

Router-naar-router IPSec (RSA-toetsen) op GRE-tunnels met Configuratievoorbeeld van RIP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Procedure voor probleemoplossing](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie voor routers met RSA-toetsen. Beide routers worden geconfigureerd voor RSA-toetsen en IPSec/Generic Routing Encapsulation (GRE) met Routing Information Protocol (RIP).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- Cisco-router met Cisco IOS® softwarerelease 12.2

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

Conventies

Raadpleeg voor meer informatie over documentconventies de [technische Tips](#) van [Cisco](#).

Configureren

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

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het [Opdrachtplanningprogramma](#) (alleen [geregistreerd](#) klanten).

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- [Crypto configuratie voor router 10.1](#)
- [router 1010](#)
- [Crypto configuratie voor router 102](#)
- [router 102](#)

Crypto configuratie voor router 10.1

```
101(config)#crypto isakmp enable
101(config)#crypto isakmp identity hostname
101(config)#crypto isakmp policy 1
101(config-isakmp)#authentication rsa-encr
101(config)#access-list 101 permit gre host 20.1.1.1
host 20.1.1.2
101(config)#crypto ipsec transform-set test esp-des esp-
sha-hmac
101(cfg-crypto-trans)#mode transport
101(config)#crypto map test 10 ip
101(config)#crypto map test 10 ipsec-is
% NOTE: This new crypto map will remain disabled until a
peer
and a valid access list have been configured.
101(config-crypto-map)#set transform-set test
101(config-crypto-map)#match address 101
101(config-crypto-map)#set peer 20.1.1.2
101(config-crypto-map)#
```

```
101(config)#access-list 101 permit gre host 20.1.1.1
host 20.1.1.2
```

```
101(config)#interface Tunnel0
101(config-if)#crypto map test
```

```
101(config)#interface ethernet 1/0
101(config-if)#crypto map test
```

router 1010

Building configuration...

Current configuration : 1486 bytes

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 101
!
!
clock timezone PST -8
ip subnet-zero
ip domain name cisco.com
ip host 102.cisco.com 20.1.1.2
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
 authentication rsa-encr
crypto isakmp identity hostname
crypto isakmp keepalive 20 5
!
!
crypto ipsec transform-set test esp-des esp-sha-hmac
 mode transport
!
crypto map test 10 ipsec-isakmp
 set peer 20.1.1.2
 set transform-set test
 match address 101
!
!
crypto key pubkey-chain rsa
 named-key 102.cisco.com
 key-string
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00DB4FEB EF0C0D3D
 72FC5BD3 29C8E94B 726161BC F1AF337C E5F2D11D FBFC2245
95EA2AB7 9D09156C
 08A5A7CD 36E43D94 F1E3C978 37A79379 384D2A72 CE575E91
3F020301 0001
 quit
!
!
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
!
```

```

interface Tunnel0
 ip address 10.10.10.1 255.255.255.252
 ip mtu 1420
 tunnel source Ethernet1/0
 tunnel destination 20.1.1.2
 crypto map test
!
interface Ethernet0/0
 ip address 1.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 20.1.1.1 255.255.255.0
 crypto map test
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 10.0.0.0
 network 192.168.1.0
!
ip classless
no ip http server
!
!
access-list 101 permit gre host 20.1.1.1 host 20.1.1.2
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
101#

```

Crypto configuratie voor router 102

```

102(config)#crypto isakmp enable
102(config)#crypto isakmp identity hostname
102(config)#crypto isakmp policy 1
102(config-isakmp)#authentication rsa-encr
102(config)#access-list 101 permit gre host 20.1.1.2
host 20.1.1.1
102(config)#crypto ipsec transform-set test esp-des esp-
sha-hmac
102(cfg-crypto-trans)#mode transport
102(config)#crypto map test 10 ip
102(config)#crypto map test 10 ipsec-is
% NOTE: This new crypto map will remain disabled until a
peer
    and a valid access list have been configured.
102(config-crypto-map)#set transform-set test
102(config-crypto-map)#match address 101
102(config-crypto-map)#set peer 20.1.1.1

```

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

```
102(config)#interface Tunnel0
```

```
102(config-if)#crypto map test
```

```
102(config)#interface ethernet 1/0
```

```
102(config-if)#crypto map test
```

router 102

```
102#write terminal
```

```
Building configuration...
```

```
Current configuration : 1484 bytes
```

```
!
```

```
version 12.2
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname 102
```

```
!
```

```
!
```

```
clock timezone PST -8
```

```
ip subnet-zero
```

```
ip domain name cisco.com
```

```
ip host 101.cisco.com 20.1.1.1
```

```
!
```

```
ip audit notify log
```

```
ip audit po max-events 100
```

```
!
```

```
crypto isakmp policy 1
```

```
authentication rsa-encr
```

```
crypto isakmp identity hostname
```

```
crypto isakmp keepalive 20 5
```

```
!
```

```
!
```

```
crypto ipsec transform-set test esp-des esp-sha-hmac
```

```
mode transport
```

```
!
```

```
crypto map test 10 ipsec-isakmp
```

```
set peer 20.1.1.1
```

```
set transform-set test
```

```
match address 101
```

```
!
```

```
!
```

```
crypto key pubkey-chain rsa
```

```
named-key 101.cisco.com
```

```
address 20.1.1.1
```

```
key-string
```

```
305C300D 06092A86 4886F70D 01010105 00034B00 30480241
```

```
00A7D24F E6E15787
```

```
5EE1434A A76A3DC1 ADE96A4D C6B4D0F3 A7DDAD10 446EF83A
```

```
89D1115F 0C517118
```

```
ECAF418E F4C84823 2A017B97 F85690EF EBCF3414 AB3E81F6
```

```
A5020301 0001
```

```
quit
```

```
!
```

```
!
```

```
!
```

```
interface Loopback1
```

```
ip address 172.16.1.1 255.255.255.0
!
interface Tunnel0
 ip address 10.10.10.2 255.255.255.252
 ip mtu 1420
 tunnel source Ethernet0/0
 tunnel destination 20.1.1.1
 crypto map test
!
interface Ethernet0/0
 ip address 20.1.1.2 255.255.255.0
 crypto map test
!
interface Ethernet1/0
 no ip address
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface Ethernet0/0
 network 10.0.0.0
 network 172.16.0.0
!
ip classless
no ip http server
!
!
access-list 101 permit gre host 20.1.1.2 host 20.1.1.1
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
102#
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

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.](#)

- **toon crypto isakmp als detail**-Toont alle huidige IKE (Internet Key Exchange) veiligheidsassociaties (SAs) bij een peer.
- **Laat crypto ipsec sa-displays** de instellingen die worden gebruikt door de huidige SAs.
- **toont crypto motorverbindingen actief** — Geeft een samenvatting van de configuratie

informatie voor de cryptomotoren.

- **toon ip route**-Toont de huidige status van de routingtabel.

router 1010 opdrachtoutput

```
101#show crypto isakmp sa detail
```

```
*Dec 28 21:15:19.371: ISAKMP (0:14): purging node 543282640
```

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
```

```
      K - Keepalives, N - NAT-traversal
```

```
      X - IKE Extended Authentication
```

```
      psk - Preshared key, rsig - RSA signature
```

```
      renc - RSA encryption
```

```
Conn id Local          Remote          Encr Hash Auth DH Lifetime Capabilities
14      20.1.1.1            20.1.1.2      des sha rsig 1 23:59:06 D
```

```
101#show crypto ipsec sa
```

```
interface: Ethernet1/0
```

```
  Crypto map tag: test, local addr. 20.1.1.1
```

```
local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)
```

```
current_peer: 20.1.1.2:500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
```

```
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 1, #recv errors 0
```

```
local crypto endpt.: 20.1.1.1, remote crypto endpt.: 20.1.1.2
```

```
path mtu 1420, media mtu 1420
```

```
current outbound spi: 7FB7A347
```

```
inbound esp sas:
```

```
  spi: 0x7221D7D2(1914820562)
```

```
    transform: esp-des esp-sha-hmac ,
```

```
    in use settings = {Transport, }
```

```
    slot: 0, conn id: 2000, flow_id: 1, crypto map: test
```

```
    sa timing: remaining key lifetime (k/sec): (4468975/3586)
```

```
    IV size: 8 bytes
```

```
    replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
  spi: 0x7FB7A347(2142741319)
```

```
    transform: esp-des esp-sha-hmac ,
```

```
    in use settings = {Transport, }
```

```
    slot: 0, conn id: 2001, flow_id: 2, crypto map: test
```

```
    sa timing: remaining key lifetime (k/sec): (4468975/3586)
```

```
    IV size: 8 bytes
```

```
    replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

interface: Tunnel0

Crypto map tag: test, local addr. 20.1.1.1

local ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)

current_peer: 20.1.1.2:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 20.1.1.1, remote crypto endpt.: 20.1.1.2

path mtu 1420, media mtu 1420

current outbound spi: 7FB7A347

inbound esp sas:

spi: 0x7221D7D2(1914820562)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: test

sa timing: remaining key lifetime (k/sec): (4468975/3585)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x7FB7A347(2142741319)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: test

sa timing: remaining key lifetime (k/sec): (4468975/3584)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

101#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
14	Ethernet1/0	20.1.1.1	set	HMAC_SHA+DES_56_CB	0	0
2000	Ethernet1/0	20.1.1.1	set	HMAC_SHA+DES_56_CB	0	6
2001	Ethernet1/0	20.1.1.1	set	HMAC_SHA+DES_56_CB	5	0

101#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
20.0.0.0/24 is subnetted, 1 subnets
C    20.1.1.0 is directly connected, Ethernet1/0
R    172.16.0.0/16 [120/1] via 10.10.10.2, 00:00:08, Tunnel0
    10.0.0.0/30 is subnetted, 1 subnets
C    10.10.10.0 is directly connected, Tunnel0
C    192.168.1.0/24 is directly connected, Loopback1
101#
```

Router 102 opdrachtoutput

102#**show crypto isakmp sa detail**

Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption

Conn id	Local	Remote	Encr	Hash	Auth	DH	Lifetime	Capabilities
15	20.1.1.2	20.1.1.1	des	sha	rsig	1	23:58:44	D

102#**show crypto ipsec sa**

interface: Ethernet0/0

Crypto map tag: test, local addr. 20.1.1.2

local ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)
current_peer: 20.1.1.1:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 20.1.1.2, remote crypto endpt.: 20.1.1.1

path mtu 1420, media mtu 1420

current outbound spi: 92F52EF2

inbound esp sas:

spi: 0x1D25013E(488964414)

transform: esp-des esp-sha-hmac ,

in use settings = {Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: test

sa timing: remaining key lifetime (k/sec): (4596388/3494)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x92F52EF2(2465541874)

```
transform: esp-des esp-sha-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: test
sa timing: remaining key lifetime (k/sec): (4596388/3494)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

interface: Tunnel0

Crypto map tag: test, local addr. 20.1.1.2

local ident (addr/mask/prot/port): (20.1.1.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)

current_peer: 20.1.1.1:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 20.1.1.2, remote crypto endpt.: 20.1.1.1

path mtu 1420, media mtu 1420

current outbound spi: 92F52EF2

inbound esp sas:

spi: 0x1D25013E(488964414)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: test

sa timing: remaining key lifetime (k/sec): (4596388/3493)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x92F52EF2(2465541874)

transform: esp-des esp-sha-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: test

sa timing: remaining key lifetime (k/sec): (4596388/3493)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

102#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
15	Ethernet0/0	20.1.1.2	set	HMAC_SHA+DES_56_CB	0	0
2000	Ethernet0/0	20.1.1.2	set	HMAC_SHA+DES_56_CB	0	3

102#

102#**show ip route**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
20.0.0.0/24 is subnetted, 1 subnets
C    20.1.1.0 is directly connected, Ethernet0/0
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Loopback1
10.0.0.0/30 is subnetted, 1 subnets
C    10.10.10.0 is directly connected, Tunnel0
R    192.168.1.0/24 [120/1] via 10.10.10.1, 00:00:08, Tunnel0
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Zie [IP-beveiligingsprobleemoplossing](#) voor meer informatie over [het](#) oplossen van [problemen - Opdrachten begrijpen en gebruiken van debug](#).

Procedure voor probleemoplossing

Volg deze instructies om uw configuratie problemen op te lossen.

1. Generate de RSA toetsen op router 101.

```
101#show crypto key mypubkey rsa
101#
101#
101#conf t
101(config)#ip domain-name cisco.com
101(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                  encryption
  usage-keys    Generate separate RSA key pairs for signing and encryption
```

```
101(config)#crypto key generate rsa
The name for the keys will be: 101.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
```

```
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

```
101#show crypto key mypubkey rsa
% Key pair was generated at: 12:02:08 PST Dec 28 2002
Key name: 101.cisco.com
Usage: General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A7D24F E6E15787
 5EE1434A A76A3DC1 ADE96A4D C6B4D0F3 A7DDAD10 446EF83A 89D1115F 0C517118
 ECAF418E F4C84823 2A017B97 F85690EF EBCF3414 AB3E81F6 A5020301 0001
```

```

% Key pair was generated at: 12:02:12 PST Dec 28 2002
Key name: 101.cisco.com.server
Usage: Encryption Key
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B2092A 86483641
 EB09900B BA0CD88A BE915C5E 05C1496B 70093D8B BC277A88 0E256BBE 4DB7EF92
 8FE93C61 710309A3 451DAB72 93F35CD0 1CAD15AC B904B2B4 73B7A9F5 65A79E66
 8D145427 F06DD89C 862B88BB 4C671508 AB3443BB 6270388C A7020301 0001
101#

```

2. Generate de RSA toetsen op router 102.

```

102#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
102(config)#ip domain-name cisco.com
102(config)#crypto key gen rsa
The name for the keys will be: 102.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

```

```

102#show crypto key mypubkey rsa
% Key pair was generated at: 12:03:45 PST Dec 28 2002
Key name: 102.cisco.com
Usage: General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DB4FEB EF0C0D3D
 72FC5BD3 29C8E94B 726161BC F1AF337C E5F2D11D FBFC2245 95EA2AB7 9D09156C
 08A5A7CD 36E43D94 F1E3C978 37A79379 384D2A72 CE575E91 3F020301 0001
% Key pair was generated at: 12:03:48 PST Dec 28 2002
Key name: 102.cisco.com.server
Usage: Encryption Key
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00BFD36E A1642BFC
 77C88F89 8A260840 213E122E E1AF1E24 AF39B984 DACA06BC C303AD77 95BB6B6C
 89CC6D13 B16CC4E3 45C101E4 61A13924 5559891A AB59B40D 826A5066 231B48D6
 AEB2B367 94F6C492 016F8778 74B368A2 BFD1424D 79C63C94 5F020301 0001
102#

```

3. Los de hostname op.

```

102(config)#ip host 101.cisco.com 20.1.1.1

```

4. Wisselt de toetsen General purpose op Router 101.

```

101(config)#crypto key pubkey-chain rsa
101(config-pubkey-chain)#named-key 102.cisco.com
% Named public key resolved to ip address: 20.1.1.2
101(config-pubkey-key)#key-string ?
Enter a public key as a hexadecimal number ...

101(config-pubkey)#$6F70D 01010105 00034B00 30480241 00DB4FEB EF0C0D3D
101(config-pubkey)#$26161BC F1AF337C E5F2D11D FBFC2245 95EA2AB7 9D09156C
101(config-pubkey)#$1E3C978 37A79379 384D2A72 CE575E91 3F020301 0001
101(config-pubkey)#quit
101(config-pubkey-key)#exit

```

5. Wisselt de toetsen General purpose op Router 102.

```

102(config)#crypto key pubkey-chain rsa
102(config-pubkey-chain)#named-key 101.cisco.com
% Named public key resolved to ip address: 20.1.1.1
102(config-pubkey-key)#key-string

```

Enter a public key as a hexadecimal number

```
102(config-pubkey)#$6F70D 01010105 00034B00 30480241 00A7D24F E6E15787
102(config-pubkey)#$DE96A4D C6B4D0F3 A7DDAD10 446EF83A 89D1115F 0C517118
102(config-pubkey)#$A017B97 F85690EF EBCF3414 AB3E81F6 A5020301 0001
102(config-pubkey)#quit
102(config-pubkey-key)#exit
102(config-pubkey-chain)#exit
102(config)#exit
```

Opdrachten voor troubleshooting

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 Commands](#).

Router 101 Debug:

```
101#
101#
101#
101#
*Dec 28 21:14:27.011: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 20.1.1.1, remote= 20.1.1.2,
  local_proxy= 20.1.1.1/255.255.255.255/47/0 (type=1),
  remote_proxy= 20.1.1.2/255.255.255.255/47/0 (type=1),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0xA12DDC39(2704137273), conn_id= 0, keysize= 0, flags= 0x400C
*Dec 28 21:14:27.051: ISAKMP: received ke message (1/1)
*Dec 28 21:14:27.051: ISAKMP: local port 500, remote port 500
*Dec 28 21:14:27.099: ISAKMP: set new node 0 to QM_IDLE
*Dec 28 21:14:27.099: ISAKMP (0:14): constructed NAT-T vendor-03 ID
*Dec 28 21:14:27.099: ISAKMP (0:14): constructed NAT-T vendor-02 ID
*Dec 28 21:14:27.099: ISAKMP (0:14): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
*Dec 28 21:14:27.099: ISAKMP (0:14): Old State = IKE_READY New State = IKE_I_MM1

*Dec 28 21:14:27.099: ISAKMP (0:14): beginning Main Mode exchange
*Dec 28 21:14:27.099: ISAKMP (0:14): sending packet to 20.1.1.2 my_port
  500 peer_port 500 (I) MM_NO_STATE
*Dec 28 21:14:27.343: ISAKMP (0:14): received packet from 20.1.1.2 dport
  500 sport 500 (I) MM_NO_STATE
*Dec 28 21:14:27.343: ISAKMP (0:14): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Dec 28 21:14:27.343: ISAKMP (0:14): Old State = IKE_I_MM1 New State = IKE_I_MM2

*Dec 28 21:14:27.411: ISAKMP (0:14): processing SA payload. message ID = 0
*Dec 28 21:14:27.411: ISAKMP (0:14): processing vendor id payload
*Dec 28 21:14:27.411: ISAKMP (0:14): vendor ID seems Unity/DPD but bad major
*Dec 28 21:14:27.411: ISAKMP (0:14): vendor ID is NAT-T
*Dec 28 21:14:27.411: ISAKMP (0:14): Checking ISAKMP transform 1 against priority 1 policy
*Dec 28 21:14:27.411: ISAKMP:      encryption DES-CBC
*Dec 28 21:14:27.411: ISAKMP:      hash SHA
*Dec 28 21:14:27.411: ISAKMP:      default group 1
*Dec 28 21:14:27.411: ISAKMP:      auth RSA sig
*Dec 28 21:14:27.411: ISAKMP:      life type in seconds
*Dec 28 21:14:27.411: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Dec 28 21:14:27.411: ISAKMP (0:14): Authentication method offered does not
```

```
match policy!
*Dec 28 21:14:27.411: ISAKMP (0:14): atts are not acceptable. Next payload is 0
*Dec 28 21:14:27.411: ISAKMP (0:14): Checking ISAKMP transform 1 against
priority 65535 policy
*Dec 28 21:14:27.411: ISAKMP: encryption DES-CBC
*Dec 28 21:14:27.411: ISAKMP: hash SHA
*Dec 28 21:14:27.411: ISAKMP: default group 1
*Dec 28 21:14:27.411: ISAKMP: auth RSA sig
*Dec 28 21:14:27.411: ISAKMP: life type in seconds
*Dec 28 21:14:27.411: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Dec 28 21:14:27.411: ISAKMP (0:14): atts are acceptable. Next payload is 0
*Dec 28 21:14:27.411: ISAKMP (0:14): processing vendor id payload
*Dec 28 21:14:27.411: ISAKMP (0:14): vendor ID seems Unity/DPD but bad major
*Dec 28 21:14:27.411: ISAKMP (0:14): vendor ID is NAT-T
*Dec 28 21:14:27.411: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 28 21:14:27.411: ISAKMP (0:14): Old State = IKE_I_MM2
New State = IKE_I_MM2

*Dec 28 21:14:27.503: ISAKMP (0:14): constructed HIS NAT-D
*Dec 28 21:14:27.503: ISAKMP (0:14): constructed MINE NAT-D
*Dec 28 21:14:27.503: ISAKMP (0:14): sending packet to 20.1.1.2 my_port
500 peer_port 500 (I) MM_SA_SETUP
*Dec 28 21:14:27.503: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 28 21:14:27.503: ISAKMP (0:14): Old State = IKE_I_MM2 New State = IKE_I_MM3

*Dec 28 21:14:27.763: ISAKMP (0:14): received packet from 20.1.1.2 dport
500 sport 500 (I) MM_SA_SETUP
*Dec 28 21:14:27.763: ISAKMP (0:14): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Dec 28 21:14:27.763: ISAKMP (0:14): Old State = IKE_I_MM3 New State = IKE_I_MM4

*Dec 28 21:14:27.811: ISAKMP (0:14): processing KE payload. message ID = 0
*Dec 28 21:14:27.811: ISAKMP (0:14): processing NONCE payload. message ID = 0
*Dec 28 21:14:27.811: ISAKMP (0:14): SKEYID state generated
*Dec 28 21:14:27.811: ISAKMP (0:14): processing vendor id payload
*Dec 28 21:14:27.811: ISAKMP (0:14): vendor ID is Unity
*Dec 28 21:14:27.811: ISAKMP (0:14): vendor ID is NAT-T
*Dec 28 21:14:27.811: ISAKMP (0:14): processing vendor id payload
*Dec 28 21:14:27.811: ISAKMP (0:14): vendor ID is DPD
*Dec 28 21:14:27.811: ISAKMP (0:14): vendor ID is NAT-T
*Dec 28 21:14:27.811: ISAKMP (0:14): processing vendor id payload
*Dec 28 21:14:27.811: ISAKMP (0:14): speaking to another IOS box!
*Dec 28 21:14:27.811: ISAKMP:received payload type 17
*Dec 28 21:14:27.811: ISAKMP (0:14): Detected NAT-D payload
*Dec 28 21:14:27.811: ISAKMP (0:14): NAT match MINE hash
*Dec 28 21:14:27.811: ISAKMP:received payload type 17
*Dec 28 21:14:27.811: ISAKMP (0:14): Detected NAT-D payload
*Dec 28 21:14:27.811: ISAKMP (0:14): NAT match HIS hash
*Dec 28 21:14:27.811: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 28 21:14:27.811: ISAKMP (0:14): Old State = IKE_I_MM4
New State = IKE_I_MM4

*Dec 28 21:14:27.903: ISAKMP (0:14): Send initial contact
*Dec 28 21:14:27.903: ISAKMP (0:14): SA is doing RSA signature
authentication using id type ID_FQDN
*Dec 28 21:14:27.903: ISAKMP (14): ID payload
next-payload : 9
type : 2
FQDN name : 101.cisco.com
protocol : 17
port : 0
length : 17
```

*Dec 28 21:14:27.903: ISAKMP (14): Total payload length: 21
*Dec 28 21:14:27.903: ISAKMP (0:14): using the default keypair to sign
*Dec 28 21:14:28.003: ISAKMP (0:14): sending packet to 20.1.1.2
my_port 500 peer_port 500 (I) MM_KEY_EXCH
*Dec 28 21:14:28.003: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 28 21:14:28.003: ISAKMP (0:14): Old State = IKE_I_MM4 New State = IKE_I_MM5

*Dec 28 21:14:28.435: ISAKMP (0:14): received packet from 20.1.1.2 dport
500 sport 500 (I) MM_KEY_EXCH
*Dec 28 21:14:28.435: ISAKMP (0:14): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Dec 28 21:14:28.435: ISAKMP (0:14): Old State = IKE_I_MM5 New State = IKE_I_MM6

*Dec 28 21:14:28.435: ISAKMP (0:14): received packet from 20.1.1.2 dport
500 sport 500 (I) MM_KEY_EXCH
*Dec 28 21:14:28.435: ISAKMP: set new node 226463539 to QM_IDLE
*Dec 28 21:14:28.435: ISAKMP (0:14): Unknown Input: state = IKE_I_MM6,
major, minor = IKE_MESG_FROM_PEER, IKE_INFO_DELETE

*Dec 28 21:14:28.435: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of
Informational mode failed with peer at 20.1.1.2
*Dec 28 21:14:28.503: ISAKMP (0:14): processing ID payload. message ID = 0
*Dec 28 21:14:28.503: ISAKMP (14): Process ID payload
type : 2
FQDN name : 102.cisco.com
protocol : 17
port : 0
length : 13
*Dec 28 21:14:28.503: ISAKMP (0:14): processing SIG payload. message ID = 0
*Dec 28 21:14:28.503: ISAKMP (14): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn =
102.cisco.com
*Dec 28 21:14:28.551: ISAKMP (0:14): SA has been authenticated with 20.1.1.2
*Dec 28 21:14:28.551: ISAKMP (0:14): IKE_DPD is enabled, initializing timers
*Dec 28 21:14:28.551: ISAKMP: Locking peer struct 0x18E6620, IKE refcount 2
for from crypto_ikmp_dpd_ike_init
*Dec 28 21:14:28.551: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 28 21:14:28.551: ISAKMP (0:14): Old State = IKE_I_MM6 New State = IKE_I_MM6

*Dec 28 21:14:28.551: ISAKMP (0:14): received packet from 20.1.1.2 dport 500 sport
500 (I) MM_KEY_EXCH
*Dec 28 21:14:28.551: ISAKMP: set new node 2089493550 to QM_IDLE
*Dec 28 21:14:28.551: ISAKMP (0:14): Unknown Input: state = IKE_I_MM6, major,
minor = IKE_MESG_FROM_PEER, IKE_INFO_DELETE

*Dec 28 21:14:28.611: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 28 21:14:28.611: ISAKMP (0:14): Old State = IKE_I_MM6
New State = IKE_P1_COMPLETE

*Dec 28 21:14:28.651: ISAKMP (0:14): beginning Quick Mode exchange,
M-ID of 543282640
*Dec 28 21:14:28.683: ISAKMP (0:14): sending packet to 20.1.1.2
my_port 500 peer_port 500 (I) QM_IDLE
*Dec 28 21:14:28.683: ISAKMP (0:14): Node 543282640, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM
*Dec 28 21:14:28.683: ISAKMP (0:14): Old State = IKE_QM_READY
New State = IKE_QM_I_QM1
*Dec 28 21:14:28.683: ISAKMP (0:14): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 28 21:14:28.683: ISAKMP (0:14): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE

*Dec 28 21:14:29.303: ISAKMP (0:14): received packet from 20.1.1.2

```
dport 500 sport 500 (I) QM_IDLE
*Dec 28 21:14:29.303: ISAKMP (0:14): processing HASH payload. message
ID = 543282640
*Dec 28 21:14:29.303: ISAKMP (0:14): processing SA payload. message
ID = 543282640
*Dec 28 21:14:29.303: ISAKMP (0:14): Checking IPSec proposal 1
*Dec 28 21:14:29.303: ISAKMP: transform 1, ESP_DES
*Dec 28 21:14:29.303: ISAKMP:   attributes in transform:
*Dec 28 21:14:29.303: ISAKMP:     encaps is 2
*Dec 28 21:14:29.303: ISAKMP:     SA life type in seconds
*Dec 28 21:14:29.303: ISAKMP:     SA life duration (basic) of 3600
*Dec 28 21:14:29.303: ISAKMP:     SA life type in kilobytes
*Dec 28 21:14:29.303: ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Dec 28 21:14:29.303: ISAKMP:     authenticator is HMAC-SHA
*Dec 28 21:14:29.303: ISAKMP (0:14): atts are acceptable.
*Dec 28 21:14:29.303: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 20.1.1.1, remote= 20.1.1.2,
local_proxy= 20.1.1.1/255.255.255.255/47/0 (type=1),
remote_proxy= 20.1.1.2/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Dec 28 21:14:29.303: ISAKMP (0:14): processing NONCE payload.
message ID = 543282640
*Dec 28 21:14:29.303: ISAKMP (0:14): processing ID payload. message ID = 543282640
*Dec 28 21:14:29.303: ISAKMP (0:14): processing ID payload. message ID = 543282640
*Dec 28 21:14:29.351: ISAKMP: Locking peer struct 0x18E6620, IPSEC refcount 1
for for stuff_ke
*Dec 28 21:14:29.351: ISAKMP (0:14): Creating IPSec SAs
*Dec 28 21:14:29.351:   inbound SA from 20.1.1.2 to 20.1.1.1
(proxy 20.1.1.2 to 20.1.1.1)
*Dec 28 21:14:29.351:   has spi 0xA12DDC39 and conn_id 2000 and flags 4
*Dec 28 21:14:29.351:   lifetime of 3600 seconds
*Dec 28 21:14:29.351:   lifetime of 4608000 kilobytes
*Dec 28 21:14:29.351:   has client flags 0x0
*Dec 28 21:14:29.351:   outbound SA from 20.1.1.1
to 20.1.1.2 (proxy 20.1.1.1 to 20.1.1.2 )
*Dec 28 21:14:29.351:   has spi -437189881 and conn_id 2001 and flags C
*Dec 28 21:14:29.351:   lifetime of 3600 seconds
*Dec 28 21:14:29.351:   lifetime of 4608000 kilobytes
*Dec 28 21:14:29.351:   has client flags 0x0
*Dec 28 21:14:29.351: ISAKMP (0:14): sending packet to 20.1.1.2 my_port
500 peer_port 500 (I) QM_IDLE
*Dec 28 21:14:29.351: ISAKMP (0:14): deleting node 543282640 error
FALSE reason ""
*Dec 28 21:14:29.351: ISAKMP (0:14): Node 543282640, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
*Dec 28 21:14:29.351: ISAKMP (0:14): Old State = IKE_QM_I_QM1
New State = IKE_QM_PHASE2_COMPLETE
*Dec 28 21:14:29.371: IPSEC(key_engine): got a queue event...
*Dec 28 21:14:29.371: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 20.1.1.1, remote= 20.1.1.2,
local_proxy= 20.1.1.1/0.0.0.0/47/0 (type=1),
remote_proxy= 20.1.1.2/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xA12DDC39(2704137273), conn_id= 2000, keysize= 0, flags= 0x4
*Dec 28 21:14:29.371: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 20.1.1.1, remote= 20.1.1.2,
local_proxy= 20.1.1.1/0.0.0.0/47/0 (type=1),
remote_proxy= 20.1.1.2/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xE5F10307(3857777415), conn_id= 2001, keysize= 0, flags= 0xC
```



```
*Dec 28 21:14:29.371: IPSEC(add mtree): src 20.1.1.1, dest 20.1.1.2, dest_port 0
*Dec 28 21:14:29.371: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.1.1.1, sa_prot= 50,
sa_spi= 0xA12DDC39(2704137273),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
*Dec 28 21:14:29.371: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.1.1.2, sa_prot= 50,
sa_spi= 0xE5F10307(3857777415),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
```

Router 102 Debug:

102#

```
*Dec 28 21:18:12.111: ISAKMP (0:0): received packet from 20.1.1.1
dport 500 sport 500 (N) NEW SA
*Dec 28 21:18:12.111: ISAKMP: local port 500, remote port 500
*Dec 28 21:18:12.147: ISAKMP (0:15): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Dec 28 21:18:12.147: ISAKMP (0:15): Old State = IKE_READY New State = IKE_R_MM1

*Dec 28 21:18:12.187: ISAKMP (0:15): processing SA payload. message ID = 0
*Dec 28 21:18:12.187: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID seems Unity/DPD but bad major
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID is NAT-T
*Dec 28 21:18:12.187: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID seems Unity/DPD but bad major
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID is NAT-T
*Dec 28 21:18:12.187: ISAKMP (0:15): Checking ISAKMP transform 1 against
priority 1 policy
*Dec 28 21:18:12.187: ISAKMP: encryption DES-CBC
*Dec 28 21:18:12.187: ISAKMP: hash SHA
*Dec 28 21:18:12.187: ISAKMP: default group 1
*Dec 28 21:18:12.187: ISAKMP: auth RSA sig
*Dec 28 21:18:12.187: ISAKMP: life type in seconds
*Dec 28 21:18:12.187: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Dec 28 21:18:12.187: ISAKMP (0:15): Authentication method offered does not
match policy!
*Dec 28 21:18:12.187: ISAKMP (0:15): atts are not acceptable. Next payload is 0
*Dec 28 21:18:12.187: ISAKMP (0:15): Checking ISAKMP transform 1 against
priority 65535 policy
*Dec 28 21:18:12.187: ISAKMP: encryption DES-CBC
*Dec 28 21:18:12.187: ISAKMP: hash SHA
*Dec 28 21:18:12.187: ISAKMP: default group 1
*Dec 28 21:18:12.187: ISAKMP: auth RSA sig
*Dec 28 21:18:12.187: ISAKMP: life type in seconds
*Dec 28 21:18:12.187: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Dec 28 21:18:12.187: ISAKMP (0:15): atts are acceptable. Next payload is 0
*Dec 28 21:18:12.187: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID seems Unity/DPD but bad major
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID is NAT-T
*Dec 28 21:18:12.187: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID seems Unity/DPD but bad major
*Dec 28 21:18:12.187: ISAKMP (0:15): vendor ID is NAT-T
*Dec 28 21:18:12.187: ISAKMP (0:15): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 28 21:18:12.187: ISAKMP (0:15): Old State = IKE_R_MM1 New State = IKE_R_MM1

*Dec 28 21:18:12.255: ISAKMP (0:15): constructed NAT-T vendor-03 ID
*Dec 28 21:18:12.255: ISAKMP (0:15): sending packet to 20.1.1.1 my_port
500 peer_port 500 (R) MM_SA_SETUP
*Dec 28 21:18:12.255: ISAKMP (0:15): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 28 21:18:12.255: ISAKMP (0:15): Old State = IKE_R_MM1 New State = IKE_R_MM2
```

```

*Dec 28 21:18:12.563: ISAKMP (0:15): received packet from 20.1.1.1 dport
500 sport 500 (R) MM_SA_SETUP
*Dec 28 21:18:12.563: ISAKMP (0:15): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Dec 28 21:18:12.563: ISAKMP (0:15): Old State = IKE_R_MM2 New State = IKE_R_MM3

*Dec 28 21:18:12.619: ISAKMP (0:15): processing KE payload. message ID = 0
*Dec 28 21:18:12.619: ISAKMP (0:15): processing NONCE payload. message ID = 0
*Dec 28 21:18:12.695: ISAKMP (0:15): SKEYID state generated
*Dec 28 21:18:12.695: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.695: ISAKMP (0:15): vendor ID is Unity
*Dec 28 21:18:12.695: ISAKMP (0:15): vendor ID is NAT-T
*Dec 28 21:18:12.695: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.695: ISAKMP (0:15): vendor ID is DPD
*Dec 28 21:18:12.695: ISAKMP (0:15): vendor ID is NAT-T
*Dec 28 21:18:12.695: ISAKMP (0:15): processing vendor id payload
*Dec 28 21:18:12.695: ISAKMP (0:15): speaking to another IOS box!
*Dec 28 21:18:12.695: ISAKMP:received payload type 17
*Dec 28 21:18:12.695: ISAKMP (0:15): Detected NAT-D payload
*Dec 28 21:18:12.695: ISAKMP (0:15): NAT match MINE hash
*Dec 28 21:18:12.695: ISAKMP:received payload type 17
*Dec 28 21:18:12.695: ISAKMP (0:15): Detected NAT-D payload
*Dec 28 21:18:12.695: ISAKMP (0:15): NAT match HIS hash
*Dec 28 21:18:12.695: ISAKMP (0:15): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 28 21:18:12.695: ISAKMP (0:15): Old State = IKE_R_MM3
New State = IKE_R_MM3

*Dec 28 21:18:12.735: ISAKMP (0:15): constructed HIS NAT-D
*Dec 28 21:18:12.735: ISAKMP (0:15): constructed MINE NAT-D
*Dec 28 21:18:12.735: ISAKMP (0:15): sending packet to 20.1.1.1
my_port 500 peer_port 500 (R)
MM_KEY_EXCH *Dec 28 21:18:12.735: ISAKMP (0:15): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 28 21:18:12.735: ISAKMP (0:15): Old State = IKE_R_MM3 New State = IKE_R_MM4

*Dec 28 21:18:13.395: ISAKMP (0:15): received packet from 20.1.1.1 dport
500 sport 500 (R) MM_KEY_EXCH
*Dec 28 21:18:13.395: ISAKMP (0:15): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Dec 28 21:18:13.395: ISAKMP (0:15): Old State = IKE_R_MM4 New State = IKE_R_MM5

*Dec 28 21:18:13.435: ISAKMP (0:15): processing ID payload. message ID = 0
*Dec 28 21:18:13.435: ISAKMP (15): Process ID payload
type : 2
FQDN name : 101.cisco.com
protocol : 17
port : 0
length : 13
*Dec 28 21:18:13.435: ISAKMP (0:15): processing SIG payload. message ID = 0
*Dec 28 21:18:13.435: ISAKMP (15): sa->peer.name = ,
sa->peer_id.id.id_fqdn.fqdn = 101.cisco.com
*Dec 28 21:18:13.567: ISAKMP:received payload type 14
*Dec 28 21:18:13.567: ISAKMP (0:15): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 1AD8D08
*Dec 28 21:18:13.567: ISAKMP (0:15): Process initial contact,
bring down existing phase 1 and 2 SA's with local 20.1.1.2 remote 20.1.1.1
remote port 500
*Dec 28 21:18:13.587: ISAKMP (0:15): SA has been authenticated with 20.1.1.1
*Dec 28 21:18:13.587: ISAKMP (0:15): IKE_DPD is enabled, initializing timers
*Dec 28 21:18:13.587: ISAKMP: Locking peer struct 0x18EA370, IKE refcount 2
for from crypto_ikmp_dpd_ike_init
*Dec 28 21:18:13.587: ISAKMP (0:15): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Dec 28 21:18:13.587: ISAKMP (0:15): Old State = IKE_R_MM5 New State = IKE_R_MM5

```

```
*Dec 28 21:18:13.599: IPSEC(key_engine): got a queue event...
*Dec 28 21:18:13.627: ISAKMP (0:15): SA is doing RSA signature authentication
using id type ID_FQDN
*Dec 28 21:18:13.627: ISAKMP (15): ID payload
    next-payload : 9
    type          : 2
    FQDN name     : 102.cisco.com
    protocol      : 17
    port          : 0
    length        : 17
*Dec 28 21:18:13.627: ISAKMP (15): Total payload length: 21
*Dec 28 21:18:13.627: ISAKMP (0:15): using the default keypair to sign
*Dec 28 21:18:13.731: ISAKMP (0:15): sending packet to 20.1.1.1 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Dec 28 21:18:13.731: ISAKMP (0:15): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Dec 28 21:18:13.731: ISAKMP (0:15): Old State = IKE_R_MM5
New State = IKE_P1_COMPLETE
*Dec 28 21:18:13.779: ISAKMP (0:15): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 28 21:18:13.779: ISAKMP (0:15): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
*Dec 28 21:18:14.215: ISAKMP (0:15): received packet from 20.1.1.1
dport 500 sport 500 (R) QM_IDLE
*Dec 28 21:18:14.215: ISAKMP: set new node 1098460553 to QM_IDLE
*Dec 28 21:18:14.215: ISAKMP (0:15): processing HASH payload.
message ID = 1098460553
*Dec 28 21:18:14.215: ISAKMP (0:15): processing SA payload.
message ID = 1098460553
*Dec 28 21:18:14.215: ISAKMP (0:15): Checking IPSec proposal 1
*Dec 28 21:18:14.215: ISAKMP: transform 1, ESP_DES
*Dec 28 21:18:14.215: ISAKMP:   attributes in transform:
*Dec 28 21:18:14.215: ISAKMP:     encaps is 2
*Dec 28 21:18:14.215: ISAKMP:     SA life type in seconds
*Dec 28 21:18:14.215: ISAKMP:     SA life duration (basic) of 3600
*Dec 28 21:18:14.215: ISAKMP:     SA life type in kilobytes
*Dec 28 21:18:14.215: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Dec 28 21:18:14.215: ISAKMP:     authenticator is HMAC-SHA
*Dec 28 21:18:14.215: ISAKMP (0:15): atts are acceptable.
*Dec 28 21:18:14.215: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 20.1.1.2, remote= 20.1.1.1,
local_proxy= 20.1.1.2/255.255.255.255/47/0 (type=1),
remote_proxy= 20.1.1.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Dec 28 21:18:14.215: ISAKMP (0:15): processing NONCE payload.
message ID = 1098460553
*Dec 28 21:18:14.215: ISAKMP (0:15): processing ID payload.
message ID = 1098460553
*Dec 28 21:18:14.215: ISAKMP (0:15): processing ID payload.
message ID = 1098460553
*Dec 28 21:18:14.215: ISAKMP (0:15): asking for 1 spis from ipsec
*Dec 28 21:18:14.215: ISAKMP (0:15): Node 1098460553, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
*Dec 28 21:18:14.215: ISAKMP (0:15): Old State = IKE_QM_READY
New State = IKE_QM_SPI_STARVE
*Dec 28 21:18:14.235: IPSEC(key_engine): got a queue event...
*Dec 28 21:18:14.235: IPSEC(spi_response): getting spi 488964414 for SA
from 20.1.1.2 to 20.1.1.1 for prot 3
*Dec 28 21:18:14.267: ISAKMP: received ke message (2/1)
```

```

*Dec 28 21:18:14.547: ISAKMP (0:15): sending packet to 20.1.1.1 my_port
500 peer_port 500 (R) QM_IDLE

*Dec 28 21:18:14.547: ISAKMP (0:15): Node 1098460553, Input = IKE_MSG_FROM_IPSEC,
IKE_SPI_REPLY
*Dec 28 21:18:14.547: ISAKMP (0:15): Old State = IKE_QM_SPI_STARVE
New State = IKE_QM_R_QM2
*Dec 28 21:18:14.707: ISAKMP (0:15): received packet from 20.1.1.1
dport 500 sport 500 (R) QM_IDLE
*Dec 28 21:18:14.747: ISAKMP: Locking peer struct 0x18EA370, IPSEC
refcount 1 for for stuff_ke
*Dec 28 21:18:14.747: ISAKMP (0:15): Creating IPsec SAs
*Dec 28 21:18:14.747: inbound SA from 20.1.1.1 to 20.1.1.2
(proxy 20.1.1.1 to 20.1.1.2)
*Dec 28 21:18:14.747: has spi 0x1D25013E and conn_id 2000 and flags 4
*Dec 28 21:18:14.747: lifetime of 3600 seconds
*Dec 28 21:18:14.747: lifetime of 4608000 kilobytes
*Dec 28 21:18:14.747: has client flags 0x0
*Dec 28 21:18:14.747: outbound SA from 20.1.1.2 to 20.1.1.1
(proxy 20.1.1.2 to 20.1.1.1 )
*Dec 28 21:18:14.747: has spi -1829425422 and conn_id 2001 and flags C
*Dec 28 21:18:14.747: lifetime of 3600 seconds
*Dec 28 21:18:14.747: lifetime of 4608000 kilobytes
*Dec 28 21:18:14.747: has client flags 0x0
*Dec 28 21:18:14.747: ISAKMP (0:15): deleting node 1098460553 error FALSE
reason "quick mode done (await())"
*Dec 28 21:18:14.747: ISAKMP (0:15): Node 1098460553, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
*Dec 28 21:18:14.747: ISAKMP (0:15): Old State = IKE_QM_R_QM2
New State = IKE_QM_PHASE2_COMPLETE
*Dec 28 21:18:14.767: IPSEC(key_engine): got a queue event...
*Dec 28 21:18:14.767: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 20.1.1.2, remote= 20.1.1.1,
local_proxy= 20.1.1.2/0.0.0.0/47/0 (type=1),
remote_proxy= 20.1.1.1/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x1D25013E(488964414), conn_id= 2000, keysize= 0, flags= 0x4
*Dec 28 21:18:14.767: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 20.1.1.2, remote= 20.1.1.1,
local_proxy= 20.1.1.2/0.0.0.0/47/0 (type=1),
remote_proxy= 20.1.1.1/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x92F52EF2(2465541874), conn_id= 2001, keysize= 0, flags= 0xC
*Dec 28 21:18:14.767: IPSEC(add mtree): src 20.1.1.2, dest 20.1.1.1, dest_port 0

*Dec 28 21:18:14.767: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.1.1.2, sa_prot= 50,
sa_spi= 0x1D25013E(488964414),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
*Dec 28 21:18:14.767: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.1.1.1, sa_prot= 50,
sa_spi= 0x92F52EF2(2465541874),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001

```

[Gerelateerde informatie](#)

- [IPsec-ondersteuningspagina](#)
- [Technische ondersteuning - Cisco-systemen](#)