm van **de crypto** mapopdracht.

<#root>

```
router(config-if)#
```

**no crypto map mymap**

Ga verder met het formulier om een volledige crypto-kaart te verwijderen.

<#root>

```
router(config)#
```

**no crypto map mymap 10**

Vervang de cryptokaart op interface Ethernet0/0 voor de peer**10.0.0.1**. Dit voorbeeld toont de minimum vereiste crypto kaartconfiguratie:

<#root>

```
router(config)#
```

**crypto map mymap 10 ipsec-isakmp**

```
router(config-crypto-map)#
```

**match address 101**

```
router(config-crypto-map)#
```

**set transform-set mySET**

```
router(config-crypto-map)#
```

**set peer 10.0.0.1**

```
router(config-crypto-map)#
```

**exit**

```
router(config)#
```

**interface ethernet0/0**

```
router(config-if)#
```

```
crypto map mymap
```

Gebruik deze opdrachten om een cryptokaart op de ASA te verwijderen en te vervangen:

Begin met het verwijderen van de crypto map van de interface. Gebruik de no-vorm van **de crypto** mapopdracht.

<#root>

```
securityappliance(config)#
```

```
no crypto map mymap interface outside
```

Ga verder met het formulier om de andere crypto-kaartopdrachten te verwijderen.

<#root>

```
securityappliance(config)#
```

```
no crypto map mymap 10 match
   address 101
```

```
securityappliance(config)#
```

```
no crypto map mymap set
   transform-set mySET
```

```
securityappliance(config)#
```

```
no crypto map mymap set
   peer 10.0.0.1
```

Vervang de crypto kaart voor peer**10.0.0.1**. Dit voorbeeld toont de minimum vereiste crypto kaartconfiguratie:

<#root>

```
securityappliance(config)#
```

```
crypto map mymap 10 ipsec-isakmp
```

```
securityappliance(config)#
```

```
crypto map mymap 10
   match address 101
```

```
securityappliance(config)#
```

```
crypto map mymap 10 set
   transform-set mySET
```

```
securityappliance(config)#
```

```
crypto map mymap 10 set
   peer 10.0.0.1
```

```
securityappliance(config)#
```

```
crypto map mymap interface outside
```

Als u de crypto-kaart verwijdert en opnieuw toepast, lost dit ook het connectiviteitsprobleem op als het IP-adres van head-end is gewijzigd.

## Controleer of er systolopdrachten aanwezig zijn (alleen ASA)

De **commandssysopt-verbinding staat toe-ipsecandsysopt verbinding staat toe-**vpnallow pakketten van een IPsec-tunnel en hun payloads om interface-ACLs op het security apparaat te omzeilen.

IPsec-tunnels die eindigen op de security applicatie, zullen waarschijnlijk mislukken als een van deze opdrachten niet ingeschakeld is.

In Security Appliance Software versie 7.0 en eerder is de relevante sysopt-opdracht voor deze situatie **sysopt connection license-ipsec**.

In Security Appliance Software versie 7.1(1) en hoger is de relevante sysopt-opdracht voor deze situatie **sysopt connection license-vpn**.

In 6.x is deze functionaliteit standaard uitgeschakeld. Met /ASA 7.0(1) en hoger is deze functionaliteit standaard ingeschakeld. Gebruik deze showbevelen om te bepalen als het relevante sysoptcommando op uw apparaat is ingeschakeld:

Cisco ASA

<#root>

```
securityappliance#
```

```
show running-config all sysopt
```

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
```

```
sysopt connection permit-vpn
```

```
!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

Gebruik deze opdrachten om de opdracht Correctsysoptvoor uw apparaat in te schakelen:

Cisco ASA

<#root>

```
securityappliance(config)#
```

```
sysopt connection permit-vpn
```

Als u geen gebruik wilt maken van **de** opdracht Verbindingsverbinding **stoppen**, moet u expliciet het gewenste interessante verkeer van bron naar bestemming toestaan.

Bijvoorbeeld, van Remote naar Local LAN van het externe apparaat en "UDP-poort 500" voor de buiteninterface van het externe apparaat naar de buiteninterface van het lokale apparaat, in externe ACL.

## De ISAKMP-identiteit controleren

Als de IPsec VPN-tunnel is mislukt binnen de IKE-onderhandeling, kan de fout te wijten zijn aan het feit of het onvermogen van de peer om de identiteit van zijn peer te herkennen.

Wanneer twee peers IKE gebruiken om IPsec security koppelingen op te zetten, stuurt elke peer zijn ISAKMP-identiteit naar de externe peer.

Elke peer stuurt of zijn IP-adres of de hostnaam, afhankelijk van de manier waarop de ISAKMP-identiteit ervan is ingesteld.

De ISAKMP-identiteit van de firewall wordt standaard ingesteld op het IP-adres.

Stel de security applicatie en de identiteit van de peers doorgaans op dezelfde manier in om een storing in de IKE-onderhandeling te voorkomen.

Om de fase 2-ID in te stellen die naar de peer wordt verzonden, gebruikt u **de** opdracht **isakmp**-identiteit in globale configuratiemodus.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication type
```

OF

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection type
```

OF

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (default
```

VPN-tunnels komen niet op na een verschuiving van configuratie van naar ASA met de ASA-configuratiemigratietool; deze berichten verschijnen in het logbestand:

**[IKEv1]: Groep = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry gevonden, het verwijderen!**

**[IKEv1]: Groep = x.x.x.x, IP = x.x.x.x, peer verwijderen uit correlatortabel is mislukt, geen overeenkomst!**

**[IKEv1]: Groep = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): Geen SPI om fase 2 SA te identificeren!**

**[IKEv1]: Groep = x.x.x.x, IP = x.x.x.x, peer verwijderen uit correlatortabel is mislukt, geen overeenkomst!**

## Time-out bij inactiviteit/sessietime-out controleren

Als de time-out voor inactiviteit is ingesteld op 30 minuten (zoals standaard) betekent dit dat de tunnel wordt verbroken na 30 minuten zonder verkeer.

De VPN-client wordt na 30 minuten losgekoppeld, ongeacht de parameter voor onbelaste time-out, en komt **de PEER_DELETE-IKE_DELETE**_UNSPECIFICEDerror tegen.

**Configureer de time-outen** sessietime-outeen om de tunnel **altijd** te maken, zodat de tunnel nooit wordt gedropt, zelfs wanneer apparaten van derden worden gebruikt.

### ASA

Voer **het vpn-idle-**timeoutcommando in in de configuratiemodus voor groepsbeleid of in de configuratiemodus voor de gebruikersnaam om de gebruikerstijd te configureren:

<#root>

hostname(config)#

**group-policy DfltGrpPolicy attributes**

hostname(config-group-policy)#

**vpn-idle-timeout none**

Configureer een maximale tijd voor VPN-verbindingen met **de vpn-sessie-**timeoutopdracht in configuratiemodus voor groepsbeleid of in configuratiemodus voor gebruikersnaam:

<#root>

hostname(config)#

**group-policy DfltGrpPolicy attributes**

hostname(config-group-policy)#

**vpn-session-timeout none**

Wanneer u **tunnelallgeconfigureerd** hebt, hoeft u geen **idle-**timeout te **configureren**, want zelfs als u een VPN-idle timeout configureert, werkt dit niet omdat al het verkeer door de tunnel gaat (omdat tunnel-all is geconfigureerd).

Daarom is het interessante verkeer (of zelfs het verkeer dat door de PC wordt gegenereerd) interessant en laat Idle-time-out niet in werking treden.

**Cisco IOS® router**

Gebruik **de crypto ipsec security-association idle-**time opdracht in globale configuratiemodus of crypto map configuratie modus om de IPsec SA inactiviteitstimer te configureren.

IPsec SA-inactiviteitstimers zijn standaard uitgeschakeld.

<#root>

**crypto ipsec security-association idle-time**

*seconds*

De tijd wordt gemeten in seconden, die de nutteloze timer een inactieve peer toestaat om een SA te handhaven. Het waardebereik voor het argument seconds is van 60 tot 86400.

## Controleren of ACLâ€™s correct en aan crypto map gebonden zijn

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 definieert 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 ACLâ€™s onjuist zijn geconfigureerd of gemist, loopt het verkeer mogelijk in één richting over de VPN-tunnel, of wordt het helemaal niet over de tunnel verzonden.

Zorg ervoor dat u de crypto ACL met crypto-kaart bindt met de opdracht **crypto map match address** in globale configuratiemodus.

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 u eenvoudig kunt controleren als 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.

Zorg ervoor dat uw apparaat is geconfigureerd om de ACL voor NAT-uitzonderingen te gebruiken. Voor een router betekent dit dat u **de route**-map opdracht gebruikt.

Voor ASA betekent dit dat u **de opdracht (0)**gebruikt. Een ACL voor NAT-uitzonderingen is vereist voor zowel LAN-to-LAN als externe toegang-configuraties.

Hier wordt een Cisco IOS® router geconfigureerd om verkeer vrij te stellen dat wordt verzonden tussen **192.168.100.0 /24** en **192.168.200.0 /24** of **192.168.1.0 /24**van NAT. Verkeer met andere bestemmingen is onderworpen aan NAT-overload:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

NAT-vrijstelling ACLâ€™s werken alleen met het IP-adres of IP-netwerken, zoals de genoemde voorbeelden (toegangslijst niet NAT), en moeten identiek zijn aan de crypto-map ACLâ€™s.

De NAT-vrijstelling ACLâ€™s werken niet met de poortnummers (bijvoorbeeld 23, 25,...).

In een VOIP-omgeving, waar de spraakoproepen tussen netwerken worden gecommuniceerd via VPN, werken de spraakoproepen niet als de NAT 0 ACLâ€™s niet goed zijn geconfigureerd.

Vóór het oplossen van problemen, wordt voorgesteld om de VPN connectiviteitsstatus te controleren omdat het probleem met misconfiguratie van NAT vrijgestelde ACLs zou kunnen zijn.

U kunt de foutmelding krijgen zoals weergegeven als er een foutieve configuratie is in NAT-vrijstelling (NAT 0) ACLâ€™s.

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

**Onjuist voorbeeld:**

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

**eq 25**

Als NAT-vrijstelling (nat 0) niet werkt, probeer dan deze te verwijderen en **de NAT 0-**opdracht te geven zodat deze werkt.

Zorg ervoor dat uw ACL's niet in de verkeerde volgorde staan en dat ze van het juiste type zijn.

LAN-to-LAN configuraties voor crypto-ACL's en ACL's met NAT-uitzondering moeten worden geschreven vanuit het perspectief van het apparaat waarop de ACL is geconfigureerd.

Dit betekent dat de ACLâ€™s elkaar moeten spiegelen. In dit voorbeeld is een LAN-naar-LAN-tunnel ingesteld tussen **192.168.100.0 /24** en **192.168.200.0 /24**.

Crypto-ACL op router A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

Crypto-ACL op router B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

Hoewel het hier niet wordt geïllustreerd, is dit zelfde concept van toepassing op de ASA security applicaties.

In ASA moeten ACLâ€™s met gesplitste tunnels voor configuraties met externe toegang standaardtoegangslijsten zijn die verkeer toestaan naar het netwerk waartoe de VPN-clients toegang nodig hebben.

Cisco IOS® routers kunnen uitgebreide ACL gebruiken voor gesplitste tunnels. In de uitgebreide toegangslijst is het gebruik van **'elke'** bij de bron in de gesplitste tunnel ACL gelijk aan het uitschakelen van gesplitste tunnel.

Gebruik alleen de bronnetwerken in de uitgebreide ACL voor gesplitste tunnel.

**Juist voorbeeld:**

<#root>

```
access-list 140 permit ip
```

**10.1.0.0 0.0.255.255**

```
 10.18.0.0 0.0.255.255
```

**Onjuist voorbeeld:**

<#root>

```
access-list 140 permit ip
```

**any**

```
 10.18.0.0 0.0.255.255
```

Cisco IOS®

<#root>

```
router(config)#
```

**access-list 10 permit ip 192.168.100.0**

```
router(config)#
```

```
crypto isakmp client configuration group MYGROUP
router(config-isakmp-group)#
acl 10
```

Cisco ASA

<#root>

```
securityappliance(config)#
access-list 10 standard
   permit 192.168.100.0 255.255.255.0
securityappliance(config)#
group-policy MYPOLICY internal
securityappliance(config)#
group-policy MYPOLICY attributes
securityappliance(config-group-policy)#
split-tunnel-policy
   tunnelspecified
securityappliance(config-group-policy)#
split-tunnel-network-list
   value 10
```

**Configuratie voor NAT-uitzondering in ASA versie 8.3. voor een site-to-site VPN-tunnel:**

Er moet een site-to-site VPN worden opgezet tussen HOASA en BOASA met beide ASAâ€™s in versie 8.3. De NAT-vrijstellingsconfiguratie op HOASA ziet er ongeveer als volgt uit:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

## Het ISAKMP-beleid controleren

Als de IPsec-tunnel niet actief is, controleer dan of het ISAKMP-beleid overeenkomt met de externe peers. Dit ISAKMP-beleid is toepasselijk voor zowel site-to-site (L2L) VPN's als IPsec VPN's voor externe toegang.

Als de Cisco VPN-clients of de site-to-site VPN niet in staat zijn de tunnel met het elders geplaatste apparaat tot stand te brengen, controleert u of **de twee peers dezelfde waarden voor encryptie, hash, verificatie en Diffie-Hellman parameter bevatten.**

Controleer wanneer het beleid van de externe peer een levensduur aangeeft die kleiner is dan of gelijk is aan de levensduur in het beleid dat de initiator heeft verzonden.

Als de levensduur niet identiek is, gebruikt de security applicatie de kortere levensduur. Als er geen aanvaardbare overeenkomst bestaat, weigert ISAKMP de onderhandeling en wordt de SA niet opgebouwd.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

Het gedetailleerde logboekbericht is als volgt:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

Dit bericht verschijnt gewoonlijk wegens slecht gecombineerd ISAKMP beleid of een gemiste NAT 0 verklaring.

Bovendien wordt deze melding weergegeven:

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Dit bericht geeft aan dat fase 2-berichten in de wachtrij staan nadat fase 1 is voltooid. Deze foutmelding is het gevolg van een van de volgende redenen:

- Mismatch in fase op een van de peers
- ACL blokkeert de peers na voltooiing van fase 1

Dit bericht komt gewoonlijk nadat **`deVerwijderende peer uit peer-tabel is mislukt, geen match!`**foutmelding.

Als de Cisco VPN-client het head-end apparaat niet kan verbinden, is het probleem mogelijk dat een mismatch in ISAKMP-beleid. Het head-end apparaat moet overeenkomen met een van de IKE-voorstellen van de Cisco VPN-client.

Voor het ISAKMP-beleid en de IPsec Transform-set die op de ASA worden gebruikt, kan de Cisco VPN-client geen beleid met een combinatie van DES en SHA gebruiken.

Als u DES gebruikt, moet u MD5 voor het hash-algoritme gebruiken, of u kunt de andere combinaties gebruiken: 3DES met SHA en 3DES met MD5.

## Controleren of de routing juist is

Zorg ervoor dat uw encryptie-apparaten zoals Routers en ASA security applicaties de juiste routing informatie hebben om verkeer te verzenden via uw VPN-tunnel.

Als er andere routers achter uw gatewayapparaat bestaan, ben zeker dat die routers het weten hoe te om de tunnel te bereiken en welke netwerken aan de andere kant zijn.

Eén belangrijke component van routing in een VPN-implementatie is RRI (Reverse Route Injection).

RRI plaatst dynamische vermeldingen voor externe netwerken of VPN-clients in de routingtabel van een VPN-gateway.

Deze routes zijn nuttig voor het apparaat waarop ze geïnstalleerd zijn, en voor andere apparaten in het netwerk, omdat de RRI-routes geherdistribueerd kunnen worden door een routingprotocol zoals EIGRP of OSPF.

Voor een LAN-to-LAN configuratie is het belangrijk dat elk endpoint één of meerdere routes heeft naar de netwerken waarvan het endpoint het verkeer moet versleutelen.

In dit voorbeeld, router A moet routes aan de netwerken achter router B door **10.89.129.2** hebben. De router B moet een gelijkaardige route aan **192.168.100.0 /24** hebben:

De eerste manier om ervoor te zorgen dat elke router de juiste route(s) kent, is om voor elk bestemmingsnetwerk statische routes te configureren. Bijvoorbeeld, voor Router A kunnen de volgende route-instructies zijn geconfigureerd.

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

Als router A is vervangen door een ASA, kan de configuratie er als volgt uitzien:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

Als er achter elk endpoint een groot aantal netwerken bestaat, wordt het ingewikkeld om de configuratie van statische routes te onderhouden.

In plaats daarvan raden we u aan om Reverse Route Injection te gebruiken, zoals beschreven. RRI plaatst routes voor alle externe netwerken die in de crypto-ACL zijn vermeld in de routingtabel.

De crypto-ACL en crypto map van Router A kan er bijvoorbeeld als volgt uitzien:

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

**reverse-route**

```
 set transform-set mySET
 match address 110
```

Als router A door ah ASA was vervangen, kan de configuratie als dit kijken:

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

**crypto map mymap 10 set reverse-route**

In een configuratie voor externe toegang zijn wijzigingen in de routing niet altijd nodig.

Maar als andere routers bestaan achter de VPN-gatewayrouter of security applicatie, moeten die routers het pad naar de VPN-clients op de een of andere manier leren.

In dit voorbeeld, veronderstel dat de VPN-clients adressen in het bereik van **10.0.0.0 /24** worden gegeven wanneer ze verbinding maken.

Als er geen routingprotocol in gebruik is tussen de gateway en de andere router(s), kunnen statische routes worden gebruikt op routers als Router 2:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Als er een routingprotocol zoals EIGRP of OSPF in gebruik is tussen de gateway en andere routers, wordt aanbevolen Reverse Route Injection te gebruiken zoals beschreven.

RRI voegt automatisch routes voor de VPN-client toe aan de routingtabel van de gateway. Deze routes kunnen vervolgens naar de andere routers in het netwerk worden gedistribueerd.

Cisco IOS® router:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

**reverse-route**

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASA security applicatie:

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

**crypto dynamic-map dynMAP 10 set reverse-route**

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

De routeringskwestie doet zich voor als de pool van IP-adressen die voor de VPN-clients zijn toegewezen, overlapt met interne netwerken van het head-end apparaat. Raadpleeg voor meer informatie het gedeelte Overlapping Private Networks (Overlappende particuliere netwerken).

## Controleren of de transformatieset juist is

Zorg ervoor dat de IPsec-encryptie en hash-algoritmen die gebruikt worden door de transformatieset aan beide uiteinden hetzelfde zijn.

Raadpleeg de opdrachtreferentie van de configuratiehandleiding van Cisco Security Appliance voor meer informatie.

Voor het ISAKMP-beleid en de IPsec Transform-set die op de ASA worden gebruikt, kan de Cisco VPN-client geen beleid met een combinatie van DES en SHA gebruiken.

Als u DES gebruikt, moet u MD5 voor het hash-algoritme gebruiken, of u kunt de andere combinaties gebruiken: 3DES met SHA en 3DES met MD5.

## Volgnummers en naam van crypto map controleren en ook of de crypto map wordt toegepast in de juiste interface waarin de IPsec-tunnel start/eindigt

Als statische en dynamische peers op dezelfde crypto map zijn geconfigureerd, is de volgorde van de crypto map-vermeldingen zeer belangrijk.

Het volgnummer van de dynamische crypto-map **moet** hoger zijn dan alle andere statische crypto-map-

items.

Als de statische vermeldingen een hoger volgnummer hebben dan de dynamische, mislukken de verbindingen met deze peers en wordt de volgende debug-informatie getoond.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Voor elke interface in de security applicatie is slechts één Dynamische Crypto-kaart toegestaan.

Dit is een voorbeeld van een goed genummerde crypto map die een statische en een dynamische vermelding bevat. Merk op dat de dynamische ingang het hoogste volgnummer heeft, en er ruimte is overgelaten voor aanvullende statische vermeldingen:

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

**`crypto map mymap 60000 ipsec-isakmp dynamic ciscothe`**

Crypto kaartnamen zijn hoofdlettergevoelig.

Deze foutmelding kan ook worden gezien wanneer de dynamische crypto man sequentie niet correct is wat ervoor zorgt dat de peer de verkeerde crypto map raakt.

Dit wordt ook veroorzaakt door een slecht samengestelde cryptotoegangslijst die het interessante verkeer definieert:**`%ASA-3-713042: IKE-initiator kan beleid niet vinden:`**

In een scenario waarin meerdere VPN-tunnels worden beëindigd in dezelfde interface, maakt u crypto-kaarten met dezelfde naam (slechts één crypto-kaart is toegestaan per interface) maar met een ander volgnummer.

Dit geldt voor de router en ASA.

Zie ook ASA: Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco voor meer informatie over de crypto-kaartconfiguratie voor zowel L2L als Remote Access VPN-scenario.

## Controleren of het peer-IP-adres juist is

Maak en beheer de database van verbindingsspecifieke records voor IPsec.

Specificeer voor een ASA security applicatie LAN-to-LAN (L2L) IPsec VPN-configuratie de **<naam>**van de tunnelgroep als het **externe peer IP-adres** (externe tunneleindpunt) in **de opdracht tunnelgroep <naam> type ipsec-l2**ll.

Het peer IP-adres moet overeenkomen met de namen van de **tunnelgroep** en **de** adresopdrachten **van de Crypto-kaartset**.

Bij het configureren van het VPN met ASDM wordt de naam van de tunnelgroep automatisch met het juiste peer-IP-adres gegenereerd.

Als het peer IP-adres niet goed is geconfigureerd, kunnen de logbestanden dit bericht bevatten, dat kan worden opgelost door de juiste configuratie van **het peer IP-adres**.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

Wanneer het peer IP-adres niet goed is geconfigureerd op de ASA crypto-configuratie, kan de ASA de VPN-tunnel niet tot stand brengen en hangt alleen in *de* fase MM_wait_*MSG4*.

Corrigeer in de configuratie het peer-IP-adres om dit probleem op te lossen.

Hier is de output van **de crypto isakmp-**opdracht wanneer de VPN-tunnel in de toestand MM_wait_MSG4 hangt.

<#root>

```
hostname#
```

**show crypto isakmp sa**

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

## De tunnelgroep en groepsnamen controleren

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

Dit bericht wordt weergegeven wanneer een tunnel wordt verbroken doordat de toegestane tunnel zoals gespecificeerd in het groepsbeleid afwijkt van de toegestane tunnel in de tunnelgroep-configuratie.

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

**Both lines read:**

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

Schakel IPsec in voor de bestaande protocollen in het standaardgroepsbeleid.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

## XAUTH voor L2L-peers uitschakelen

Als een LAN-to-LAN-tunnel en een Remote Access VPN-tunnel op dezelfde cryptografische kaart zijn geconfigureerd, wordt de LAN-to-LAN-peer gevraagd om XAUTH-informatie, en mislukt de LAN-to-LAN-tunnel met "***CONF_XAUTH***" in de uitvoer van **deze how crypto-**isakmp-opdracht.

Dit is een voorbeeld van de SA-output:

<#root>

```
Router#
```

**show crypto isakmp sa**

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

Dit probleem is alleen van toepassing op Cisco IOS® terwijl ASA niet door dit probleem wordt beïnvloed omdat er tunnelgroepen worden gebruikt.

Gebruik **theno-**xauthkeyword wanneer u de isakmp-toets invoert, zodat het apparaat niet om de peer voor XAUTH-informatie (gebruikersnaam en wachtwoord) vraagt.

Dit trefwoord schakelt XAUTH uit voor statische IPsec-peers. Voer een vergelijkbare opdracht in op het apparaat dat zowel L2L VPN als VPN voor externe toegang op dezelfde crypto map heeft geconfigureerd.

<#root>

```
router(config)#
```

**crypto isakmp key cisco123 address**
**   172.22.1.164 no-xauth**

In het scenario waarin de ASA fungeert als de Easy VPN Server, kan de eenvoudige VPN-client geen verbinding maken met head-end vanwege het Xauth-probleem.

Schakel de gebruikersverificatie in de ASA uit om het probleem op te lossen zoals hieronder wordt getoond:

<#root>

```
ASA(config)#
```

**tunnel-group example-group type ipsec-ra**

```
ASA(config)#
tunnel-group example-group ipsec-attributes
ASA(config-tunnel-ipsec)#
isakmp ikev1-user-authentication none
```

Zie de sectie Diversen van dit document voor meer informatie over **de** opdracht **isakmp ikev1-user-**authentication.

## Uitputting van de VPN-pool

Wanneer het bereik van de IP-adressen die aan de VPN-pool is toegewezen niet voldoet, kan de beschikbaarheid van de IP-adressen op twee manieren worden uitgebreid.

1. Verwijder het bestaande bereik en definieer een nieuw bereik. Hierna volgt een voorbeeld:

```
<#root>
CiscoASA(config)#
no ip local pool testvpnpool 10.76.41.1-10.76.41.254
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. Wanneer opgedeelde subnetten aan de VPN-pool moeten worden toegevoegd, kunt u twee afzonderlijke VPN-pools definiëren en ze vervolgens in volgorde specificeren onder de "tunnelgroepkenmerken". Hierna volgt een voorbeeld:

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

De volgorde waarin u de pools specificeert is zeer belangrijk, omdat de ASA adressen van deze pools toewijst in de volgorde waarin de pools in deze opdracht staan.

De instellingen voor adrespools in de opdracht adrespools voor groepsbeleid negeren altijd de lokale poolinstellingen in de opdracht adrespool voor tunnelgroepen.

### Problemen met latentie voor VPN-clientverkeer

Wanneer er latentieproblemen zijn via een VPN-verbinding, controleert u of aan deze voorwaarden is voldaan om dit op te lossen:

1. Controleer of de MSS-waarde van het pakket verder kan worden verkleind.
2. Als IPsec/tcp in plaats van IPsec/udp wordt gebruikt, configureer dan save-vpn-flow.
3. Laad Cisco ASA opnieuw.

# VPN-clients kunnen geen verbinding maken met ASA

## Probleem

Cisco VPN-clients kunnen niet verifiëren wanneer XAUTH wordt gebruikt met de RADIUS-server.

## Oplossing

Het probleem kan zijn dat bij XAUTH een time-out is opgetreden. Verhoog de time-outwaarde voor de AAA-server om dit probleem op te lossen.

Voorbeeld:

<#root>

```
Hostname(config)#
aaa-server test protocol radius

hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

## Probleem

Cisco VPN-clients kunnen niet verifiëren wanneer XAUTH wordt gebruikt met de RADIUS-server.

## Oplossing

Zorg er ten eerste voor dat de authenticatie correct werkt. Om het probleem te bepalen verifieert u eerst de

verificatie met de lokale database op de ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

Als dit goed werkt, is het probleem gerelateerd aan de Radius-serverconfiguratie.

Controleer de connectiviteit van de RADIUS-server vanaf de ASA. Als de ping zonder enig probleem werkt, controleer dan de RADIUS-configuratie op de ASA en de databaseconfiguratie op de RADIUS-server.

U kunt **de debug** radiusopdracht gebruiken om problemen met de straal op te lossen. Raadpleeg voor **voorbeelddebug** radiusuitvoer **deze voorbeelduitvoer**.

Alvorens u het debugcommando op de ASA gebruikt, raadpleegt u deze documentatie:**Waarschuwingsbericht**.

# VPN-client verliest vaak verbinding bij eerste poging of "Security VPN Connection terminated by peer. Reden 433." of "Beveiligde VPN-verbinding beëindigd door peer Reden 433:(reden niet opgegeven door peer)"

## Probleem

Cisco VPN-clientgebruikers ontvangen deze fout wanneer ze proberen verbinding te maken met het head-end VPN-apparaat.

**VPN-client laat verbinding vaak vallen bij eerste poging**

**Beveiliging VPN-verbinding beëindigd door peer. Reden 43.**

**Secure VPN-verbinding beëindigd door peer-reden 433:(reden niet opgegeven door peer)**

**Probeert een netwerk toe te wijzen of IP-adres uit te zenden, door x.x.x.x) uit pool te verwijderen**

## Oplossing 1

Het probleem kan bij de toewijzing van de IP-pool zijn door ASA, Radius server, DHCP server of door Radius server die fungeert als DHCP server.

Gebruik **de debug** cryptoopdracht om te verifiëren dat het netmasker en IP-adressen correct zijn. Controleer ook of de pool het netwerkadres en het broadcastadres niet bevat.

RADIUS-servers moeten de juiste IP-adressen aan de clients kunnen toewijzen.

## Oplossing 2

Dit probleem kan ook veroorzaakt zijn door het mislukken van uitgebreide verificatie. U moet de AAA-server controleren om deze fout te troubleshooten.

Controleer het wachtwoord voor de serververificatie op de server en de client. Door de AAA-server opnieuw te laden, kan dit probleem worden opgelost.

### Oplossing 3

Een andere tijdelijke oplossing voor dit probleem is om de functie voor bedreigingsdetectie uit te schakelen.

Op momenten dat er meerdere heruitzendingen zijn voor verschillende incomplete **Security Associations (SAâ€™s)**, denkt de ASA met de ingeschakelde bedreigingsdetectiefunctie dat er een scanaanval heeft plaatsgevonden en dat de VPN-poorten als de belangrijkste overtreder zijn gemarkeerd.

Probeer de functie voor bedreigingsdetectie uit te schakelen, omdat deze veel overhead kan veroorzaken bij de verwerking op de ASA. Gebruik deze opdrachten om de bedreigingsdetectie uit te schakelen:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Dit kan worden gebruikt als tijdelijke oplossing om te controleren of het werkelijke probleem hiermee is opgelost.

Zorg ervoor dat om de detectie van bedreigingen op Cisco ASA uit te schakelen, feitelijk verschillende beveiligingsfuncties worden gecompromitteerd, zoals beperking van de **scanpogingen**, **DoS met ongeldige SPI**, pakketten die **Application Inspection** mislukken en **onvolledige sessies**.

### Oplossing 4

Dit probleem kan ook veroorzaakt worden door een onjuiste configuratie van een transformatieset. Een juiste configuratie van de transformatieset lost het probleem op.

## Externe en EZVPN-gebruikers verbinden met VPN maar hebben geen toegang tot externe bronnen

### Probleem

Gebruikers met externe toegang hebben geen internetconnectiviteit na verbinding te hebben gemaakt met het VPN.

Gebruikers van externe toegang hebben geen toegang tot bronnen achter andere VPNâ€™s op hetzelfde apparaat.

Gebruikers van externe toegang hebben alleen toegang tot het lokale netwerk.

### Oplossingen

Probeer deze oplossingen om dit probleem op te lossen:

- Kan de servers in de DMZ niet bereiken

- VPN-clients kunnen DNS niet oplossen
- Split-Tunnelâ€”kan geen toegang tot internet of uitgesloten netwerken krijgen
- Lokale LAN-toegang
- Overlappende private netwerken

Kan de servers in de DMZ niet bereiken

Zodra de VPN-client de IPsec-tunnel met het VPN-head-end apparaat (ASA/Cisco IOS® router) is opgezet, kunnen de VPN-clientgebruikers toegang krijgen tot de interne netwerkbronnen (10.10.10.0/24), maar ze kunnen geen toegang krijgen tot het DMZ-netwerk (10.1.1.0/24).

**Diagram**

Controleer dat de configuratie met split-tunnel en NAT-uitzondering op het head-end apparaat is toegevoegd om toegang te hebben tot bronnen in het DMZ-netwerk.

**Voorbeeld:**

**ASA-configuratie:**

Deze configuratie toont hoe u de NAT-uitzondering voor het DMZ-netwerk kunt configureren om de VPN-gebruikers toegang te geven tot het DMZ-netwerk.

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

Nadat u een nieuwe vermelding voor de NAT-configuratie heeft toegevoegd, verwijdert u de NAT-vertaling.

```
Clear xlate
Clear local
```

**Verifiëren:**

Als de tunnel tot stand is gebracht, gaat u naar **de Cisco VPN-**client en **kiest u Status >** Routedetails om te controleren of de beveiligde routes voor zowel de DMZ- als de INSIDE-netwerken worden weergegeven.

Raadpleeg ASA: Voeg een nieuwe tunnel of externe toegang toe aan een bestaande L2L VPN - Cisco voor stappen die nodig zijn om een nieuwe VPN-tunnel of een externe VPN-toegang toe te voegen aan een L2L VPN-configuratie die al bestaat.

Verwijs naar ASA: Laat Split Tunneling toe voor VPN-clients in het ASA Configuration Voorbeeld voor stapsgewijze instructies over hoe VPN-clients toegang tot internet kan worden gegeven wanneer deze worden getunneld in een **Cisco 5500 Series adaptieve security applicatie (ASA)**.

## VPN-clients kunnen DNS niet oplossen

Nadat de tunnel is opgezet, als de VPN-clients niet in staat zijn de DNS op te lossen, kan het probleem de DNS-serverconfiguratie in het head-end apparaat (ASA) zijn.

Controleer ook de connectiviteit tussen de VPN-clients en de DNS-server. De DNS-serverconfiguratie moet worden geconfigureerd onder het groepsbeleid en worden toegepast onder het groepsbeleid in de tunnelgroep algemene kenmerken; bijvoorbeeld:

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a
```

```
group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com
```

```
!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.
```

```
tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

### VPN-clients zijn niet in staat om op naam verbinding te maken met interne servers

De VPN-client kan niet op naam een ping versturen naar de hosts of servers van het externe of head-end interne netwerk. U moet de configuratie van split-dns inschakelen op ASA om dit probleem op te lossen.

## Split-Tunnelâ€”kan geen toegang tot internet of uitgesloten netwerken krijgen

Met een gesplitste tunnel kunnen IPsec-clients met externe toegang voorwaardelijk pakketten rechtstreeks via de IPsec-tunnel in versleutelde vorm of naar een netwerkinterface in onversleutelde vorm, gedecrypteerd, waar ze worden gerouteerd naar een eindbestemming.

Split-tunnel is standaard uitgeschakeld, dat wil zeggen stilstaand verkeer.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

De **gespecificeerde** optie wordt alleen ondersteund voor Cisco VPN-clients, niet voor EZVPN-clients.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

Raadpleeg deze documenten voor gedetailleerde configuratievoorbeelden van gesplitste tunnels:

- ASA: Sta Split Tunneling toe voor VPN-clients in het ASA Configuration Voorbeeld
- Configuratievoorbeeld van router staat VPN-clients toe IPsec en het internet te verbinden met split-tunneling

### haarspeldoplossing

Deze optie is handig voor VPN-verkeer dat een interface betreedt maar vervolgens uit dezelfde interface wordt gerouteerd.

Bijvoorbeeld, in een hub en een spaak-VPN-netwerk, waar het beveiligingstoestel de hub is en de externe VPN-netwerken spokes zijn, moet **spaak-to-spaak** communicatieverkeer naar het beveiligingstoestel gaan en dan weer uit naar de andere spaak.

Gebruik **de** configuratie **van hetzelfde** beveiligingsverkeer om verkeer toe te staan dezelfde interface in te voeren en te verlaten.

<#root>

```
securityappliance(config)#
```

```
same-security-traffic permit intra-interface
```

### Lokale LAN-toegang

Gebruikers van externe toegang maken verbinding met het VPN maar hebben slechts toegang tot het lokale netwerk.

Raadpleeg voor een gedetailleerder configuratievoorbeeld ASA: Laat lokale LAN-toegang toe voor VPN-clients.

### Overlappende private netwerken

#### Probleem

Als u geen toegang heeft tot het interne netwerk nadat de tunnel is opgezet, controleer het IP-adres dat toegewezen is aan de VPN-client die overlapt met het interne netwerk achter het head-end apparaat.

#### Oplossing

Controleer of de IP-adressen in de pool die aan de VPN-clients moeten worden toegewezen, het interne netwerk van het head-end apparaat en het interne netwerk van de VPN-client zich in verschillende netwerken bevinden.

U kunt hetzelfde hoofdnetwerk met verschillende subnetten toewijzen, maar soms komen routingproblemen voor.

Zie voor meer voorbeelden DiagramenVoorbeeld van de sectieKan geen toegang krijgen tot de servers in DMZ.

## Kan geen verbinding maken met meer dan drie VPN-

# clientgebruikers

## Probleem

Slechts drie VPN-clients kunnen verbinding maken met ASA/; verbinding voor de vierde client mislukt. De volgende foutmelding wordt getoond:

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

## Oplossingen

In de meeste gevallen houdt dit probleem verband met een instelling voor gelijktijdige aanmelding binnen het groepsbeleid en de maximale sessielimiet.

Probeer deze oplossingen om dit probleem op te lossen:

- Gelijktijdige aanmeldingen configureren
- ASA configureren met CLI
- Configureren Configureren

## Gelijktijdige aanmeldingen configureren

Als het vakje Inheritcheck in ASDM is ingeschakeld, is alleen het standaardaantal gelijktijdige aanmeldingen voor de gebruiker toegestaan. De standaardwaarde voor gelijktijdige logins is drie (3).

Om dit probleem op te lossen, verhoogt u de waarde voor gelijktijdige aanmeldingen.

1. Start ASDM en navigeer vervolgens **naar Configuration > VPN > Group Policy**.
2. Kies de juiste groep en klik op de knop Bewerken.
3. Annuleert in het tabblad Algemeen het vakje Inheritcheck **voor gelijktijdige aanmelding onder Verbindingsinstellingen**. Kies een geschikte waarde in het veld.

   De minimumwaarde voor dit veld is nul (0), waardoor de aanmelding wordt uitgeschakeld en de toegang van gebruikers wordt verhinderd.

   Wanneer u inlogt met dezelfde gebruikersaccount vanaf een andere pc, wordt de huidige sessie (de verbinding die tot stand is gebracht vanaf een andere pc met dezelfde gebruikersaccount) beëindigd en wordt de nieuwe sessie gestart.

Dit is het standaardgedrag en is onafhankelijk van gelijktijdige VPN-aanmeldingen.

## ASA configureren met CLI

Voltooi deze stappen om het gewenste aantal gelijktijdige logins te configureren. In dit voorbeeld werd twintig (20) gekozen als de gewenste waarde.

<#root>

```
ciscoasa(config)#
```

**group-policy Bryan attributes**

```
ciscoasa(config-group-policy)#
```

**vpn-simultaneous-logins 20**

Raadpleeg de Opdrachtreferentie voor Cisco security applicatie voor meer informatie over deze opdracht.

Gebruik **de** opdracht **max-sessie**-limiet in globale configuratiemodus om VPN-sessies te beperken tot een lagere waarde dan het security apparaat toestaat.

Gebruik de versie van deze opdracht om de sessielimiet te verwijderen. Gebruik de opdracht opnieuw om de huidige instelling te overschrijven.

```
vpn-sessiondb max-session-limit {session-limit}
```

Dit voorbeeld toont hoe u een maximum VPN-sessielimit van 450 instelt:

<#root>

```
hostname#
```

**vpn-sessiondb max-session-limit 450**

## Configureren

### Fout

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

### Oplossing

Volg deze stappen om het gewenste aantal gelijktijdige aanmeldingen te configureren. U kunt ook proberen de gelijktijdige aanmeldingen voor deze SA in te stellen op 5:

**Kies Configuratie > Gebruikersbeheer > Groepen > Wijzigen 10.19.187.229 > Algemeen > Gelijktijdige logins**, en verander het aantal logins in **5**.

# Kan sessie of toepassing niet starten en overdracht nadat tunnel tot stand is gebracht is langzaam

## Probleem

De toepassing of sessie initieert niet door de tunnel nadat een IPsec-tunnel is opgebouwd.

## Oplossingen

Gebruik deze opdracht om het netwerk te controleren of om te weten te komen of de toepassingsserver bereikbaar is via uw netwerk.

Het kan een probleem zijn met de maximale segmentgrootte (MSS) voor tijdelijke pakketten die een router of /ASA apparaat oversteken, specifiek TCP-segmenten met de SYN-bitset.

## Cisco IOS® routerâ€”Wijzig de MSS-waarde in de buiteninterface (Tunnel End Interface) van de router

Voer de volgende opdrachten uit om de MSS-waarde in de buiteninterface (interface aan tunnel-einde) van de router te wijzigen:

<#root>

```
Router>
enable

Router#
configure terminal
Router(config)#
interface ethernet0/1

Router(config-if)#ip tcp adjust-mss 1300
Router(config-if)#
end
```

Deze berichten tonen de debug-output voor TCP MSS:

<#root>

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
```

```
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

De MSS wordt ingesteld op 1300 op de router zoals geconfigureerd.

Raadpleeg voor meer informatie ASA en Cisco IOS®: VPN Fragmentation.

### ASA â€" Raadpleeg de documentatie over /ASA

Er is geen toegang tot het internet of langzame overdracht door de tunnel vanwege MSS-problemen, en de foutmelding over MTU-grootte wordt gegeven.

Raadpleeg dit document om het probleem op te lossen:

- ASA en Cisco IOS®: VPN-fragmentatie

## Kan VPN-tunnel niet starten vanaf ASA

### Probleem

U kunt de VPN-tunnel niet starten vanaf de ASA-interface, en na de tunnelinstelling kan de externe end/VPN-client de interne interface van ASA niet pingen in de VPN-tunnel.

De pn-client kan bijvoorbeeld geen SSH- of HTTP-verbinding met ASA's initiëren binnen de interface via VPN-tunnel.

### Oplossing

De binneninterface van de tunnel kan niet van het andere eind van de tunnel worden gepingeld tenzij **het beheer**-toegangsbevel op de globale configuratiewijze wordt gevormd.

<#root>

```
ASA-02(config)#
management-access inside

ASA-02(config)#
show management-access

management-access inside
```

Deze opdracht helpt ook met ssh-initiatie of http-verbinding naar binnen-interface van ASA via een VPN-tunnel.

Deze informatie geldt ook voor de DMZ-interface. Bijvoorbeeld, als u de interface DMZ van /ASA wilt pingelen of een tunnel van interface DMZ wilt in werking stellen, dan wordt **het beheer-toegang** bevel

DMZ vereist.

<#root>

```
ASA-02(config)#
```

```
management-access DMZ
```

Als de VPN-client geen verbinding kan maken, zorg er dan voor dat de ESP- en UDP-poorten geopend zijn.

Als die poorten echter niet open zijn, probeer dan op TCP 10000 verbinding te maken met de selectie van deze poort onder de VPN-clientverbindingsingang.

Rechtsklik op **wijzigen > tabblad transport > IPsec via TCP**.

# Verkeer kan niet door de VPN-tunnel

## Probleem

U kunt geen verkeer via een VPN-tunnel doorgeven.

## Oplossing

Dit probleem kan ook optreden wanneer de ESP-pakketten worden geblokkeerd. Om dit probleem op te lossen, configureer je de VPN-tunnel opnieuw.

Dit probleem kan optreden wanneer gegevens niet worden versleuteld maar alleen worden gedecrypteerd via de VPN-tunnel zoals in deze uitvoer wordt getoond:

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y
```

```
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

Controleer of aan de volgende voorwaarden is voldaan om dit probleem op te lossen:

1. Of de crypto-toegangslijsten overeenkomen met de externe locatie en de toegangslijsten met NAT 0 juist zijn.

2. Als routing correct is en het verkeer raakt buiten interface die binnenin passeert. De voorbeeldoutput toont dat decryptie werkt, maar encryptie niet.

3. Als deze optie verbinding-vpn-opdracht toestaat is geconfigureerd op de ASA. Indien niet geconfigureerd, configureer deze opdracht omdat de ASA het versleutelde/VPN-verkeer kan vrijstellen van interface-ACL-controle.

# Back-uppeer voor VPN-tunnel op dezelfde cryptografische kaart configureren

## Probleem

U wilt meerdere back-up peers gebruiken voor één VPN-tunnel.

## Oplossing

De configuratie van meerdere peers is gelijk aan de levering van een reservelijst. Voor elke tunnel probeert de security applicatie te onderhandelen met de eerste peer op de lijst.

Als deze peer niet reageert, gaat de security applicatie de lijst af totdat of een peer reageert of er geen peers meer op de lijst staan.

ASA heeft een cryptokaart die reeds als primaire peer is geconfigureerd. De secundaire peer kan na de primaire worden toegevoegd.

Deze voorbeeldconfiguratie toont de primaire peer als X.X.X.X en back-up peer als Y.Y.Y.Y:

<#root>

ASA(config)#

**crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y**

# VPN-tunnel uitschakelen/opnieuw starten

## Probleem

Voltooi de procedure in deze sectie om de VPN-tunnel tijdelijk uit te schakelen en de service opnieuw te starten.

## Oplossing

Gebruik **de crypto map** interfaceopdracht in globale configuratiemodus om een eerder gedefinieerde crypto map te verwijderen die is ingesteld op een interface.

Gebruik de enoform van deze opdracht om de crypto map set van de interface te verwijderen.

<#root>

```
hostname(config)#
```

**no crypto map**

*map-name*

**interface**

*interface-name*

Deze opdracht verwijdert een crypto map die op een actieve interface van de security applicatie is ingesteld en maakt de IPsec VPN-tunnel inactief in die interface.

Om de IPsec-tunnel op een interface te hervatten, moet u een crypto map toewijzen die op een interface is ingesteld voordat die interface IPsec-services kan leveren.

<#root>

```
hostname(config)#
```

**crypto map**

*map-name*

**interface**

*interface-name*

# Sommige tunnels zijn niet versleuteld

## Probleem

Wanneer een zeer groot aantal tunnels op de VPN-gateway wordt geconfigureerd, geven sommige tunnels geen verkeer door. ASA ontvangt geen versleutelde pakketten voor die tunnels.

## Oplossing

Dit probleem treedt op omdat ASA de versleutelde pakketten niet door de tunnels kan sturen. In de ASP-tabel worden dubbele encryptieregels gemaakt.

# Fout:- %ASA-5-713904: Groep = DefaultRAGroup, IP = x.x.x.x, ... niet-ondersteunde Transaction Mode v2, versie 2.Tunnel beëindigd.

## Probleem

De**%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... niet-ondersteunde Transaction Mode v2,** wordt weergegeven.

### Oplossing

De reden voor de foutmelding `Transaction Mode v2` is dat ASA alleen IKE Mode Config V6 ondersteunt en niet de oude versie van de V2-modus.

Gebruik de IKE Mode Config V6-versie om deze fout op te lossen.

## Fout:- %ASA-6-722036: Groep client-groep Gebruiker xxxx IP x.x.x.x.x Zend groot pakket 1220 (drempelwaarde 1206)

### Probleem

De foutmelding**`%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x> Transmitting large packet 1220 (drempelwaarde 1206)`** verschijnt in de logs van ASA.

Wat betekent deze melding en hoe kan dit probleem worden opgelost?

### Oplossing

Dit logboekbericht geeft aan dat een groot pakket naar de client is verzonden. De bron van het pakket is niet op de hoogte van de MTU van de client.

Dit kan ook het gevolg zijn van compressie van data die niet kunnen worden gecomprimeerd. De tijdelijke oplossing is om de SVC compressie uit te schakelen zonder opdracht voor **compressie**, waardoor het probleem wordt opgelost.

## Foutmelding wanneer QoS aan één einde van de VPN-tunnel is ingeschakeld

### Probleem

Als u QoS in één uiteinde van de VPN-tunnel inschakelt, kunt u deze foutmelding ontvangen:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

### Oplossing

Dit bericht wordt normaal veroorzaakt wanneer één eind van de tunnel QoS uitvoert. Dit gebeurt wanneer een pakket als buiten bedrijf wordt gedetecteerd.

Om dit te stoppen kunt u QoS uitschakelen, maar zolang de tunnel werkt kan dit ook worden genegeerd.

## WAARSCHUWING: crypto map entry incomplete

### Probleem

Wanneer u **de opdracht crypto map mymap 20 ipsec-**isakmpcommando uitvoert, kunt u deze fout ontvangen:

**WAARSCHUWING: crypto map entry incomplete**

Voorbeeld:

<#root>

```
ciscoasa(config)#
```

**crypto map mymap 20 ipsec-isakmp**

**WARNING: crypto map entry incomplete**

## Oplossing

Dit is een gebruikelijke waarschuwing wanneer u een nieuwe crypto-kaart definieert; een herinnering dat parameters zoals access-list (match address), transformatie set en peer address moeten worden geconfigureerd voordat het kan werken.

Het is ook normaal dat de eerste regel die u typt om de crypto map te definiëren niet in de configuratie wordt getoond.

# Fout:- %ASA-4-400024: IDS:2151 groot ICMP-pakket van naar buiten op interface

## Probleem

Het is niet mogelijk grote ping-pakketten door te VPN-tunnel te sturen. Wanneer we proberen grote pingpakketten over te gaan, krijgen we de fout**%ASA-4-400024: IDS:2151 Large ICMP-pakket van naar buiten op de interface.**

## Oplossing

Schakel de handtekeningen 2150 en 2151 uit om dit probleem op te lossen. Zodra de handtekeningen zijn uitgeschakeld, werkt ping als normaal.

Gebruik deze opdrachten om de handtekeningen uit te schakelen:

ASA(config)#**ip audit signature 2151 disable**

ASA(config)#**ip audit signature 2150 disable**

# Fout:- %ASA-4-402119: IPSEC: Ontvangen een protocolpakket (SPI=spi, volgnummer= seq_num) van remote_IP (gebruikersnaam) naar local_IP dat anti-replay controle niet heeft uitgevoerd.

### Probleem

De volgende foutmelding wordt weergegeven in de logboekberichten van ASA:

**Fout:- %|ASA-4-402119: IPSEC: Ontvangen van een protocolpakket (SPI=spi, sequentienummer= seq_num) van remote_IP (gebruikersnaam) naar local_IP dat anti-replay controle niet heeft uitgevoerd.**

### Oplossing

Om deze fout op te lossen, gebruik **de crypto ipsec security-association replay venster-**size opdracht om de venstergrootte te variëren.

<#root>

hostname(config)#

**crypto ipsec security-association replay window-size 1024**

Cisco raadt u aan het volledige 1024-venster te gebruiken om eventuele problemen met de terugspelen te voorkomen.

## Foutmelding - %ASA-4-407001: Verkeer ontkennen voor local-host interface_name:inside_address, licentielimiet van aantal overschreden

### Probleem

Een aantal hosts kan geen verbinding maken met het internet, en deze foutmelding wordt in het syslog weergegeven:

**Foutmelding - %ASA-4-407001: Verkeer ontkennen voor local-host interface_name:inside_address, licentielimiet van aantal overschreden**

### Oplossing

Deze foutmelding komt voor als het aantal gebruikers de gebruikerslimiet van de licentie overstijgt. Deze fout kan worden opgelost door de licentie te upgraden naar een hoger aantal gebruikers.

De gebruikerslicentie kan naar wens 50, 100 of een onbeperkt aantal gebruikers ondersteunen.

## Fout: - %VPN_HW-4-PACKET_ERROR:

### Probleem

`De foutmelding - %VPN_HW-4-PACKET_ERROR:`foutmelding geeft aan dat het ESP-pakket met HMAC dat door de router wordt ontvangen, niet goed overeenkomt. Deze fout kan door deze kwesties worden veroorzaakt:

- De VPN H/W-module is defect

- Het ESP-pakket is beschadigd

### Oplossing

Om dit probleem op te lossen:

- Negeer de foutmelding indien verkeersonderbreking optreedt.
- Vervang de module als een verkeersonderbreking optreedt.

# Foutmelding: Opdracht verworpen: verwijder eerst de cryptoverbinding tussen VLAN XXXX en XXXX.

### Probleem

Deze foutmelding wordt weergegeven wanneer u probeert een toegestaan VLAN toe te voegen aan de trunkpoort op een switch:`Opdracht verworpen: crypto-verbinding tussen VLAN XXXX en VLAN XXXX verwijderen, eerst..`

De WAN-edge-trunk kan niet worden aangepast om extra VLANâ€™s toe te staan. Dat wil zeggen, u kunt geen VLANâ€™s toevoegen in **de IPSEC VPN** SPAtrunk.

Dit commando wordt afgewezen omdat het resulteert in een crypto verbonden interface VLAN die behoort tot de toegestane VLAN lijst, die een potentiële IPSec security breuk vormt.

Merk op dat dit gedrag van toepassing is op alle trunkpoorten.

### Oplossing

In plaats van `de` opdracht `van de switchport trunk toegestaan VLAN (vlanlist)`, gebruik `de trunk van switchport toegestaan VLAN-`non-commando of de `"switchport trunk toegestaan vlan verwijderen (vlanlist)"`opdracht.

# Foutmelding - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for sessie x.x.x.x:27331 to x.x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

### Probleem

Het volgende probleem treedt op bij het telnetten vanaf een apparaat aan het andere uiteinde van een VPN-tunnel of vanaf de router zelf:

**`Foutmelding - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for sessie x.x.x.x:27331 to x.x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]`**

### Oplossing

De gebruikerslicentie kan naar wens 50, 100 of een onbeperkt aantal gebruikers ondersteunen. De functie

van de vensterschaal werd toegevoegd om voor snelle transmissie van gegevens over lange vetnetwerken (LFN) toe te staan.

Dit zijn doorgaans verbindingen met zeer hoge bandbreedte maar ook hoge latentie.

Een voorbeeld van een LFN is een netwerk met satellietverbindingen, aangezien dergelijke links altijd hoge verspreidingsvertragingen maar doorgaans ook een hoge bandbreedte hebben.

Om de functie van de vensterschaal toe te laten om LFNs te steunen, moet de het venstergrootte van TCP meer dan 65.535 zijn. Deze foutmelding kan worden opgelost als u de TCP venstergrootte vergroot om meer dan 65.535 te zijn.

# %ASA-5-305013: Asymmetrische NAT-regels voor voor- en achteruit aangepast. Please update this issue flows

## Probleem

De volgende foutmelding wordt weergegeven zodra de VPN-tunnel is opgezet:

```
%ASA-5-305013: Asymmetrische NAT-regels voor voor- en achteruit aangepast. Please update this issue flows
```

## Oplossing

Om dit probleem op te lossen wanneer niet op dezelfde interface als de host met NAT, gebruik het toegewezen adres in plaats van het eigenlijke adres om verbinding te maken met de host.

Schakel bovendien de opdracht Inspectie in als de toepassing het IP-adres insluit.

# %ASA-5-713068: Ontvangen niet-routinematig Melden-bericht: notification_type

## Probleem

De volgende foutmelding wordt weergegeven als de VPN-tunnel niet wordt opgebouwd:

```
%ASA-5-713068: Ontvangen niet-routinematig Melden-bericht: notification_type
```

## Oplossing

Deze melding wordt veroorzaakt door een onjuiste configuratie (de ACL's of het beleid op de peers komen niet overeen)

Zodra het beleid en de ACL's overeenkomen, wordt de tunnel zonder problemen opgezet.

# %ASA-5-720012: (VPN-Secundair) Kan IPSec failover runtime data op de standby unit (of) %ASA-6-720012 niet bijwerken: (VPN-unit) Kan IPsec failover runtime data op de standby unit niet bijwerken

### Probleem

Een van de volgende foutmeldingen wanneer u de Cisco adaptieve security applicatie (ASA) probeert te upgraden:

**%ASA-5-720012: (VPN-Secondary) Kan IPSec failover-runtime gegevens op de standby-unit niet bijwerken.**

**%ASA-6-720012: (VPN-unit) Kan IPsec failover-runtime gegevens op de standby-unit niet bijwerken.**

### Oplossing

Deze foutmeldingen zijn informatief. De berichten hebben geen invloed op de functionaliteit van de ASA of het VPN.

Deze berichten verschijnen wanneer het VPN failover subsysteem geen IPsec-gerelateerde runtime gegevens kan bijwerken omdat de gerelateerde IPsec-tunnel is verwijderd op de standby-unit.

Om deze problemen op te lossen, geeft u **de opdracht wr** standby op de actieve eenheid.

## Fout:- %ASA-3-713063: IKE-peer adres niet geconfigureerd voor bestemming 0.0.0.0

### Probleem

**Het** **%ASA-3-713063: IKE-peer-adres dat niet is geconfigureerd voor de** foutmelding **bestemming 0.0.0** verschijnt en de tunnel kan niet worden geopend.

### Oplossing

Deze melding wordt weergegeven wanneer het IKE peer-adres niet geconfigureerd is voor een L2L-tunnel.

Deze fout kan worden opgelost als u het volgnummer van crypto map wijzigt, en vervolgens de crypto map verwijderen en opnieuw toepassen.

## Fout: %ASA-3-752006: Tunnel Manager heeft geen KEY_ACQUIRE-bericht verzonden.

### Probleem

De`%ASA-3-752006: Tunnel Manager heeft geen KEY_ACQUIRE-bericht verzonden.Mogelijke verkeerde configuratie van de crypto-kaart of tunnelgroep."`Foutmelding wordt aangemeld bij Cisco ASA.

### Oplossing

Deze foutmelding kan worden veroorzaakt door een onjuiste configuratie van de crypto map of tunnelgroep. Zorg ervoor dat beide op de juiste manier zijn geconfigureerd. Zie Fout 752006 voor meer informatie over deze foutmelding.

Dit zijn enkele van de corrigerende maatregelen:

- Verwijder de crypto-ACL (bijvoorbeeld gekoppeld aan de dynamische kaart).
- Verwijder eventueel ongebruikte IKEv2-configuratie.
- Controleer dat de crypto-ACL overeenkomt.
- Verwijder eventuele dubbele vermeldingen in toegangslijsten.

# Fout: %ASA-4-402116: IPSEC: Ontvangen van een ESP-pakket (SPI= 0x99554D4E, volgnummer= 0x9E) van XX.XX.XX.XX (gebruiker= XX.XX.XX.XX) naar YY.YY.YY.YY

Bij het opbouwen van een LAN-to-LAN VPN-tunnel wordt de volgende foutmelding weergegeven op een eind-ASA:

```
Het gedecapsuleerde binnenpakket komt niet overeen met het onderhandelde beleid in de SA.

Het pakket specificeert zijn bestemming als 10.32.77.67, zijn bron als 10.105.30.1, en zijn protocol als icmp.

De SA specificeert zijn lokale proxy als 10.32.77.67/255.255.255.255/ip/0 en zijn externe proxy als 10.105.42.192/255.255.255.224/ip/0.
```

## Oplossing

U moet de toegangslijsten voor interessant verkeer verifiëren die op beide einden van de VPN-tunnel zijn gedefinieerd. Beide moeten overeenkomen met exacte spiegelafbeeldingen.

# Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff

## Probleem

`Het installatieprogramma voor 64-bits VA kan niet worden gestart om de virtuele adapter in te schakelen als gevolg van de` melding `van fout 0`xffffflog die wordt ontvangen wanneer AnyConnect geen verbinding kan maken.

## Oplossing

Voer de volgende stappen uit om dit probleem op te lossen:

1. Ga **naar Systeem > Internet Communicatiebeheer > Internet Communicatie** instellingen en zorg ervoor **dat Automatische Root Certificaten** Update uitgeschakeld is.
2. Als deze optie is uitgeschakeld, schakelt u het **volledigeAdministratieve** Temperatuuronderdeel van de GPO uit die aan de betreffende machine is toegewezen en test u het opnieuw.

Zie Automatische rootcertificaten uitschakelen voor meer informatie.

# Cisco VPN-client werkt niet met datakaart op Windows 7

### Probleem

Cisco VPN-client werkt niet met datakaart op Windows 7.

### Oplossing

De Cisco VPN-client op Windows 7 werkt niet met 3G-verbindingen omdat VPN-clients op Windows 7 geen gegevenskaarten ondersteunen.

## Waarschuwing: "VPN-functionaliteit werkt misschien helemaal niet"

### Probleem

Tijdens pogingen om de isakmp op de buiteninterface van ASA in te schakelen, wordt dit waarschuwingsbericht ontvangen:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

Maak nu via ssh verbinding met de ASA. HTTPS is gestopt, en andere SSL-clients worden ook getroffen.

### Oplossing

Dit probleem is het gevolg van de geheugenvereisten van verschillende modules als logger en crypto.

Zorg ervoor dat u geen **wachtrij 0**opdracht hebt. Het maakt de wachtrijgrootte ingesteld op 8192 en de geheugentoewijzing wordt verhoogd.

In platforms zoals ASA5505 en ASA5510, heeft deze geheugentoewijzing de neiging om andere modules te verhongeren.

## IPSec Padding-foutmelding

### Probleem

De volgende foutmelding wordt ontvangen:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

### Oplossing

De kwestie komt voor omdat IPSec VPN zonder een knoeiboelalgoritme onderhandelt. Packet hash garandeert integriteitscontrole voor het ESP-kanaal.

Daarom worden misvormde pakketten zonder hash niet gedetecteerd door Cisco ASA en wordt geprobeerd deze pakketten te decoderen.

Aangezien deze pakketten echter misvormd zijn, vindt de ASA tekortkomingen tijdens pakketdecryptie. Dit veroorzaakt de getoonde padding-foutmeldingen.

U wordt aangeraden een hash-algoritme toe te voegen aan de transformatieset voor het VPN en ervoor te zorgen dat de link tussen de peers minieme pakketmisvorming heeft.

# VPN-tunnel wordt elke 18 uur verbroken

## Probleem

De VPN-tunnel wordt elke 18 uur verbroken ondanks dat de levensduur is ingesteld op 24 uur.

## Oplossing

De levensduur is de maximale tijd dat de SA kan worden gebruikt voor rekey. De waarde voor de levensduur die u invoert in de configuratie verschilt van de rekey-tijd van de SA.

Daarom is het noodzakelijk om voorafgaand aan het verstrijken van de huidige SA te onderhandelen over een nieuwe SA (of SA-paar in het geval van IPsec).

De rekey-tijd moet altijd kleiner zijn dan de levensduur, zodat er meerdere pogingen kunnen worden gedaan indien de eerste poging mislukt.

De RFC's specificeren niet hoe de rekey-tijd moet worden berekend. Dit wordt overgelaten aan het oordeel van de uitvoerders.

Daarom varieert de tijd met platform. Sommige implementaties kunnen een willekeurige factor gebruiken om de rekey-timer te berekenen.

Als de ASA de tunnel bijvoorbeeld initieert, is het normaal dat deze rekeys heeft bij 64800 seconden = 75% van de 86400.

Als de router initieert, dan kan ASA langer wachten om de peer meer tijd te geven om de sleutel te initiëren.

Het is dus normaal dat de VPN-sessie elke 18 uur wordt verbroken om een andere sleutel te gebruiken voor de VPN-onderhandeling. Dit mag geen VPN-uitval of -probleem veroorzaken.

# Verkeersstroom wordt onderbroken nadat LAN-naar-LAN-tunnel opnieuw is onderhandeld

## Probleem

De verkeersstroom wordt onderbroken nadat de LAN-to-LAN tunnel opnieuw is onderhandeld.

## Oplossing

ASA bewaakt elke verbinding die er doorheen loopt en onderhoudt een vermelding in de toestandstabel in overeenstemming met de toepassingsinspectiefunctie.

De details van het versleutelde verkeer dat door het VPN gaat, worden behouden in de vorm van een security koppeling (SA) database. Voor LAN-to-LAN VPN-verbindingen worden twee verschillende verkeersstromen onderhouden.

Eén van deze is het versleutelde verkeer tussen de VPN-gateways. De andere is de verkeersstroom tussen de netwerkbron achter de VPN-gateway en de eindgebruiker achter het andere einde.

Wanneer VPN wordt beëindigd, worden de verkeersstroomdetails voor deze specifieke SA verwijderd.

De vermelding in de toestandstabel die bijgehouden wordt door de ASA voor deze TCP-verbinding raakt echter vanwege het gebrek aan activiteit verouderd. Dit belemmert de download.

Dit betekent dat de ASA de TCP-verbinding voor die bepaalde stroom behoudt terwijl de gebruikersapplicatie wordt afgesloten.

De TCP-verbindingen raken echter verloren en uiteindelijk vervalt de time-out nadat de TCP-stootloze timer is verlopen.

Dit probleem is opgelost met de introductie van een functie genaamd **Persistente IPSec Tunneling Flows**.

Er is een nieuwe opdracht sysopt connection preserve-vpn-flows in Cisco ASA geïntegreerd om de toestandstabelinformatie te behouden bij het opnieuw onderhandelen van de VPN-tunnel.

Deze opdracht is standaard uitgeschakeld. Om dit in te schakelen, behoudt Cisco ASA de TCP-statustabelinformatie wanneer L2L VPN van de verstoring herstelt en de tunnel opnieuw instelt.

# Foutmelding dat limiet van bandbreedte voor Crypto-functionaliteit is bereikt

## Probleem

De volgende foutmelding wordt weergegeven op de 2900 Series router:

```
Fout: Mar 20 10:51:29: %CERM-4-TX_BW_limit: Maximale Tx Bandbreedtelimiet van 85000 Kbps bereikt voor Crypto functionaliteit met SecuritySwitch9 technologie pakket licentie.
```

## Oplossing

Dit is een bekend probleem dat zich voordoet vanwege de strenge richtlijnen die door de Amerikaanse regering zijn uitgevaardigd.

In overeenstemming hiermee kan de **security**k**9** licentie alleen een payload-encryptie tot snelheden van bijna 90 Mbps toestaan en het aantal versleutelde tunnels/TLS-sessies beperken tot het apparaat.

Raadpleeg Cisco ISR G2 SEC- en HSEC-licentiëring voor meer informatie over de exportbeperkingen van crypto.

Cisco-apparaten zijn ingesteld om unidirectioneel verkeer in of uit de ISR G2-router onder 85 Mbps te houden, met een bidirectioneel totaal van 170 Mbps.

Deze eis is van toepassing op Cisco 1900, 2900 en 3900 ISR G2-platforms. Deze opdracht helpt u deze

beperkingen te bekijken:

<#root>

```
Router#
```

**show platform cerm-information**

```
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)         85000                  85000
 Rx Bandwidth(in kbps)         85000                  85000
 Number of tunnels               225                    225
 Number of TLS sessions         1000                   1000
---Output truncated----
```

Om dit probleem te voorkomen, koop je een HSECK9 licentie. Een "hseck9" functielicentie biedt verbeterde functionaliteit voor payload-encryptie met hogere aantallen VPN-tunnels en beveiligde spraaksessies.

Raadpleeg Softwareactivering voor meer informatie over Cisco ISR-routerlicenties.

# Probleem: Uitgaand encryptieverkeer in een IPsec-tunnel mislukt, zelfs als inbound decryptie-verkeer werkt.

## Oplossing

Dit probleem is waargenomen bij een IPsec-verbindingen na meerdere rekeys, maar de trigger of oorzaak is onbekend.

De aanwezigheid van dit probleem kan worden vastgesteld als u de uitvoer van **de** opdracht **automatisch** versturen controleert en controleert dat de teller Verlopen VPN-context toeneemt voor elk verzonden pakket.

# Diversen

## AG_INIT_EXCH-melding wordt weergegeven in de output voor de opdrachten "show crypto isakmp sa" en "debug"

Als de tunnel niet geïnitieerd wordt, verschijnt **hetAG_INIT**_EXCH bericht in output van **de hoe crypto isakmp** opdracht en indexoutput eveneens.

De reden kan zijn als gevolg van een wanverhouding van de isakmp beleid of als port udp 500 wordt geblokkeerd op de weg.

## Debug-melding "Received an IPC message during invalid state" wordt weergegeven

Dit is een informatief bericht en heeft niets te maken met het verbreken van de VPN-tunnel.

## Gerelateerde informatie

- **ASA en Cisco IOS®: VPN-fragmentatie**
- **Cisco ASA 5500 Series security applicaties**
- **IPsec-onderhandeling/IKE-protocollen**
- **Technische ondersteuning en documentatie â€“ 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.