# Configuratie- en probleemoplossing van Cisco Network-Layer Encryption: Achtergrond - Deel 1

## Inhoud



# Inleiding

Dit document behandelt het configureren en oplossen van Cisco-netwerklaagencryptie met IPSec en Internet Security Association en Key Management Protocol (ISAKMP) en bestrijkt achtergrondinformatie en basisconfiguratie met IPSec en ISAKMP.

# Voorwaarden

## Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de software- en hardwareversies:

- Cisco IOS® softwarerelease 11.2 en hoger

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

## Conventies

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

# Background-informatie en -configuratie van netwerklaag

De functie Network-Layer Encryption is geïntroduceerd in Cisco IOS® softwarerelease 11.2. Het biedt een mechanisme voor beveiligde gegevensoverdracht en bestaat uit twee componenten:

- **Routerverificatie:** Alvorens gecodeerd verkeer over te gaan, voeren twee routers een eenmalige, tweevoudige authenticatie uit met behulp van DSS (Digital Signature Standard)-toetsen om willekeurige uitdagingen te tekenen.
- **Encryptie van netwerklaag:** Voor IP-payload-encryptie gebruiken de routers de uitwisseling van Diffie-Hellman om veilig een DES (40- of 56-bits sessiesleutel), Triple DES - 3DES (168-bits) of de meer recente Advanced Encryption Standard - AES (128-bits (standaard) of 192-bits of 256-bits toets) te genereren, geïntroduceerd in 1 2.2(13)T. Nieuwe sessies worden op een configureerbare basis gegenereerd. Het beleid van de encryptie wordt ingesteld door crypto-kaarten die uitgebreide IP toegangslijsten gebruiken om te bepalen welke netwerk, net, host, of protocol paren tussen routers moeten worden versleuteld.

## Background van cryptografie

Het terrein van de cryptografie heeft betrekking op het privé houden van communicatie. De bescherming van gevoelige communicatie is gedurende een groot deel van zijn geschiedenis de nadruk geweest op cryptografie. Encryptie is de transformatie van gegevens in een onleesbare vorm. Het doel is de privacy te verzekeren door de informatie verborgen te houden voor iedereen voor wie het niet bedoeld is, zelfs als ze de gecodeerde gegevens kunnen zien. Decryptie is het omgekeerde van encryptie: het is de omzetting van gecodeerde gegevens in een begrijpelijke vorm .

Versleuteling en decryptie vereisen het gebruik van bepaalde geheime informatie, gewoonlijk een "sleutel" genoemd. Afhankelijk van het gebruikte encryptiemechanisme kan dezelfde toets worden gebruikt voor zowel encryptie als decryptie; hoewel voor andere mechanismen , kunnen de sleutels die gebruikt worden voor encryptie en decryptie verschillend zijn .

Een digitale handtekening bindt een document aan de bezitter van een bepaalde sleutel, terwijl een digitale tijdstempel een document aan zijn creatie op een bepaald moment bindt. Deze cryptografische mechanismen kunnen worden gebruikt om de toegang tot een gedeeld diskstation, een hoge-beveiligingsinstallatie of een betaalbaar televisiekanaal te regelen.

Hoewel moderne cryptografie steeds diverser wordt, is cryptografie fundamenteel gebaseerd op moeilijk op te lossen problemen. Een probleem kan moeilijk zijn omdat de oplossing ervan vereist dat u de sleutel kent, zoals het decrypteren van een versleuteld bericht of het ondertekenen van een digitaal document. Het probleem kan ook moeilijk zijn, omdat het intrinsiek moeilijk te voltooien is, zoals het vinden van een boodschap die een bepaalde hashwaarde veroorzaakt.

Nu het terrein van de cryptografie is geavanceerd, zijn de scheidslijnen voor wat is en wat niet cryptografie is, vervaagd. Cryptografie vandaag de dag kan worden samengevat als de studie van technieken en toepassingen die afhangen van het bestaan van wiskundige problemen die moeilijk op te lossen zijn. Een cryptoanalyst probeert cryptografische mechanismen in gevaar te brengen, en cryptologie is de discipline van cryptografie en cryptoanalyse gecombineerd.

## Definities

In deze sectie worden de betreffende termen gedefinieerd die in dit document worden gebruikt.

- **Verificatie:** De eigendom van het weten dat de ontvangen gegevens daadwerkelijk door de beweerde afzender worden verzonden.
- **Vertrouwelijkheid:** De eigenschap van de communicatie zodat de bedoelde ontvangers weten wat er wordt verzonden, maar onbedoelde partijen kunnen niet bepalen wat er wordt verzonden.
- **Data Encryption Standard (DES):** DES gebruikt een symmetrische sleutelmethode, ook bekend als een geheime sleutelmethode. Dit betekent dat als een blok gegevens versleuteld is met de sleutel, het gecodeerde blok met dezelfde sleutel moet worden gedecrypteerd, zodat zowel de encryptieapparaat als de decrypter dezelfde toets moeten gebruiken. Hoewel de versleutelingsmethode bekend is en goed wordt gepubliceerd, is de bekendste methode van de aanslag gebaseerd op brute kracht. De sleutels moeten worden getest tegen de gecodeerde blokken om te zien of ze op de juiste manier kunnen worden opgelost. Naarmate processoren sterker worden, nadert de natuurlijke levensduur van DES zijn einde. Een gecoördineerde inspanning met reserveverwerkingskracht van duizenden computers op het internet kan bijvoorbeeld de 56-bits toets naar een DES-gecodeerd bericht in 21 dagen vinden.DES wordt om de vijf jaar door de National Security Agency (NSA) van de VS gevalideerd om te voldoen aan de doelstellingen van de Amerikaanse regering. De huidige goedkeuring verstrijkt in 1998 en de NSA heeft aangegeven dat zij DES niet opnieuw zal certificeren. Verder dan DES zijn er andere encryptie-algoritmen die ook geen bekende zwakheden hebben, behalve brute krachtaanvallen. Voor meer informatie, zie DES FIPS 46-2 door het National Institute of Standards and Technology (NIST) .
- **decryptie:** De omgekeerde toepassing van een encryptie algoritme op gecodeerde gegevens, waarbij die gegevens in zijn oorspronkelijke, niet gecodeerde staat worden hersteld.
- **DSS- en digitale signaalalgoritme (DSA):** Het DSA werd gepubliceerd door NIST in het Digital Signature Standard (DSS), een onderdeel van het Capstone-project van de Amerikaanse overheid. DSS werd geselecteerd door NIST, in samenwerking met de NSA, om de digitale authenticatienorm van de Amerikaanse overheid te zijn. De standaard werd uitgegeven op 19 mei 1994.
- **Encryptie:** De toepassing van een specifiek algoritme op gegevens om het uiterlijk van de gegevens te wijzigen, waardoor het onbegrijpelijk wordt voor degenen die niet gemachtigd zijn de informatie te zien.
- **Integriteit:** Het vermogen om ervoor te zorgen dat de gegevens van bron naar bestemming zonder onherkende wijziging worden doorgegeven.

- **Niet-verwerping:** Het bezit van een ontvanger die kan bewijzen dat de afzender van bepaalde gegevens de gegevens in feite heeft verzonden, ook al zou de afzender later kunnen ontkennen dat hij die gegevens heeft verzonden.
- **Publieke sleutelcryptografie:** Traditionele cryptografie is gebaseerd op de zender en de ontvanger van een bericht met dezelfde geheime sleutel. De afzender gebruikt de geheime sleutel om het bericht te versleutelen, en de ontvanger gebruikt dezelfde geheime sleutel om het bericht te decrypteren. Deze methode staat bekend als "geheime sleutel" of "symmetrische cryptografie." Het belangrijkste is dat de zender en de ontvanger het eens worden over de geheime sleutel zonder dat iemand anders dat weet. Als ze op verschillende fysieke locaties liggen, moeten ze vertrouwen op een koerier, een telefoonsysteem of een ander transmissiemiddel om te voorkomen dat er informatie over de geheime sleutel wordt verspreid. Iedereen die de sleutel in het douanevervoer overneemt of onderschept kan later alle berichten lezen, wijzigen en vervalsen versleuteld of geauthentiseerd met behulp van die sleutel. De opwekking, transmissie en opslag van sleutels wordt sleutelbeheer genoemd; alle cryptosystemen moeten zich bezighouden met essentiële beheerskwesties . Omdat alle sleutels van een geheim sleutelcryptosysteem geheim moeten blijven, heeft geheime sleutelcryptografie vaak moeite met het leveren van veilig sleutelbeheer, vooral in open systemen met een groot aantal gebruikers.Het concept van cryptografie van de openbare sleutel werd in 1976 geïntroduceerd door Whitfield Diffie en Martin Hellman om het belangrijkste beheersprobleem op te lossen. In hun concept krijgt elke persoon een paar sleutels, de ene heet de publieke sleutel en de andere de private sleutel. De openbare sleutel van iedere persoon wordt gepubliceerd terwijl de particuliere sleutel geheim wordt gehouden. De noodzaak voor de afzender en de ontvanger om geheime informatie te delen wordt weggenomen en alle communicatie omvat alleen openbare sleutels, en er wordt nooit een particuliere sleutel verzonden of gedeeld. Het is niet langer nodig om een of ander communicatiekanaal te vertrouwen om veilig te zijn voor afluisteren of verraad. Het enige vereiste is dat de toetsen van het publiek op een vertrouwde (geauthentiseerde) manier met hun gebruikers worden geassocieerd (bijvoorbeeld in een vertrouwde folder). Iedereen kan een vertrouwelijke boodschap sturen door gebruik te maken van openbare informatie, maar de boodschap kan alleen worden decrypteerd met een private sleutel, die in het enige bezit is van de beoogde ontvanger. Bovendien kan de cryptografie van de openbare sleutel niet alleen gebruikt worden voor privacy (encryptie), maar ook voor authenticatie (digitale handtekeningen).
- **Publieke belangrijkste digitale handtekeningen:** Om een bericht te tekenen, voert een persoon een berekening uit met zowel hun privé sleutel als de boodschap zelf. De uitvoer wordt de digitale handtekening genoemd en wordt aan het bericht toegevoegd, dat vervolgens wordt verzonden. Een tweede persoon verifieert de handtekening door een berekening uit te voeren met betrekking tot het bericht, de vermeende handtekening en de publieke sleutel van de eerste persoon. Indien het resultaat naar behoren in een eenvoudige wiskundige relatie blijft, wordt de handtekening als echt beschouwd. Anders kan de handtekening frauduleus zijn of kan het bericht gewijzigd zijn.
- **Openbare sleutel:** Wanneer een persoon een geheim bericht naar een andere persoon wil sturen, kijkt de eerste persoon op de openbare sleutel van de tweede persoon in een folder, gebruikt deze om het bericht te versleutelen en het uit te sturen. De tweede persoon gebruikt dan hun privé sleutel om het bericht te decrypteren en het te lezen. Niemand die luistert kan de boodschap ontcijferen. Iedereen kan een versleuteld bericht naar de tweede sturen, maar alleen de tweede persoon kan het lezen. Eén vereiste is duidelijk dat niemand de private sleutel kan uitzoeken uit de corresponderende publieke sleutel.

- **Verkeersanalyse:** De analyse van netwerkverkeersstromen met het oog op het afleiden van informatie die nuttig is voor een tegenstander. Voorbeelden van dergelijke informatie zijn de frequentie van de transmissie, de identiteit van de conversiende partijen, de omvang van de pakketten, de gebruikte stroomidentificatoren, enz.

## Voorlopige informatie

In dit gedeelte worden enkele basisconcepten voor Network-Layer Encryption besproken. Het bevat de aspecten van encryptie waar je op moet letten. Aanvankelijk zijn deze kwesties voor u misschien niet logisch, maar het is een goed idee om ze nu te lezen en ze te kennen, omdat ze zinvoller zullen zijn nadat u een paar maanden met encryptie hebt gewerkt.

- Het is belangrijk om op te merken dat encryptie alleen op de uitvoer van een interface voorkomt en dat decryptie uitsluitend bij invoer naar de interface plaatsvindt. Dit onderscheid is belangrijk bij het uitstippelen van uw beleid. Het beleid voor encryptie en decryptie is symmetrisch. Dit betekent dat het definiëren van de ene je de andere automatisch geeft. Met de crypto kaarten en hun bijbehorende uitgebreide toegangslijsten wordt alleen het encryptiebeleid expliciet gedefinieerd.Het decryptiebeleid gebruikt de identieke informatie, maar wanneer het overeenkomende pakketten, keert het bron en bestemmingsadressen en havens om. Op deze manier worden de gegevens in beide richtingen van een duplexverbinding beschermd. De opdracht *matchadres x* ***statement in de crypto map*** wordt gebruikt om pakketten te beschrijven die een interface verlaten. Met andere woorden, het beschrijft de encryptie van pakketten. Packet moeten echter ook voor decryptie worden aangepast wanneer ze de interface binnendringen. Dit gebeurt automatisch door de toegangslijst te verplaatsen met de bron- en doeladressen en omgekeerde poorten. Dit levert symmetrie op voor de verbinding. De toegangslijst waarop de **crypto-kaart** wijst, dient alleen verkeer in één (uitgaande) richting te beschrijven. IP-pakketten die niet overeenkomen met de toegangslijst die u definieert, worden verzonden maar niet versleuteld. Een "ontkennen" in de toegangslijst geeft aan dat deze hosts niet gematcht moeten worden, wat betekent dat ze niet versleuteld zullen worden. In deze context betekent "ontkennen" niet dat het pakje wordt ingetrokken.
- Wees heel voorzichtig met het woord 'elk' in uitgebreide toegangslijsten. Wanneer u "een" gebruikt, wordt uw verkeer verbroken, tenzij het naar de bijbehorende "niet-versleutelde" interface gaat. Bovendien is, met de IPSec in Cisco IOS-softwarerelease 11.3(3)T, 'geen' toegestaan.
- Het gebruik van "om het even welk"sleutelwoord wordt ontmoedigd in het specificeren van bron of bestemmingsadressen. Het specificeren van "elk" kan problemen veroorzaken met het routeren van protocollen, Network Time Protocol (NTP), echo, echo reactie, en multicast verkeer, aangezien de ontvangende router dit verkeer in stilte wegwijst. Als "enige" gebruikt moet worden, moet deze worden voorafgegaan door "ontkennen" statements die niet versleuteld worden, zoals "ntp".
- Om tijd te besparen, zorg ervoor dat u de peer router kunt **pingelen** waarmee u een encryptie associatie probeert te hebben. Ook, hebben de eindapparaten (die van het krijgen van hun verkeer afhangen) elkaar geworteld alvorens u te veel tijd besteed aan het oplossen van het verkeerde probleem. Met andere woorden, zorg dat het routingwerk werkt voordat u probeert **crypto** te doen. De externe peer heeft mogelijk geen route voor de spanning-interface. In dat geval hebt u geen encryptie-sessie met die peer (u kunt **ip ongenummerd** gebruiken op die seriële interface).

- Veel WAN-point-to-point links gebruiken niet-routeerbare IP-adressen en Cisco IOS-softwarerelease 11.2 Encryptie is gebaseerd op Internet Control Message Protocol (ICMP) (wat betekent dat het IP-adres van de seriële interface voor ICMP gebruikt). Dit kan u dwingen om **ip ongenummerd** op de WAN-interface te gebruiken. Voer altijd een **pingelen** en **traceroute** opdracht uit om te verzekeren dat de routing op zijn plaats is voor de twee peerende (encryptie/decryptie) routers.
- Slechts twee routers mogen een Diffie-Hellman sessiesleutel delen. Met andere woorden, één router kan versleutelde pakketten niet met twee peers uitwisselen via dezelfde sessiesleutel. elk paar routers moet een sessiesleutel hebben die het resultaat is van een Diffie-Hellman uitwisseling tussen hen.
- De crypto-motor is ofwel in Cisco IOS, de VIP2 Cisco IOS, of in hardware de Encryption Services adapter (ESA) op VIP2. Zonder VIP2 bestuurt de Cisco IOS crypto-motor encryptiebeleid op alle poorten. Op platforms die VIP2 gebruiken, zijn er meerdere cryptomotoren: één in Cisco IOS, en één op elke VIP2. De crypto motor op een VIP2 beheerst encryptie op de havens die op het bord wonen.
- Zorg ervoor dat het verkeer is ingesteld om op een interface te arriveren die is bereid om het te versleutelen. Als het verkeer op een of andere manier op een andere interface kan aankomen dan het verkeer met een **crypto-kaart** toegepast, wordt het stilletjes laten vallen.
- Het helpt om troost (of afwisselende) toegang tot beide routers te hebben wanneer het zeer belangrijk ruilt; het is mogelijk om de passieve kant op te hangen terwijl ze op een sleutel wacht .
- De **cfb-64** is efficiënter te verwerken dan **cfb-8** wat betreft de CPU-belasting.
- De router moet het algoritme draaien dat u wilt gebruiken met de algoritme-feedback (CFB) die u wilt gebruiken; De standaardinstellingen voor elke afbeelding zijn de naam van de afbeelding (zoals "56") met **cfb-64**.
- Overweeg het wijzigen van de key-timeout. Het standaard 30 minuten is erg kort. Probeer het op één dag te brengen (1440 minuten).
- IP-verkeer wordt verbroken tijdens belangrijke heronderhandeling telkens wanneer de toets verstrijkt.
- Selecteer alleen het verkeer dat u echt wilt versleutelen (hiermee worden CPU-cycli opgeslagen).
- Met dial-on-demand routing (DDR) maakt ICMP interessant of deze zal nooit uitbellen.
- Als u ander verkeer dan IP wilt versleutelen, gebruikt u een tunnel. Gebruik met tunnels de crypto kaarten op zowel de fysieke als tunnelinterfaces. Zie voorbeeld 5: Versleuteling van IPX-verkeer in een IP-tunnels voor meer informatie.
- De twee routers van coderingsgelijken hoeven niet rechtstreeks te worden aangesloten.
- Een router met een lage temperatuur kan u een "CPU-melding" geven. Dit kan worden genegeerd omdat het u vertelt dat encryptie veel CPU-middelen gebruikt.
- Plaats versleutelde routers niet redundante zodat u het verkeer en de afvalCPU ontsleutelt en opnieuw versleutelt. Eenvoudig versleutelen op de twee eindpunten. Zie monster 3: Encryptie naar en door een router voor meer informatie.
- Op dit moment wordt encryptie van broadcast- en multicast-pakketten niet ondersteund. Als "veilig" routingupdates belangrijk zijn voor een netwerkontwerp, zou een protocol met ingebouwd authenticatie moeten worden gebruikt, zoals het Enhanced Interior Gateway Routing Protocol (DHCP), Open Shortest Path First (OSPF) of Routing Information Protocol versie 2 (RIPv2) om update integriteit te verzekeren.

## Caveats

**N.B.:** De hieronder genoemde voorbehouden zijn allemaal opgelost.

- Een Cisco 7200-router die een ESA voor encryptie gebruikt, kan een pakket onder één sessiesleutel niet decrypteren en het dan opnieuw versleutelen onder een andere sessiesleutel. Raadpleeg Cisco bug-ID CSCdj82613 (alleen geregistreerde klanten).
- Wanneer twee routers worden aangesloten door een versleutelde huurlijn en een ISDN-reservelijn, als de huurlijn zakt, wordt de ISDN-verbinding fijn gemaakt. Wanneer de huurlijn echter opnieuw verschijnt, is de router die de ISDN-aanroep plaatste, ingestort. Raadpleeg Cisco bug-ID CSCdj0310 (alleen geregistreerde klanten).
- Voor Cisco 7500 Series routers met meerdere VIP's, als een **crypto-kaart** wordt toegepast op zelfs één interface van een VIP, een of meer VIP's-crash. Raadpleeg Cisco bug-ID CSCdi8459 (alleen geregistreerde klanten).
- Voor Cisco 7500 Series routers met een VIP2 en ESA, geeft de opdracht Crypto-kaart niet uitvoer weer tenzij de gebruiker zich op de console poort bevindt. Raadpleeg Cisco bug-ID CSCdj89070 (alleen geregistreerde klanten).

# Cisco IOS-encryptie van netwerklaag

De werkende steekproef van Cisco IOS configuraties in dit document kwam direct van laboratoriumrouters. De enige wijziging was het verwijderen van niet-verbonden interfaceconfiguraties. Al het materiaal hier kwam van vrij beschikbare bronnen op het internet of in het Gerelateerde Informatie gedeelte aan het eind van dit document.

Alle voorbeeldconfiguraties in dit document zijn van Cisco IOS-softwarerelease 11.3. Er zijn verschillende veranderingen geweest van de opdrachten van Cisco IOS-softwarerelease 11.2, zoals de toevoeging van de volgende woorden:

- dss in enkele van de belangrijkste configuratieopdrachten.
- cisco in sommige van de **show** opdrachten en de opdrachten **crypto map** om onderscheid te maken tussen de eigen encryptie van Cisco (zoals gevonden in Cisco IOS-softwarerelease 11.2 en hoger) en IPSec dat zich in Cisco IOS-softwarerelease 11.3(2)T bevindt.

**Opmerking:** De IP-adressen die in deze configuratievoorbeelden worden gebruikt, zijn willekeurig gekozen in het lab van Cisco en zijn bedoeld om volledig generiek te zijn.

## Stap 1: DSS-hoofdparen handmatig genereren

Een DSS-sleutelpaar (een openbare en privé-toets) moet handmatig worden gegenereerd op elke router die aan de coderingssessie deelneemt. Met andere woorden, elke router moet zijn eigen DSS toetsen hebben om deel te kunnen nemen. Een coderingsmotor kan slechts één DSS-toets hebben die het uniek identificeert. Het sleutelwoord "dss" werd toegevoegd in Cisco IOS-softwarerelease 11.3 om DSS van RSA-toetsen te onderscheiden. U kunt een naam voor de eigen DSS-toetsen van de router specificeren (hoewel het aangeraden wordt om de router hostname te gebruiken). Op een minder krachtige CPU (zoals de Cisco 2500-serie) duurt de generatie van sleutelparen ongeveer 5 seconden of minder.

De router genereert een paar toetsen:

- Een openbare sleutel (die later wordt verzonden naar routers die deelnemen aan coderingssessies).

- Een privésleutel (die niet met iemand anders wordt gezien of uitgewisseld); In feite wordt het opgeslagen in een afzonderlijk gedeelte van NVRAM dat niet kan worden bekeken).

Nadat het DSS-toetsenbord van de router is gegenereerd, wordt het uniek geassocieerd met de crypto-motor in die router. Belangrijkste paargeneratie wordt in de onderstaande voorbeeldopdrachtoutput weergegeven.

```
dial-5(config)#crypto key generate dss dial5
Generating DSS keys ....
 [OK]

dial-5#show crypto key mypubkey dss
crypto public-key dial5 05679919
 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
 F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
quit


dial-5#show crypto engine configuration
slot:                0
engine name:         dial5
engine type:         software
serial number:       05679919
platform:            rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    43
input queue bot:    43
input queue count:  0

dial-5#
```

Omdat u slechts één zeer belangrijk paar kunt genereren dat de router identificeert, kunt u uw originele sleutel overschrijven en uw openbare sleutel met elke router in de encryptie associatie opnieuw verzenden. Dit wordt weergegeven in de onderstaande voorbeeldopdrachtoutput:

```
StHelen(config)#crypto key generate dss barney
% Generating new DSS keys will require re-exchanging
   public keys with peers who already have the public key
   named barney!
Generate new DSS keys? [yes/no]: yes
Generating DSS keys ....
 [OK]


StHelen(config)#
Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

## Stap 2: Handmatig DSS-openbare toetsen met peers (out-of-band) ruilen

Het genereren van het eigen DSS-sleutelpaar van de router is de eerste stap in het vestigen van een encryptiesessie associatie. De volgende stap is om openbare sleutels met elke andere router uit te wisselen. U kunt deze openbare toetsen handmatig invoeren door eerst de opdracht **Show crypto mypubkey** in te voeren om de openbare DSS-toets van de router weer te geven. U wisselt dan deze openbare sleutels uit (via e-mail, bijvoorbeeld) en, met de **crypto belangrijkste pubkey-chain dss** opdracht, snijd en plak de openbare sleutel van uw peer router in de router.

U kunt ook de **opdracht Crypto-toets gebruiken** om de routers automatisch te laten uitwisselen

openbare toetsen. Als u de geautomatiseerde methode gebruikt, zorg er dan voor dat er geen **crypto kaart** statements zijn die gebruikt worden voor de sleuteluitwisseling. Een **debug-cryptotoets** is hier handig.

**Opmerking:** het is een goed idee om je peer **te** pingelen voordat je probeert om sleutels uit te wisselen.

```
Loser#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!

Loser(config)#crypto key exchange dss passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]
Waiting ....


  StHelen(config)#crypto key exchange dss 19.19.19.19 barney
  Public key for barney:
  Serial Number 05694352
  Fingerprint   309E D1DE B6DA 5145 D034

  Wait for peer to send a key[confirm]


Public key for barney:
   Serial Number 05694352
   Fingerprint   309E D1DE B6DA 5145 D034

Add this public key to the configuration? [yes/no]:yes


         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.


Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes.
Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes.

Send peer a key in return[confirm]
Which one?

fred? [yes]:
Public key for fred:
   Serial Number 02802219
   Fingerprint   2963 05F9 ED55 576D CF9D


         Waiting ....
         Public key for fred:
           Serial Number 02802219
         Fingerprint   2963 05F9 ED55 576D CF9D
```

```
        Add this public key to the configuration? [yes/no]:

Loser(config)#
Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.
Loser(config)#

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
Add this public key to the configuration? [yes/no]: yes
StHelen(config)#^Z
StHelen#
```

Nu de openbare DSS-toetsen zijn uitgewisseld, moet u ervoor zorgen dat beide routers elkaars openbare toetsen hebben en dat ze overeenkomen, zoals in de onderstaande opdrachtoutput wordt weergegeven.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit

Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

--------

StHelen#show crypto key mypubkey dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

## Steekproef 1: Cisco IOS-configuratie voor speciale link

Nadat de DSS-toetsen op elke router zijn gegenereerd en de DSS-openbare toetsen zijn uitgewisseld, kan de opdracht **Encrypto map** op de interface worden toegepast. De crypto sessie begint met het genereren van verkeer dat overeenkomt met de toegangslijst die gebruikt wordt door de crypto kaarten.

```
Loser#write terminal
Building configuration...
```

```
Current configuration:
!
! Last configuration change at 13:01:18 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
crypto map oldstyle 10
 set peer barney
 match address 133
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
   732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
  quit
!
interface Ethernet0
 ip address 40.40.40.41 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 2400
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.20
access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
-------------------------
```

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:03:05 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
crypto map oldstyle 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
   C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
  quit
 !
 !
interface Ethernet0
 ip address 30.30.30.31 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 encapsulation x25
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 compress stac
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.19
access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
```

```
line vty 0 4
 password ww
 login
!
end

StHelen#
```

## Steekproef 2: Cisco IOS-configuratie voor multipoint Frame Relay

De volgende voorbeeldopdrachtoutput is van de HUB router genomen.

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 10:45:20 UTC Wed Mar 11 1998
! NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
!
crypto map oldstuff 10
 set peer barney
 match address 133
crypto map oldstuff 20
 set peer wilma
 match address 144
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
   D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D
  quit
 named-key wilma
  serial-number 01496536
  key-string
   C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70 7B29279C
   E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939
  quit
!
crypto cisco pregen-dh-pairs 5
!
crypto cisco key-timeout 1440
!
interface Ethernet0
 ip address 190.190.190.190 255.255.255.0
 no ip mroute-cache
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
```

```
 encapsulation frame-relay
 no ip mroute-cache
 clockrate 500000
 crypto map oldstuff
!
!
ip default-gateway 10.11.19.254
ip classless
ip route 200.200.200.0 255.255.255.0 19.19.19.20
ip route 210.210.210.0 255.255.255.0 19.19.19.21
access-list 133 permit ip 190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255
access-list 144 permit ip 190.190.190.0 0.0.0.255 210.210.210.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
```

De volgende voorbeeldopdrachtoutput is afkomstig van Remote Site A.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
 set peer fred
 match address 133
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 210.210.210.210 255.255.255.0
 shutdown
!
interface Serial0
 ip address 19.19.19.21 255.255.255.0
 encapsulation frame-relay
 no fair-queue
 crypto map mymap
```

```
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line 1
 no exec
 transport input all
line 2 16
 no exec
line aux 0
line vty 0 4
 password ww
 login
!
end

WAN-2511a#
```

De volgende voorbeeldopdrachtoutput is afkomstig van Remote Site B.

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 19:00:34 UTC Tue Mar 10 1998
! NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 200.200.200.200 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation frame-relay
```

```
 no ip mroute-cache
 crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

De volgende voorbeeldopdrachtoutput is afkomstig van de Frame Relay switch.

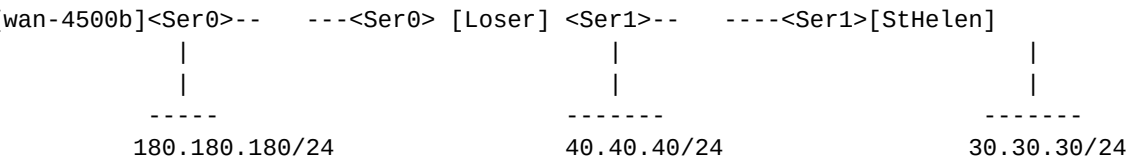
```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

## Steekproef 3: Encryptie naar en via een router

Peer routers hoeven niet één hop weg te zijn. U kunt een sessie maken met een externe router. In het volgende voorbeeld is het doel om al netwerkverkeer tussen 180.180.180.0/24 en

40.40.40.0/24 en tussen 180.180.180.0/24 en 30.30.30.0/24 te versleutelen. Er is geen zorg om verkeer tussen 40.40.40.0/24 en 30.30.30.0/24 te versleutelen.

De router wan-4500b heeft een coderingssessie met Loser en ook SintHelen. Door het verkeer te versleutelen van het Ethernet-segment van wan-4500b naar het Ethernet-segment van StHelen vermijdt u de onnodige decryptie stap bij Loser. Loser geeft het gecodeerde verkeer door naar StHelen's seriële interface, waar het gedecrypteerd wordt. Dit vermindert de verkeersvertraging voor de IP-pakketten en de CPU-cycli op de routergebruiker Loser. Belangrijker nog is dat het de beveiliging van het systeem aanzienlijk verhoogt, aangezien een afluisteraar bij Loser het verkeer niet kan lezen. Als Loser het verkeer zou decrypteren, zou er een kans zijn dat de ontcijferde gegevens worden afgeleid.




```
wan-4500b#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname wan-4500b
!
enable password 7 111E0E
!
username cse password 0 ww
no ip domain-lookup
!
crypto map toworld 10
 set peer loser
 match address 133
crypto map toworld 20
 set peer sthelen
 match address 144
!
crypto key pubkey-chain dss
 named-key loser
  serial-number 02802219
  key-string
   F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
   6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
  quit
 named-key sthelen
  serial-number 05694352
  key-string
   5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
   A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
  quit
 !
interface Ethernet0
 ip address 180.180.180.180 255.255.255.0
!
interface Serial0
 ip address 18.18.18.19 255.255.255.0
 encapsulation ppp
```

```
 crypto map toworld
!
router rip
 network 18.0.0.0
 network 180.180.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.31
ip route 171.68.118.0 255.255.255.0 10.11.19.254
access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255
access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 044C1C
line vty 0 4
 login local
!
end

wan-4500b#

--------------------

Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:01:54 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
ip host StHelen.cisco.com 19.19.19.20
ip domain-name cisco.com
!
crypto map towan 10
 set peer wan
 match address 133
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
```

```
 encapsulation ppp
 no ip mroute-cache
 clockrate 64000
 crypto map towan
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 priority-group 1
 clockrate 64000
!
!
router rip
 network 19.0.0.0
 network 18.0.0.0
 network 40.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#

-------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:13:18 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map towan 10
 set peer wan
 match address 144
!
crypto key pubkey-chain dss
 named-key wan
```

```
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 no ip address
!
interface Ethernet1
 ip address 30.30.30.30 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 crypto map towan
!
router rip
 network 30.0.0.0
 network 19.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#

--------------------------

wan-4500b#show crypto cisco algorithms
  des cfb-64
  40-bit-des cfb-64

wan-4500b#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

wan-4500b#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 0

wan-4500b#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         18.18.18.19 set    DES_56_CFB64    1683     1682
 5    Serial0         18.18.18.19 set    DES_56_CFB64    1693     1693

wan-4500b#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.19   52
wan-4500b#show crypto engine configuration
slot:               0
engine name:        wan
engine type:        software
```

```
serial number:      07365004
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    303
input queue bot:    303
input queue count:  0

wan-4500b#show crypto key mypubkey dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

wan-4500b#show crypto key pubkey-chain dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit

wan-4500b#show crypto map interface serial 1
No crypto maps found.

wan-4500b#show crypto map
Crypto Map "toworld" 10 cisco
        Connection Id = 1        (1 established,    0 failed)
        Peer = loser
        PE = 180.180.180.0
        UPE = 40.40.40.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 40.40.40.0/0.0.0.255

Crypto Map "toworld" 20 cisco
        Connection Id = 5        (1 established,    0 failed)
        Peer = sthelen
        PE = 180.180.180.0
        UPE = 30.30.30.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255

wan-4500b#

--------------------------

Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8

Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 61   Serial0         18.18.18.18 set    DES_56_CFB64    1683     1682

Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.18   1
Serial1              19.19.19.19   90
Loser#show crypto engine configuration
slot:               0
engine name:        loser
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    235
input queue bot:    235
input queue count:  0

Loser#show crypto key mypubkey dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit

Loser#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

Loser#show crypto map interface serial 1
No crypto maps found.

Loser#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 61       (0 established,    0 failed)
        Peer = wan
        PE = 40.40.40.0
        UPE = 180.180.180.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

Loser#

----------------------------------------

StHelen#show crypto cisco algorithms
  des cfb-64

StHelen#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

StHelen#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

StHelen#show crypto engine connections active
```

```
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 58   Serial1         19.19.19.20 set    DES_56_CFB64    1694     1693

StHelen#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Ethernet0            0.0.0.0       1
Serial1              19.19.19.20   80
StHelen#show crypto engine configuration
slot:               0
engine name:        sthelen
engine type:        software
serial number:      05694352
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    220
input queue bot:    220
input queue count:  0

StHelen#show crypto key mypubkey dss
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

StHelen#show crypto map interface serial 1
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#
```

## Steekproef 4: Crypto met DDR

Omdat Cisco IOS van ICMP afhankelijk is om encryptiesessies in te stellen, moet ICMP-verkeer als "interessant" in de dialerlijst worden geclassificeerd wanneer u encryptie via een DDR-link doet.

**Opmerking:** compressie werkt wel in Cisco IOS-softwarerelease 11.3, maar is niet erg gebruikersvol voor versleutelde gegevens. Omdat de gecodeerde gegevens vrij willekeurig zijn, vertraagt compressie alleen dingen. Maar u kunt de functie inschakelen voor niet-versleuteld verkeer.

In sommige situaties, zult u steun van de wijzerplaat aan de zelfde router willen. Het is bijvoorbeeld nuttig wanneer gebruikers tegen het falen van een bepaalde link in hun WAN-netwerken willen beschermen. Als twee interfaces naar dezelfde peer gaan, kan dezelfde crypto kaart op beide interfaces worden gebruikt. De back-upinterface moet worden gebruikt zodat deze optie correct werkt. Als een reservekopie ontwerp een routerknop in een ander vak heeft, moeten er verschillende crypto-kaarten worden gemaakt en moeten de peers dienovereenkomstig worden ingesteld. Opnieuw dient de **back-**upinterface-opdracht te worden gebruikt.

```
dial-5#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-5
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10
!
username dial-6 password 0 cisco
isdn switch-type basic-ni1
!
crypto map dial6 10
 set peer dial6
 match address 133
!
crypto key pubkey-chain dss
 named-key dial6
  serial-number 05679987
  key-string
   753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82
   2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 ip address 10.10.10.11 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 dialer idle-timeout 9000
 dialer map ip 10.10.10.10 name dial-6 4724118
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 compress stac
 ppp authentication chap
 ppp multilink
```

```
 crypto map dial6
!
ip classless
ip route 40.40.40.0 255.255.255.0 10.10.10.10
access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-5#

-----------------------

dial-6#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-6
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc.
!
username dial-5 password 0 cisco
no ip domain-lookup
isdn switch-type basic-ni1
!
 crypto map dial5 10
 set peer dial5
 match address 144
!
crypto key pubkey-chain dss
 named-key dial5
  serial-number 05679919
  key-string
   160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
   F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
  quit
 !
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface BRI0
 ip address 10.10.10.10 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 9000
 dialer map ip 10.10.10.11 name dial-5 4724171
 dialer hold-queue 40
 dialer load-threshold 5 outbound
 dialer-group 1
 isdn spid1 919472411800 4724118
```

```
 isdn spid2 919472411901 4724119
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial5
!
ip classless
ip route 20.20.20.0 255.255.255.0 10.10.10.11
access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-6#
```

## Steekproef 5: Versleuteling van IPX-verkeer in een IP-tunnels

In dit voorbeeld wordt het IPX-verkeer in een IP-tunnel versleuteld.

**Opmerking:** Alleen verkeer in deze tunnel (IPX) is versleuteld. Al het andere IP-verkeer blijft alleen.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c34.aa6a
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map wan2516 10
 set peer wan2516
 match address 133
!
!
interface Loopback1
 ip address 50.50.50.50 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
```

```
 tunnel source 50.50.50.50
 tunnel destination 60.60.60.60
 crypto map wan2516
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 ipx network 600
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map wan2516
!
interface Serial1
 no ip address
 shutdown
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
line aux 0
 password ww
 login
line vty 0 4
 password ww
 login
!
end

WAN-2511a#

------------------------

WAN-2516a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname WAN-2516a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c3b.cc1e
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
```

```
crypto map wan2511 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
! <other hub interfaces snipped>
!
hub ether 0 14
 link-test
 auto-polarity
!
interface Loopback1
 ip address 60.60.60.60 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 60.60.60.60
 tunnel destination 50.50.50.50
 crypto map wan2511
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
 ipx network 400
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map wan2511
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit ip host 60.60.60.60 host 50.50.50.50
access-list 188 permit gre any any
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end
```

```
WAN-2516a#
----------------------

WAN-2511a#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        100 (TUNNEL),        Tu1
C        600 (NOVELL-ETHER),  Et0
R        400 [151/01] via      100.0000.0c3b.cc1e,   24s, Tu1


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    207      207


WAN-2511a#ping 400.0000.0c3b.cc1e
Translating "400.0000.0c3b.cc1e"

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212


WAN-2511a#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms


WAN-2511a#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212

WAN-2511a#
```

## Steekproef 6: L2F-tunnels versleutelen

In dit voorbeeld wordt alleen het L2F-verkeer versleutelen voor gebruikers die inbellen. Hier, "user@cisco.com" roept de lokale Server van de Toegang van het Netwerk (NAS) genoemd "DEMO2" in hun stad en wordt gericht aan de gateway CD van het huis. Al het DEMO2 verkeer (samen met dat van andere L2F-bellers) is versleuteld. Omdat L2F UDP-poort 1701 gebruikt, is dit hoe de toegangslijst geconstrueerd is, en bepaalt welk verkeer versleuteld is.

**Opmerking:** Als de coderingsassociatie nog niet is ingesteld, betekent dat de beller de eerste

persoon is die de L2F-tunnel belt en maakt, kan de beller vallen vanwege de vertraging bij het instellen van de coderingsassociatie. Dit kan niet gebeuren bij routers met voldoende CPU-voeding. Bovendien kunt u de **keytimeout** willen uitbreiden zodat de encryptie set-up en de afbraak alleen tijdens off-piek uren plaatsvindt.

De volgende voorbeeldopdrachtoutput is van de afstandsbediening genomen.

```
DEMO2#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname DEMO2
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
no ip domain-lookup
vpdn enable
vpdn outgoing cisco.com NAS1 ip 20.20.20.20
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map vpdn 10
 set peer wan2516
 match address 133
!
crypto key-timeout 1440
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface Group-Async1
 no ip address
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 no cdp enable
 ppp authentication chap pap
 group-range 1 16
!
ip default-gateway 10.11.19.254
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit udp host 20.20.20.21 eq 1701
 host 20.20.20.20 eq 1701
!
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line aux 0
 login local
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

DEMO2#
```

De volgende voorbeeldopdrachtoutput werd van de Thuispoort gehaald.

```
CD#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CD
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco
no ip domain-lookup
vpdn enable
vpdn incoming NAS1 HomeGateway virtual-template 1
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto key-timeout 1440
!
crypto map vpdn 10
 set peer wan2511
 match address 144
!
```

```
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no ip mroute-cache
 peer default ip address pool default
 ppp authentication chap
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip local pool default 70.70.70.2 70.70.70.77
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit udp host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end
```

## Probleemoplossing

Het is over het algemeen best om elke sessie voor het oplossen van problemen te beginnen door informatie te verzamelen met de volgende **tonen** opdrachten. Een sterretje (*) geeft een bijzonder nuttige opdracht aan. Zie ook IP Security Problemen opsporen en verhelpen - Opdrachten begrijpen en gebruiken voor meer informatie.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show**

genereren.

**Opmerking:** Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

| Opdrachten | |
|---|---|
| toont cryptocisco algoritmen | vastlegging van de sleutelfunctie van Cisco tonen |
| tonen van crypto cisco pregen-dh-paren | * toont actieve cryptoommotorverbindingen |
| cryptomotorverbindingen laten zien met gedropt pakje | configuratie van de cryptomotor |
| code van de sleutel van de sleutel | * toont cryptoomsleutelketens |
| toont crypto kaart interface seriële 1 | * toont cryptografische kaart |
| debug van crypto-motor | * cryptografie debug |
| debug strijdkreet | duidelijke cryptoverbinding |
| cryptotechniek | geen crypto openbare sleutel |

- **toont cryptocisco algoritmen**- U moet alle Data Encryption Standard (DES)-algoritmen inschakelen die worden gebruikt om met een andere peer-encryptie-router te communiceren. Als u geen DES algoritme toelaat, zult u dat algoritme niet kunnen gebruiken, zelfs als u het algoritme aan een **crypto kaart** op een later tijdstip probeert toe te wijzen.Als uw router probeert een gecodeerde communicatiesessie met een peer router in te stellen en de twee routers niet hetzelfde DES-algoritme hebben dat aan beide eindpunten is ingeschakeld, mislukt de gecodeerde sessie. Als op beide eindpunten ten minste één gemeenschappelijk DES-algoritme is ingeschakeld, kan de versleutelde sessie worden voortgezet.**Opmerking:** het extra woord cisco verschijnt in Cisco IOS-softwarerelease 11.3 en is nodig om onderscheid te maken tussen IPSec en de eigen encryptie van Cisco die is gevonden in Cisco IOS-softwarerelease 11.2.

```
Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8
```

- **toont crypto cisco key-timeout** - Nadat een versleutelde communicatiesessie is ingesteld is deze geldig voor een bepaalde tijd. Na deze tijdsduur zijn de sessies verlopen. Er moet over een nieuwe sessie worden onderhandeld en er moet een nieuwe DES (sessie)-toets worden gegenereerd zodat versleutelde communicatie kan worden voortgezet. Gebruik deze opdracht om de tijd te veranderen dat een gecodeerde communicatiesessie duurt voordat deze vervalt (time-out).

```
Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes
```

Gebruik deze opdrachten om de tijdsduur te bepalen voordat de DES-toetsen opnieuw worden onderhandeld.

```
StHelen#show crypto conn
Connection Table
```

```
PE              UPE         Conn_id New_id Algorithm    Time
0.0.0.1         0.0.0.1        4    0      DES_56_CFB64 Mar 01 1993 03:16:09
                flags:TIME_KEYS


StHelen#show crypto key
Session keys will be re-negotiated every 30 minutes

StHelen#show clock
*03:21:23.031 UTC Mon Mar 1 1993
```

- **Toon crypto cisco pregen-dh-paren** - Elke gecodeerde sessie gebruikt een uniek paar DH nummers. Telkens wanneer een nieuwe sessie wordt ingesteld, moeten er nieuwe DH-nummerparen worden gegenereerd. Wanneer de sessie is voltooid, worden deze getallen verworpen. Het genereren van nieuwe DH-nummerparen is een CPU-intensieve activiteit, die sessieinstelling langzaam kan maken, met name voor routers met lage dichtheid.Om de opzet van de sessie te versnellen, kunt u ervoor kiezen een bepaalde hoeveelheid DH aantal paren te hebben die vooraf gegenereerd en in reserve gehouden worden. Vervolgens wordt, wanneer een versleutelde communicatiesessie wordt ingesteld, een DH-nummerpaar uit die reserve geleverd. Nadat een DH aantal paar wordt gebruikt, wordt de reserve automatisch aangevuld met een nieuw DH aantal paar, zodat er altijd een DH aantal paar klaar voor gebruik is.Het is meestal niet nodig om meer dan een of twee DH nummerparen te hebben pregenereerd, tenzij uw router meerdere versleutelde sessies zo vaak instelt dat een pregenereerde reserve van een of twee DH nummerparen te snel wordt uitgeput.
```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```
- **actieve verbindingen van crypto cisco tonen**Het volgende is uitvoer van een voorbeeldopdracht.
```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 16   Serial1         19.19.19.19 set    DES_56_CFB64    376      884
```
- **tonen crypto cisco motorverbindingen die zakpakket lieten vallen**Het volgende is uitvoer van een voorbeeldopdracht.
```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```
- **toont crypto-motorconfiguratie** (**toont cryptomotor-**instructies in Cisco IOS-softwarerelease 11.2.)Het volgende is uitvoer van een voorbeeldopdracht.
```
Loser#show crypto engine configuration
slot:               0
engine name:        fred
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    465
input queue bot:    465
input queue count:  0
```
- **code van de sleutel van de sleutel**Het volgende is uitvoer van een voorbeeldopdracht.
```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```
- **toonbanketers van crypto-sleutelketens tonen**Het volgende is uitvoer van een

voorbeeldopdracht.

```
Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit
```

- **toont crypto kaart interface seriële 1**Het volgende is uitvoer van een voorbeeldopdracht.

```
Loser#show crypto map interface serial 1
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

Let op het tijdverschil wanneer u de opdracht **ping** gebruikt.

```
wan-5200b#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
wan-5200b#
-----------
wan-5200b#ping 30.30.30.31

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms
-----------------

wan-5200b#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
------------
```

- **toont crypto kaart interface seriële 1**Het volgende is uitvoer van een voorbeeldopdracht.

```
Loser#show crypto map
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

- **debug van crypto-motor**Het volgende is uitvoer van een voorbeeldopdracht.

```
Loser#debug crypto engine
Mar 17 11:49:07.902: Crypto engine 0: generate alg param

Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:11.758: Crypto engine 0: generate alg param

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
```

```
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25
Mar 17 11:49:24.946: Crypto engine 0: generate alg param
```

- **debug van crypto sessmgmt**Het volgende is uitvoer van een voorbeeldopdracht.

```
StHelen#debug crypto sessmgmt

Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328,
              Found an ICMP connection message.

Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK
Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19
Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent
Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK
Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM
Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK
Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0)
Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0.
Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0
Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK
                           ~~ <---------- This is good ----------> ~~
```

  Als de verkeerde peer op de Crypto Kaart wordt ingesteld, ontvangt u deze foutmelding.

```
Mar  2 12:19:12.639: CRYPTO-SDU:Far end authentication error:
          Connection message verify failed
```

  Als de crypto algoritmen niet overeenkomen, ontvangt u deze foutmelding.

```
Mar  2 12:26:51.091: CRYPTO-SDU: Connection
failed due to incompatible policy
```

  Als de DSS-toets ontbreekt of ongeldig is, ontvangt u deze foutmelding.

```
Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:
           Connection message verify failed
```

- **cryptoomsleutel debug**Het volgende is uitvoer van een voorbeeldopdracht.

```
StHelen#debug crypto key
Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes.

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
```

- **duidelijke cryptoverbinding**Het volgende is uitvoer van een voorbeeldopdracht.

```
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 9    Serial0         20.20.20.21 set    DES_56_CFB64    29       28

wan-2511#clear crypto connection 9
wan-2511#
*Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0)
```

```
*Mar  5 04:58:20.694: Crypto engine 0: delete connection 9
*Mar  5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK
wan-2511#
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt

wan-2511#
```

- **cryptotechniek**Het volgende is uitvoer van een voorbeeldopdracht.

```
wan-2511#show crypto mypubkey
crypto public-key wan2511 01496536
 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named wan2511.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto mypubkey
wan-2511#
```

- **geen crypto openbare sleutel**Het volgende is uitvoer van een voorbeeldopdracht.

```
wan-2511#show crypto pubkey
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto public-key ?
  WORD  Peer name

wan-2511(config)#
wan-2511(config)#no crypto public-key wan2516 01698232
wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto pubkey
wan-2511#
```

## Problemen oplossen met Cisco 7200 met ESA

Cisco biedt ook een optie voor hardware help om encryptie te doen op Cisco 7200 Series routers, die het ESA wordt genoemd. Het ESA is in de vorm van een poortadapter voor de VIP2-40 kaart of een standalone poortadapter voor Cisco 7200. Deze indeling maakt het gebruik van een hardwareadapter of de VIP2-softwaremotor mogelijk om gegevens te versleutelen en te decrypteren die in de interfaces op de Cisco 7500 VIP2-kaart komen of achterblijven. Met Cisco 7200 biedt u hardwareondersteuning voor het versleutelen van verkeer voor interfaces op het Cisco 7200 chassis. Met een encryptie kunt u waardevolle CPU-cycli opslaan die voor andere doeleinden kunnen worden gebruikt, zoals routing of een van de andere Cisco IOS-functies.

Op een Cisco 7200, wordt de standalone poortadapter gevormd precies het zelfde als de Cisco IOS software crypto motor, maar heeft een paar extra opdrachten die slechts voor hardware

worden gebruikt en voor het beslissen welke motor (software of hardware) de encryptie zal doen.

Stel eerst de router voor hardwareencryptie voor:

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine

wan-7206a#show crypto card 3

Crypto card in slot: 3

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
wan-7206a#

wan-7206a(config)#

wan-7206a(config)#crypto zeroize 3
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named hard.
Do you really want to remove these keys? [yes/no]: yes
[OK]
```

Schakel hardwareencryptie in of uit zoals hieronder wordt getoond:

```
wan-7206a(config)#crypto esa shutdown 3
...switching to SW crypto engine


wan-7206a(config)#crypto esa enable 3
There are no keys on the ESA in slot 3- ESA not enabled.
```

genereert vervolgens de toetsen voor de ESA voordat u deze instelt.

```
wan-7206a(config)#crypto gen-signature-keys hard
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

wan-7206a(config)#
wan-7206a#show crypto mypubkey
crypto public-key hard 00000052
 EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905
 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804
quit

wan-7206a#
wan-7206a(config)#crypto esa enable 3
...switching to HW crypto engine
```

```
wan-7206a#show crypto engine brie
crypto engine name:   hard
crypto engine type:   ESA
serial number:        00000052
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 3

wan-7206a#
```

## VIP2-probleemoplossing met ESA

De ESR hardware poortadapter op de VIP2-kaart wordt gebruikt om gegevens te versleutelen en te decrypteren die in de interfaces op de VIP2-kaart komen of erdoor verlaat. Net als bij Cisco 7200 kunt u met behulp van een encryptie waardevolle CPU-cycli opslaan. In dit geval bestaat de cryptograaf, die opdracht kan uitvoeren, niet omdat de ESA poortadapter de encryptie voor de poorten op de VIP2-kaart doet als de ESA is aangesloten. De crypto-ontgrendeling dient op die sleuf te worden toegepast als de ESA poortadapter voor het eerst is geïnstalleerd, dan wel verwijderd en vervolgens opnieuw geïnstalleerd.

```
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#
```

Omdat de ESA crypto module is geëxtraheerd, krijgt u de volgende foutmelding totdat u een crypto-blokkeringsopdracht op die sleuf uitvoert, zoals hieronder wordt getoond.

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ?
  <0-15>  Chassis slot number

Router(config)#crypto clear-latch 11
% Enter the crypto card password.
Password:
Router(config)#^Z
```

Als u een eerder toegewezen wachtwoord vergeet, gebruikt u de opdracht crypto zeroize in plaats van de opdracht crypto blokkering om de ESA opnieuw in te stellen. Nadat u de opdracht crypto zeroize hebt uitgegeven, moet u DSS-toetsen regenereren en opnieuw uitwisselen. Wanneer u DSS-toetsen regenereert, wordt u gevraagd een nieuw wachtwoord in te voeren. Hieronder wordt een voorbeeld gegeven.

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11

Crypto card in slot: 11
```

```
Tampered:        No
Xtracted:        No
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#

-------------------------------------------------


Router#show crypto engine brief
crypto engine name:   TERT
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  dss key generated
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   WAAA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
-----------
Router(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named TERT.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

Router(config)#crypto zeroize  11
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named WAAA.
Do you really want to remove these keys? [yes/no]: yes
[OK]

Router(config)#^Z
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   unknown
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
--------------
Router(config)#crypto gen-signature-keys VIPESA 11
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.
```

```
Password:
Re-enter password:
Generating DSS keys ....
 [OK]

Router(config)#
*Jan 24 01:39:52.923: Crypto engine 11: create key pairs.
^Z
Router#
------
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   VIPESA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
----------
Router#show crypto engine connections active 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 2    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    9996     9996

Router#
Router#clear crypto connection 2 11
Router#
*Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11)
*Jan 24 01:41:04.611: Crypto engine 11: delete connection 2
*Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK
Router#show crypto engine connections active 11
No connections.

Router#
*Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries
received from VIP 0
------------

Router#show crypto mypub
% Key for slot 11:
crypto public-key VIPESA 00000078
 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD A87BF7FE
 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508
quit

Router#show crypto pub
crypto public-key wan2516 01698232
 C5DE8C46 8A69932C 70C92A2C 729449B3 FD10AC4D 1773A997 7F6BA37D 61997AC3
 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22 CFAAC1A8 9CE82985
quit

Router#
----------
interface Serial11/0/0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
```

```
 ip route-cache distributed
 no fair-queue
 no cdp enable
 crypto map test
!
----------
Router#show crypto eng conn act 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 3    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    761      760

Router#
*Jan 24 01:50:43.555: CRYPTO ENGINE:Number of connection
entries received from VIP 1

Router#
```

# Gerelateerde informatie

- Configuratie- en probleemoplossing van Cisco Network-Layer Encryption: IPsec en ISAKMP - deel 2
- DES FIPS 46-2 bij National Institute of Standards and Technology (NIST)
- DSS FIPS 1860 bij National Institute of Standards and Technology (NIST)
- RSA Laboratories' s gestelde vragen over de hedendaagse cryptografie
- IETF-beveiligingsstandaarden
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- IPsec-netwerkbeveiliging configureren
- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen