strongSwan - Bug #2090

DPD issue when connecting to a Cisco

23.08.2016 18:40 - Alexander Velkov

Status:	Closed	**Start date:**	23.08.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.5.1		
Affected version:	5.3.5	**Resolution:**	Fixed

Description

Hello,

I have a strange behaviour with DPD while rekeying an IKE SA when connecting to a Cisco. The setup is a GRE tunnel with NHRP inside an IPsec tunnel between a StrongSwan peer and a Cisco.

DPD messages are successfully exchanged before rekeying for 60 min. The IKE SA seems to be successfully rekeyed, but still the whole connection gets regenerated right after that. A counter on the Cisco claims that DPDs did not get acknowledged by the StrongSwan peer. I am not sure whether this is a Cisco issue or if the StrongSwan peer does something wrong.

I see the following:

- successful DPD exchanges

```
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
..
*Oct  4 03:25:09.328: ISAKMP (0:134217730): received packet from 172.16.0.3 dport 500 sport 50
0 Global (R) QM_IDLE
```

- rekeying IKE SA

```
*Oct  4 03:25:09.764: ISAKMP (0:0): received packet from 172.16.0.3 dport 500 sport 500 Global
 (N) NEW SA
```

- SA is rekeyed

```
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):SA has been authenticated with 172.16.0.3
```

- error counters

```
*Oct  4 03:25:24.264: ISAKMP (0:134217730): incrementing error counter on sa, attempt 1 of 5:
PEERS_ALIVE_TIMER
...
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):peer 172.16.0.3 not responding!
```

- new SA

```
*Oct  4 03:26:05.472: ISAKMP (0:0): received packet from 172.16.0.3 dport 500 sport 500 Global
 (N) NEW SA
```

Cisco version:

```
vpntest#show version
Cisco IOS Software, 7400 Software (C7400-A3JK9S-M), Version 12.4(16), RELEASE SOFTWARE (fc1)
...
```

StrongSwan version:

```
Status of IKE charon daemon (weakSwan 5.3.5, Linux 3.10.70, armv7l):
  uptime: 3 hours, since Aug 23 10:02:49 2016
  malloc: sbrk 167936, mmap 0, used 148984, free 18952
  worker threads: 27 of 32 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon aes des sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkc
s1 pkcs7 pkcs8 pkcs12 pgp dnskey pem openssl fips-prf gmp xcbc hmac attr kernel-netlink resolve so
cket-default stroke updown xauth-generic unity
Listening IP addresses:
  172.16.0.3
Connections:
 ipsectest$0:  172.16.0.3...172.16.0.22  IKEv1
 ipsectest$0:   local:  [172.16.0.3] uses pre-shared key authentication
 ipsectest$0:   remote: [172.16.0.22] uses pre-shared key authentication
 ipsectest$0:   child:  10.0.3.1/32[gre] === 172.16.0.22/32[gre] TUNNEL
Routed Connections:
 ipsectest$0{1}:  ROUTED, TUNNEL, reqid 1
 ipsectest$0{1}:   10.0.3.1/32[gre] === 172.16.0.22/32[gre]
Security Associations (1 up, 0 connecting):
 ipsectest$0[7]: ESTABLISHED 12 minutes ago, 172.16.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
 ipsectest$0[7]: IKEv1 SPIs: 02190fd65bd0f728_i* 563ec6b41e2aad7d_r, pre-shared key reauthenticati
on in 48 minutes
 ipsectest$0[7]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
 ipsectest$0{8}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c8de512b_i 43240810_o
 ipsectest$0{8}:  3DES_CBC/HMAC_SHA1_96, 22639 bytes_i (221 pkts, 8s ago), 9695 bytes_o (70 pkts,
17s ago), rekeying in 28 minutes
 ipsectest$0{8}:   10.0.3.1/32[gre] === 172.16.0.22/32[gre]
```

StrongSwan logs when rekeying:

```
Aug 23 11:03:57 GWUZC info  charon: [ 1873] NET-20 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:03:57 GWUZC info  charon: [ 1873] ENC-20 parsed INFORMATIONAL_V1 request 1688510787 [ HA
SH N(DPD) ]
Aug 23 11:03:57 GWUZC info  charon: [ 1873] IKE-20 queueing ISAKMP_DPD task
Aug 23 11:03:57 GWUZC info  charon: [ 1873] IKE-20 activating new tasks
Aug 23 11:03:57 GWUZC info  charon: [ 1873] IKE-20   activating ISAKMP_DPD task
Aug 23 11:03:57 GWUZC info  charon: [ 1873] ENC-20 generating INFORMATIONAL_V1 request 507194415 [
 HASH N(DPD_ACK) ]
Aug 23 11:03:57 GWUZC info  charon: [ 1873] NET-20 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (92 bytes)
Aug 23 11:03:57 GWUZC info  charon: [ 1873] IKE-20 activating new tasks
Aug 23 11:03:57 GWUZC info  charon: [ 1873] IKE-20 nothing to initiate

Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 reauthenticating IKE_SA ipsectest$0[1]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 queueing ISAKMP_VENDOR task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 queueing ISAKMP_CERT_PRE task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 queueing MAIN_MODE task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 queueing ISAKMP_CERT_POST task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 queueing ISAKMP_NATD task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 activating new tasks
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25   activating ISAKMP_VENDOR task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25   activating ISAKMP_CERT_PRE task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25   activating MAIN_MODE task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25   activating ISAKMP_CERT_POST task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25   activating ISAKMP_NATD task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 sending XAuth vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 sending DPD vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 sending Cisco Unity vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 sending NAT-T (RFC 3947) vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 sending draft-ietf-ipsec-nat-t-ike-02\n vendor
ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 initiating Main Mode IKE_SA ipsectest$0[2] to 1
72.16.0.22
```

```
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 IKE_SA ipsectest$0[2] state change: CREATED =>
CONNECTING
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-25 generating ID_PROT request 0 [ SA V V V V V ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-25 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (172 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 IKE_SA ipsectest$0[1] state change: ESTABLISHED
 => REKEYING
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 activating new tasks
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-25 nothing to initiate
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-23 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (100 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-23 parsed ID_PROT response 0 [ SA V ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-23 received draft-ietf-ipsec-nat-t-ike-02\n vendor
 ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-23 reinitiating already active tasks
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-23   ISAKMP_VENDOR task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-23   MAIN_MODE task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-23 generating ID_PROT request 0 [ KE No NAT-D NAT-
D ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-23 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (244 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-24 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (304 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-24 parsed ID_PROT response 0 [ KE No V V V V NAT-D
 NAT-D ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-24 received Cisco Unity vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-24 received DPD vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-24 received unknown vendor ID: 88:6a:8d:03:48:11:7
0:f2:10:15:35:ee:b2:df:13:6f
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-24 received XAuth vendor ID
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-24 reinitiating already active tasks
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-24   ISAKMP_VENDOR task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-24   MAIN_MODE task
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-24 generating ID_PROT request 0 [ ID HASH ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-24 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (68 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-01 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (68 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-01 parsed ID_PROT response 0 [ ID HASH ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-01 IKE_SA ipsectest$0[2] established between 172.1
6.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-01 IKE_SA ipsectest$0[2] state change: CONNECTING
=> ESTABLISHED
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-01 scheduling reauthentication in 3660s
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-01 maximum IKE_SA lifetime 4200s
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-01 activating new tasks
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-01 nothing to initiate
Aug 23 11:03:58 GWUZC info  charon: [ 1873] NET-08 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:03:58 GWUZC info  charon: [ 1873] ENC-08 parsed INFORMATIONAL_V1 request 305997078 [ HAS
H N((24576)) ]
Aug 23 11:03:58 GWUZC info  charon: [ 1873] IKE-08 received (24576) notify
Aug 23 11:04:07 GWUZC info  charon: [ 1873] NET-27 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:04:07 GWUZC info  charon: [ 1873] ENC-27 parsed INFORMATIONAL_V1 request 3890636989 [ HA
SH N(DPD) ]
Aug 23 11:04:07 GWUZC info  charon: [ 1873] IKE-27 queueing ISAKMP_DPD task
Aug 23 11:04:07 GWUZC info  charon: [ 1873] IKE-27 activating new tasks
Aug 23 11:04:07 GWUZC info  charon: [ 1873] IKE-27 nothing to initiate
Aug 23 11:04:08 GWUZC info  charon: [ 1873] NET-03 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:04:08 GWUZC info  charon: [ 1873] ENC-03 parsed INFORMATIONAL_V1 request 726861173 [ HAS
H N(DPD) ]
Aug 23 11:04:08 GWUZC info  charon: [ 1873] IKE-03 queueing ISAKMP_DPD task
Aug 23 11:04:08 GWUZC info  charon: [ 1873] IKE-03 activating new tasks
Aug 23 11:04:08 GWUZC info  charon: [ 1873] IKE-03   activating ISAKMP_DPD task
Aug 23 11:04:08 GWUZC info  charon: [ 1873] ENC-03 generating INFORMATIONAL_V1 request 95535039 [
```

```
HASH N(DPD_ACK) ]
Aug 23 11:04:08 GWUZC info  charon: [ 1873] NET-03 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (92 bytes)
Aug 23 11:04:08 GWUZC info  charon: [ 1873] IKE-03 activating new tasks
Aug 23 11:04:08 GWUZC info  charon: [ 1873] IKE-03 nothing to initiate
Aug 23 11:04:08 GWUZC info  charon: [ 1873] IKE-32 IKE_SA ipsectest$0[1] state change: REKEYING =>
 DESTROYING
Aug 23 11:04:27 GWUZC info  charon: [ 1873] NET-10 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:04:27 GWUZC info  charon: [ 1873] ENC-10 parsed INFORMATIONAL_V1 request 3562704299 [ HA
SH N(DPD) ]
Aug 23 11:04:27 GWUZC info  charon: [ 1873] IKE-10 queueing ISAKMP_DPD task
Aug 23 11:04:27 GWUZC info  charon: [ 1873] IKE-10 activating new tasks
Aug 23 11:04:27 GWUZC info  charon: [ 1873] IKE-10   activating ISAKMP_DPD task
Aug 23 11:04:27 GWUZC info  charon: [ 1873] ENC-10 generating INFORMATIONAL_V1 request 3973984537
[ HASH N(DPD_ACK) ]
Aug 23 11:04:27 GWUZC info  charon: [ 1873] NET-10 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (92 bytes)
Aug 23 11:04:27 GWUZC info  charon: [ 1873] IKE-10 activating new tasks
Aug 23 11:04:27 GWUZC info  charon: [ 1873] IKE-10 nothing to initiate
Aug 23 11:04:32 GWUZC info  charon: [ 1873] NET-11 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (84 bytes)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] ENC-11 parsed INFORMATIONAL_V1 request 3720054 [ HASH
D ]
Aug 23 11:04:32 GWUZC info  charon: [ 1873] IKE-11 received DELETE for IKE_SA ipsectest$0[2]
Aug 23 11:04:32 GWUZC info  charon: [ 1873] IKE-11 deleting IKE_SA ipsectest$0[2] between 172.16.0
.3[172.16.0.3]...172.16.0.22[172.16.0.22]
Aug 23 11:04:32 GWUZC info  charon: [ 1873] IKE-11 IKE_SA ipsectest$0[2] state change: ESTABLISHED
 => DELETING
Aug 23 11:04:32 GWUZC info  charon: [ 1873] IKE-11 IKE_SA ipsectest$0[2] state change: DELETING =>
 DELETING
Aug 23 11:04:32 GWUZC info  charon: [ 1873] IKE-11 IKE_SA ipsectest$0[2] state change: DELETING =>
 DESTROYING
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting policy 10.0.3.1/32[gre] === 172.16.0.2
2/32[gre] out  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 policy still used by another CHILD_SA, not remo
ved
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 updating policy 10.0.3.1/32[gre] === 172.16.0.2
2/32[gre] out  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] in  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 policy still used by another CHILD_SA, not remo
ved
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 updating policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] in  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] fwd  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 policy still used by another CHILD_SA, not remo
ved
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 updating policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] fwd  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting policy 10.0.3.1/32[gre] === 172.16.0.2
2/32[gre] out  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 policy still used by another CHILD_SA, not remo
ved
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] in  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 policy still used by another CHILD_SA, not remo
ved
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] fwd  (mark 0/0x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 policy still used by another CHILD_SA, not remo
ved
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting SAD entry with SPI c17c3e5e  (mark 0/0
x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleted SAD entry with SPI c17c3e5e (mark 0/0x0
0000000)
```

```
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleting SAD entry with SPI 23cc9587  (mark 0/0
x00000000)
Aug 23 11:04:32 GWUZC info  charon: [ 1873] KNL-11 deleted SAD entry with SPI 23cc9587 (mark 0/0x0
0000000)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-18 received a XFRM_MSG_ACQUIRE
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-18   XFRMA_TMPL
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-18 creating acquire job for policy 10.0.3.1/32[gre
] === 172.16.0.22/32[gre] with reqid {1}
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 queueing ISAKMP_VENDOR task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 queueing ISAKMP_CERT_PRE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 queueing MAIN_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 queueing ISAKMP_CERT_POST task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 queueing ISAKMP_NATD task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 queueing QUICK_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 activating new tasks
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18   activating ISAKMP_VENDOR task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18   activating ISAKMP_CERT_PRE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18   activating MAIN_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18   activating ISAKMP_CERT_POST task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18   activating ISAKMP_NATD task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 sending XAuth vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 sending DPD vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 sending Cisco Unity vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 sending NAT-T (RFC 3947) vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 sending draft-ietf-ipsec-nat-t-ike-02\n vendor
ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 initiating Main Mode IKE_SA ipsectest$0[3] to 1
72.16.0.22
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-18 IKE_SA ipsectest$0[3] state change: CREATED =>
CONNECTING
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-18 generating ID_PROT request 0 [ SA V V V V V ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-18 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (172 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-21 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (100 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-21 parsed ID_PROT response 0 [ SA V ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-21 received draft-ietf-ipsec-nat-t-ike-02\n vendor
 ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-21 reinitiating already active tasks
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-21   ISAKMP_VENDOR task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-21   MAIN_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-21 generating ID_PROT request 0 [ KE No NAT-D NAT-
D ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-21 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (244 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-17 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (304 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-17 parsed ID_PROT response 0 [ KE No V V V V NAT-D
 NAT-D ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-17 received Cisco Unity vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-17 received DPD vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-17 received unknown vendor ID: 88:6a:8d:03:2e:7b:c
6:5c:68:0d:7c:0f:84:5e:fd:57
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-17 received XAuth vendor ID
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-17 reinitiating already active tasks
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-17   ISAKMP_VENDOR task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-17   MAIN_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-17 generating ID_PROT request 0 [ ID HASH N(INITIA
L_CONTACT) ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-17 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (100 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-13 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (68 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-13 parsed ID_PROT response 0 [ ID HASH ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-13 IKE_SA ipsectest$0[3] established between 172.1
6.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-13 IKE_SA ipsectest$0[3] state change: CONNECTING
```

```
=> ESTABLISHED
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-13 scheduling reauthentication in 3660s
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-13 maximum IKE_SA lifetime 4200s
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-13 activating new tasks
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-13   activating QUICK_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-13 got SPI ca88ba88
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-13 generating QUICK_MODE request 3887226399 [ HASH
 SA No KE ID ID ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-13 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (300 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-20 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-20 parsed INFORMATIONAL_V1 request 3689230329 [ HA
SH N((24576)) ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-20 received (24576) notify
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-25 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (316 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-25 parsed QUICK_MODE response 3887226399 [ HASH SA
 No KE ID ID N((24576)) ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 adding SAD entry with SPI ca88ba88 and reqid {1
}  (mark 0/0x00000000)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25   using encryption algorithm 3DES_CBC with key
size 192
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25   using integrity algorithm HMAC_SHA1_96 with k
ey size 160
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25   using replay window of 32 packets
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 adding SAD entry with SPI 813c88c9 and reqid {1
}  (mark 0/0x00000000)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25   using encryption algorithm 3DES_CBC with key
size 192
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25   using integrity algorithm HMAC_SHA1_96 with k
ey size 160
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25   using replay window of 32 packets
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 policy 10.0.3.1/32[gre] === 172.16.0.22/32[gre]
 out  (mark 0/0x00000000) already exists, increasing refcount
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 policy 172.16.0.22/32[gre] === 10.0.3.1/32[gre]
 in  (mark 0/0x00000000) already exists, increasing refcount
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 policy 172.16.0.22/32[gre] === 10.0.3.1/32[gre]
 fwd  (mark 0/0x00000000) already exists, increasing refcount
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 policy 10.0.3.1/32[gre] === 172.16.0.22/32[gre]
 out  (mark 0/0x00000000) already exists, increasing refcount
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 updating policy 10.0.3.1/32[gre] === 172.16.0.2
2/32[gre] out  (mark 0/0x00000000)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 policy 172.16.0.22/32[gre] === 10.0.3.1/32[gre]
 in  (mark 0/0x00000000) already exists, increasing refcount
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 updating policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] in  (mark 0/0x00000000)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 policy 172.16.0.22/32[gre] === 10.0.3.1/32[gre]
 fwd  (mark 0/0x00000000) already exists, increasing refcount
Aug 23 11:04:54 GWUZC info  charon: [ 1873] KNL-25 updating policy 172.16.0.22/32[gre] === 10.0.3.
1/32[gre] fwd  (mark 0/0x00000000)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-25 CHILD_SA ipsectest$0{4} established with SPIs c
a88ba88_i 813c88c9_o and TS 10.0.3.1/32[gre] === 172.16.0.22/32[gre]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-25 reinitiating already active tasks
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-25   QUICK_MODE task
Aug 23 11:04:54 GWUZC info  charon: [ 1873] ENC-25 generating QUICK_MODE request 3887226399 [ HASH
 ]
Aug 23 11:04:54 GWUZC info  charon: [ 1873] NET-25 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (60 bytes)
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-25 activating new tasks
Aug 23 11:04:54 GWUZC info  charon: [ 1873] IKE-25 nothing to initiate
Aug 23 11:05:04 GWUZC info  charon: [ 1873] NET-26 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:05:04 GWUZC info  charon: [ 1873] ENC-26 parsed INFORMATIONAL_V1 request 3408421384 [ HA
SH N(DPD) ]
Aug 23 11:05:04 GWUZC info  charon: [ 1873] IKE-26 queueing ISAKMP_DPD task
Aug 23 11:05:04 GWUZC info  charon: [ 1873] IKE-26 activating new tasks
```

```
Aug 23 11:05:04 GWUZC info  charon: [ 1873] IKE-26   activating ISAKMP_DPD task
Aug 23 11:05:04 GWUZC info  charon: [ 1873] ENC-26 generating INFORMATIONAL_V1 request 1717308230
[ HASH N(DPD_ACK) ]
Aug 23 11:05:04 GWUZC info  charon: [ 1873] NET-26 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (92 bytes)
Aug 23 11:05:04 GWUZC info  charon: [ 1873] IKE-26 activating new tasks
Aug 23 11:05:04 GWUZC info  charon: [ 1873] IKE-26 nothing to initiate
Aug 23 11:05:13 GWUZC info  charon: [ 1873] NET-29 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:05:13 GWUZC info  charon: [ 1873] ENC-29 parsed INFORMATIONAL_V1 request 993124506 [ HAS
H N(DPD) ]
Aug 23 11:05:13 GWUZC info  charon: [ 1873] IKE-29 queueing ISAKMP_DPD task
Aug 23 11:05:13 GWUZC info  charon: [ 1873] IKE-29 activating new tasks
Aug 23 11:05:13 GWUZC info  charon: [ 1873] IKE-29   activating ISAKMP_DPD task
Aug 23 11:05:13 GWUZC info  charon: [ 1873] ENC-29 generating INFORMATIONAL_V1 request 2854307685
[ HASH N(DPD_ACK) ]
Aug 23 11:05:13 GWUZC info  charon: [ 1873] NET-29 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (92 bytes)
Aug 23 11:05:13 GWUZC info  charon: [ 1873] IKE-29 activating new tasks
Aug 23 11:05:13 GWUZC info  charon: [ 1873] IKE-29 nothing to initiate
Aug 23 11:05:33 GWUZC info  charon: [ 1873] NET-03 received packet: from 172.16.0.22[500] to 172.1
6.0.3[500] (92 bytes)
Aug 23 11:05:33 GWUZC info  charon: [ 1873] ENC-03 parsed INFORMATIONAL_V1 request 209377410 [ HAS
H N(DPD) ]
Aug 23 11:05:33 GWUZC info  charon: [ 1873] IKE-03 queueing ISAKMP_DPD task
Aug 23 11:05:33 GWUZC info  charon: [ 1873] IKE-03 activating new tasks
Aug 23 11:05:33 GWUZC info  charon: [ 1873] IKE-03   activating ISAKMP_DPD task
Aug 23 11:05:33 GWUZC info  charon: [ 1873] ENC-03 generating INFORMATIONAL_V1 request 2375083279
[ HASH N(DPD_ACK) ]
Aug 23 11:05:33 GWUZC info  charon: [ 1873] NET-03 sending packet: from 172.16.0.3[500] to 172.16.
0.22[500] (92 bytes)
Aug 23 11:05:33 GWUZC info  charon: [ 1873] IKE-03 activating new tasks
Aug 23 11:05:33 GWUZC info  charon: [ 1873] IKE-03 nothing to initiate
```

Cisco logs when rekeying:

```
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = 1688510787
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1): seq. no 0x6B17EC2D
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1):purging node 1688510787
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALIVE
*Oct  4 03:25:09.324: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:09.328: ISAKMP (0:134217730): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) QM_IDLE
*Oct  4 03:25:09.328: ISAKMP: set new node 507194415 to QM_IDLE
*Oct  4 03:25:09.328: ISAKMP:(0:2:SW:1): processing HASH payload. message ID = 507194415
*Oct  4 03:25:09.328: ISAKMP:(0:2:SW:1): processing NOTIFY DPD/R_U_THERE_ACK protocol 1
        spi 0, message ID = 507194415, sa = 64352898
*Oct  4 03:25:09.328: ISAKMP:(0:2:SW:1): DPD/R_U_THERE_ACK received from peer 172.16.0.3, sequence
 0x6B17EC2D
*Oct  4 03:25:09.328: ISAKMP:(0:2:SW:1):deleting node 507194415 error FALSE reason "Informational
(in) state 1"
*Oct  4 03:25:09.328: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
*Oct  4 03:25:09.328: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:09.764: ISAKMP (0:0): received packet from 172.16.0.3 dport 500 sport 500 Global (N)
 NEW SA
*Oct  4 03:25:09.764: ISAKMP: Found a peer struct for 172.16.0.3, peer port 500
*Oct  4 03:25:09.764: ISAKMP: Locking peer struct 0x655D4C08, IKE refcount 2 for crypto_isakmp_pro
cess_block
*Oct  4 03:25:09.764: ISAKMP: local port 500, remote port 500
*Oct  4 03:25:09.764: ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 64395
BDC
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
```

```
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0):Old State = IKE_READY  New State = IKE_R_MM1

*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): processing SA payload. message ID = 0
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): vendor ID seems Unity/DPD but major 215 mismatch
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): vendor ID is XAUTH
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): vendor ID is DPD
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): vendor ID is Unity
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0):found peer pre-shared key matching 172.16.0.3
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0): local preshared key found
*Oct  4 03:25:09.764: ISAKMP : Scanning profiles for xauth ... PSK-Profile0
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 1 against priority 1 policy
*Oct  4 03:25:09.764: ISAKMP:      encryption 3DES-CBC
*Oct  4 03:25:09.764: ISAKMP:      hash SHA
*Oct  4 03:25:09.764: ISAKMP:      default group 2
*Oct  4 03:25:09.764: ISAKMP:      auth pre-share
*Oct  4 03:25:09.764: ISAKMP:      life type in seconds
*Oct  4 03:25:09.764: ISAKMP:      life duration (basic) of 4200
*Oct  4 03:25:09.764: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1): vendor ID is NAT-T v2
*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM1  New State = IKE_R_MM1

*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1): constructed NAT-T vendor-02 ID
*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_SA_SETUP
*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  4 03:25:09.788: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM1  New State = IKE_R_MM2

*Oct  4 03:25:09.824: ISAKMP (0:134217731): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) MM_SA_SETUP
*Oct  4 03:25:09.824: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:25:09.824: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM2  New State = IKE_R_MM3

*Oct  4 03:25:09.824: ISAKMP:(0:3:SW:1): processing KE payload. message ID = 0
*Oct  4 03:25:09.852: ISAKMP:(0:3:SW:1): processing NONCE payload. message ID = 0
*Oct  4 03:25:09.852: ISAKMP:(0:3:SW:1):found peer pre-shared key matching 172.16.0.3
*Oct  4 03:25:09.852: ISAKMP:(0:3:SW:1):SKEYID state generated
*Oct  4 03:25:09.852: ISAKMP:received payload type 20
*Oct  4 03:25:09.852: ISAKMP:received payload type 20
*Oct  4 03:25:09.852: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  4 03:25:09.852: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM3  New State = IKE_R_MM3

*Oct  4 03:25:09.852: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_KEY_EXCH
*Oct  4 03:25:09.856: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  4 03:25:09.856: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM3  New State = IKE_R_MM4

*Oct  4 03:25:09.892: ISAKMP (0:134217731): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) MM_KEY_EXCH
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM4  New State = IKE_R_MM5

*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1): processing ID payload. message ID = 0
*Oct  4 03:25:09.892: ISAKMP (0:134217731): ID payload
        next-payload : 8
        type         : 1
        address      : 172.16.0.3
        protocol     : 0
        port         : 0
        length       : 12
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):: peer matches PSK-Profile0 profile
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Found ADDRESS key in keyring PSK-Key0
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Unable to copy name into saved_grpname
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1): processing HASH payload. message ID = 0
```

```
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):SA authentication status:
        authenticated
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):SA has been authenticated with 172.16.0.3
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):IKE_DPD is enabled, initializing timers
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM5  New State = IKE_R_MM5

*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):SA is doing pre-shared key authentication using id type ID
_IPV4_ADDR
*Oct  4 03:25:09.892: ISAKMP (0:134217731): ID payload
        next-payload : 8
        type         : 1
        address      : 172.16.0.22
        protocol     : 17
        port         : 500
        length       : 12
*Oct  4 03:25:09.892: ISAKMP:(0:3:SW:1):Total payload length: 12
*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_KEY_EXCH
*Oct  4 03:25:09.896: ISAKMP: set new node 305997078 to QM_IDLE
*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1):Sending NOTIFY RESPONDER_LIFETIME protocol 1
        spi 1698331192, message ID = 305997078
*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_KEY_EXCH
*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1):purging node 305997078
*Oct  4 03:25:09.896: ISAKMP: Sending phase 1 responder lifetime 4200

*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Oct  4 03:25:09.896: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:10.668: ISAKMP:(0:2:SW:1):purging node -475850631
*Oct  4 03:25:19.264: ISAKMP: set new node -404330307 to QM_IDLE
*Oct  4 03:25:19.264: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = -404330307
*Oct  4 03:25:19.264: ISAKMP:(0:2:SW:1): seq. no 0x6B17EC2E
*Oct  4 03:25:19.264: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:19.264: ISAKMP:(0:2:SW:1):purging node -404330307
*Oct  4 03:25:19.264: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALIVE
*Oct  4 03:25:19.264: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:19.892: ISAKMP: set new node 726861173 to QM_IDLE
*Oct  4 03:25:19.892: ISAKMP:(0:3:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = 726861173
*Oct  4 03:25:19.892: ISAKMP:(0:3:SW:1): seq. no 0x6B17EC2F
*Oct  4 03:25:19.892: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:19.892: ISAKMP:(0:3:SW:1):purging node 726861173
*Oct  4 03:25:19.892: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALIVE
*Oct  4 03:25:19.892: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:19.896: ISAKMP (0:134217731): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) QM_IDLE
*Oct  4 03:25:19.896: ISAKMP: set new node 95535039 to QM_IDLE
*Oct  4 03:25:19.896: ISAKMP:(0:3:SW:1): processing HASH payload. message ID = 95535039
*Oct  4 03:25:19.896: ISAKMP:(0:3:SW:1): processing NOTIFY DPD/R_U_THERE_ACK protocol 1
        spi 0, message ID = 95535039, sa = 64395BDC
*Oct  4 03:25:19.896: ISAKMP:(0:3:SW:1): DPD/R_U_THERE_ACK received from peer 172.16.0.3, sequence
 0x6B17EC2F
*Oct  4 03:25:19.896: ISAKMP:(0:3:SW:1):deleting node 95535039 error FALSE reason "Informational (
in) state 1"
*Oct  4 03:25:19.896: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
*Oct  4 03:25:19.896: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
```

```
*Oct  4 03:25:20.492: ISAKMP:(0:2:SW:1):purging node 1913664192
*Oct  4 03:25:24.264: ISAKMP (0:134217730): incrementing error counter on sa, attempt 1 of 5: PEER
S_ALIVE_TIMER
*Oct  4 03:25:24.264: ISAKMP: set new node 1871749078 to QM_IDLE
*Oct  4 03:25:24.264: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = 1871749078
*Oct  4 03:25:24.264: ISAKMP:(0:2:SW:1): seq. no 0x6B17EC30
*Oct  4 03:25:24.264: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:24.264: ISAKMP:(0:2:SW:1):purging node 1871749078
*Oct  4 03:25:24.264: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_PEERS_ALIVE
*Oct  4 03:25:24.264: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:26.532: NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 105
*Oct  4 03:25:26.532:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Oct  4 03:25:26.532:      shtl: 4(NSAP), sstl: 0(NSAP)
*Oct  4 03:25:26.532:  (M) flags: "unique", reqid: 4
*Oct  4 03:25:26.532:      src NBMA: 10.0.3.1
*Oct  4 03:25:26.532:      src protocol: 10.4.4.4, dst protocol: 10.4.4.1
*Oct  4 03:25:26.532:  (C-1) code: no error(0)
*Oct  4 03:25:26.532:        prefix: 32, mtu: 1500, hd_time: 60
*Oct  4 03:25:26.532:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
*Oct  4 03:25:26.532: NHRP: Cache update for target 10.4.4.4/32 next-hop 10.4.4.4
*Oct  4 03:25:26.532:            10.0.3.1
*Oct  4 03:25:26.532: NHRP: Send Registration Reply via Tunnel0 vrf 0, packet size: 125
*Oct  4 03:25:26.532:  src: 10.4.4.1, dst: 10.4.4.4
*Oct  4 03:25:26.532:  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
*Oct  4 03:25:26.532:      shtl: 4(NSAP), sstl: 0(NSAP)
*Oct  4 03:25:26.532:  (M) flags: "unique", reqid: 4
*Oct  4 03:25:26.532:      src NBMA: 10.0.3.1
*Oct  4 03:25:26.532:      src protocol: 10.4.4.4, dst protocol: 10.4.4.1
*Oct  4 03:25:26.532:  (C-1) code: no error(0)
*Oct  4 03:25:26.532:        prefix: 32, mtu: 1500, hd_time: 60
*Oct  4 03:25:26.532:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
*Oct  4 03:25:29.264: ISAKMP (0:134217730): incrementing error counter on sa, attempt 2 of 5: PEER
S_ALIVE_TIMER
*Oct  4 03:25:29.264: ISAKMP: set new node 1103555729 to QM_IDLE
*Oct  4 03:25:29.264: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = 1103555729
*Oct  4 03:25:29.264: ISAKMP:(0:2:SW:1): seq. no 0x6B17EC31
*Oct  4 03:25:29.264: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:29.264: ISAKMP:(0:2:SW:1):purging node 1103555729
*Oct  4 03:25:29.264: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_PEERS_ALIVE
*Oct  4 03:25:29.264: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:30.364: ISAKMP:(0:2:SW:1):purging node -1773467410
*Oct  4 03:25:34.264: ISAKMP (0:134217730): incrementing error counter on sa, attempt 3 of 5: PEER
S_ALIVE_TIMER
*Oct  4 03:25:34.264: ISAKMP: set new node 1178091947 to QM_IDLE
*Oct  4 03:25:34.264: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = 1178091947
*Oct  4 03:25:34.264: ISAKMP:(0:2:SW:1): seq. no 0x6B17EC32
*Oct  4 03:25:34.264: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:34.264: ISAKMP:(0:2:SW:1):purging node 1178091947
*Oct  4 03:25:34.264: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_PEERS_ALIVE
*Oct  4 03:25:34.264: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:38.908: ISAKMP: set new node -732262997 to QM_IDLE
*Oct  4 03:25:38.908: ISAKMP:(0:3:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = -732262997
*Oct  4 03:25:38.908: ISAKMP:(0:3:SW:1): seq. no 0x6B17EC33
*Oct  4 03:25:38.908: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:38.908: ISAKMP:(0:3:SW:1):purging node -732262997
*Oct  4 03:25:38.908: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALIVE
```

```
*Oct  4 03:25:38.908: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:38.912: ISAKMP (0:134217731): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) QM_IDLE
*Oct  4 03:25:38.912: ISAKMP: set new node -320982759 to QM_IDLE
*Oct  4 03:25:38.912: ISAKMP:(0:3:SW:1): processing HASH payload. message ID = -320982759
*Oct  4 03:25:38.912: ISAKMP:(0:3:SW:1): processing NOTIFY DPD/R_U_THERE_ACK protocol 1
        spi 0, message ID = -320982759, sa = 64395BDC
*Oct  4 03:25:38.912: ISAKMP:(0:3:SW:1): DPD/R_U_THERE_ACK received from peer 172.16.0.3, sequence
 0x6B17EC33
*Oct  4 03:25:38.912: ISAKMP:(0:3:SW:1):deleting node -320982759 error FALSE reason "Informational
 (in) state 1"
*Oct  4 03:25:38.912: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
*Oct  4 03:25:38.912: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:39.264: ISAKMP (0:134217730): incrementing error counter on sa, attempt 4 of 5: PEER
S_ALIVE_TIMER
*Oct  4 03:25:39.264: ISAKMP: set new node 1698205467 to QM_IDLE
*Oct  4 03:25:39.264: ISAKMP:(0:2:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = 1698205467
*Oct  4 03:25:39.264: ISAKMP:(0:2:SW:1): seq. no 0x6B17EC34
*Oct  4 03:25:39.264: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:39.264: ISAKMP:(0:2:SW:1):purging node 1698205467
*Oct  4 03:25:39.264: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_PEERS_ALIVE
*Oct  4 03:25:39.264: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:25:44.264: ISAKMP (0:134217730): incrementing error counter on sa, attempt 5 of 5: PEER
S_ALIVE_TIMER
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):peer 172.16.0.3 not responding!
*Oct  4 03:25:44.264: ISAKMP:(0:3:SW:1):received initial contact, deleting SA
*Oct  4 03:25:44.264: ISAKMP:(0:3:SW:1):peer does not do paranoid keepalives.

*Oct  4 03:25:44.264: ISAKMP:(0:3:SW:1):deleting SA reason "P1 errcounter exceeded (PEERS_ALIVE_TI
MER)" state (R) QM_IDLE       (peer 172.16.0.3)
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):peer does not do paranoid keepalives.

*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):deleting SA reason "P1 errcounter exceeded (PEERS_ALIVE_TI
MER)" state (R) QM_IDLE       (peer 172.16.0.3)
*Oct  4 03:25:44.264: ISAKMP: set new node 1911970589 to QM_IDLE
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):purging node 1911970589
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_PEERS_ALIVE
*Oct  4 03:25:44.264: ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_DEST_SA

*Oct  4 03:25:44.264: ISAKMP: Unlocking IPSEC struct 0x655D4C08 from delete_siblings, count 0
*Oct  4 03:25:44.264: NHRP: Resetting hold timer of 10.4.4.4/32 to 5000 milliseconds
*Oct  4 03:25:44.264: ISAKMP: received ke message (3/1)
*Oct  4 03:25:44.264: ISAKMP: ignoring request to send delete notify (no ISAKMP sa) src 172.16.0.2
2 dst 172.16.0.3 for SPI 0x23CC9587
*Oct  4 03:25:44.264: ISAKMP: set new node 3720054 to QM_IDLE
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):purging node 3720054
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_DEST_SA

*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):deleting SA reason "P1 errcounter exceeded (PEERS_ALIVE_TI
MER)" state (R) QM_IDLE       (peer 172.16.0.3)
*Oct  4 03:25:44.268: ISAKMP: Unlocking IKE struct 0x655D4C08 for isadb_mark_sa_deleted(), count 1
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):deleting node 186501559 error FALSE reason "IKE deleted"
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):deleting node 507194415 error FALSE reason "IKE deleted"
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):Old State = IKE_DEST_SA  New State = IKE_DEST_SA

*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):deleting SA reason "No reason" state (R) MM_NO_STATE (peer
```

```
 172.16.0.3)
*Oct  4 03:25:44.268: ISAKMP:(0:0:N/A:0):Can't decrement IKE Call Admisstion Control stat incoming
_negotiating since it's already 0.
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):deleting node 186501559 error FALSE reason "IKE deleted"
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):deleting node 507194415 error FALSE reason "IKE deleted"
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:25:44.268: ISAKMP:(0:2:SW:1):Old State = IKE_DEST_SA  New State = IKE_DEST_SA

*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):deleting SA reason "No reason" state (R) QM_IDLE       (pe
er 172.16.0.3)
*Oct  4 03:25:44.268: ISAKMP: Unlocking IKE struct 0x655D4C08 for isadb_mark_sa_deleted(), count 0
*Oct  4 03:25:44.268: crypto_ikmp_dpd_refcount_zero: Freeing dpd profile_name PSK-Profile0
*Oct  4 03:25:44.268: ISAKMP: Deleting peer node by peer_reap for 172.16.0.3: 655D4C08
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):deleting node 95535039 error FALSE reason "IKE deleted"
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):deleting node -320982759 error FALSE reason "IKE deleted"
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:25:44.268: ISAKMP:(0:3:SW:1):Old State = IKE_DEST_SA  New State = IKE_DEST_SA

*Oct  4 03:25:49.264: NHRP: Hold timer expired for 10.4.4.4/32
*Oct  4 03:25:49.264: NHRP: Deleting dynamic entry for 10.4.4.4/32 interface Tunnel0
*Oct  4 03:25:49.264: ISAKMP: received ke message (3/1)
*Oct  4 03:25:49.264: ISAKMP:(0:3:SW:1):peer does not do paranoid keepalives.

*Oct  4 03:25:49.264: ISAKMP:(0:2:SW:1):peer does not do paranoid keepalives.

*Oct  4 03:26:05.472: ISAKMP (0:0): received packet from 172.16.0.3 dport 500 sport 500 Global (N)
 NEW SA
*Oct  4 03:26:05.472: ISAKMP: Created a peer struct for 172.16.0.3, peer port 500
*Oct  4 03:26:05.472: ISAKMP: New peer created peer = 0x6548C174 peer_handle = 0x800002AE
*Oct  4 03:26:05.472: ISAKMP: Locking peer struct 0x6548C174, IKE refcount 1 for crypto_isakmp_pro
cess_block
*Oct  4 03:26:05.472: ISAKMP: local port 500, remote port 500
*Oct  4 03:26:05.472: ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 64356
8AC
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0):Old State = IKE_READY  New State = IKE_R_MM1

*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): processing SA payload. message ID = 0
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): vendor ID seems Unity/DPD but major 215 mismatch
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): vendor ID is XAUTH
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): vendor ID is DPD
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): processing vendor id payload
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): vendor ID is Unity
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0):found peer pre-shared key matching 172.16.0.3
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0): local preshared key found
*Oct  4 03:26:05.476: ISAKMP : Scanning profiles for xauth ... PSK-Profile0
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 1 against priority 1 policy
*Oct  4 03:26:05.476: ISAKMP:      encryption 3DES-CBC
*Oct  4 03:26:05.476: ISAKMP:      hash SHA
*Oct  4 03:26:05.476: ISAKMP:      default group 2
*Oct  4 03:26:05.476: ISAKMP:      auth pre-share
*Oct  4 03:26:05.476: ISAKMP:      life type in seconds
*Oct  4 03:26:05.476: ISAKMP:      life duration (basic) of 4200
*Oct  4 03:26:05.476: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Oct  4 03:26:05.496: ISAKMP:(0:4:SW:1): vendor ID is NAT-T v2
*Oct  4 03:26:05.496: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  4 03:26:05.496: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM1  New State = IKE_R_MM1

*Oct  4 03:26:05.496: ISAKMP:(0:4:SW:1): constructed NAT-T vendor-02 ID
*Oct  4 03:26:05.500: ISAKMP:(0:4:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_SA_SETUP
*Oct  4 03:26:05.500: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  4 03:26:05.500: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM1  New State = IKE_R_MM2

*Oct  4 03:26:05.536: ISAKMP (0:134217732): received packet from 172.16.0.3 dport 500 sport 500 Gl
```

```
obal (R) MM_SA_SETUP
*Oct  4 03:26:05.540: ISAKMP:(0:4:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:26:05.540: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM2  New State = IKE_R_MM3

*Oct  4 03:26:05.540: ISAKMP:(0:4:SW:1): processing KE payload. message ID = 0
*Oct  4 03:26:05.564: ISAKMP:(0:4:SW:1): processing NONCE payload. message ID = 0
*Oct  4 03:26:05.564: ISAKMP:(0:4:SW:1):found peer pre-shared key matching 172.16.0.3
*Oct  4 03:26:05.568: ISAKMP:(0:4:SW:1):SKEYID state generated
*Oct  4 03:26:05.568: ISAKMP:received payload type 20
*Oct  4 03:26:05.568: ISAKMP:received payload type 20
*Oct  4 03:26:05.568: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  4 03:26:05.568: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM3  New State = IKE_R_MM3

*Oct  4 03:26:05.568: ISAKMP:(0:4:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_KEY_EXCH
*Oct  4 03:26:05.568: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  4 03:26:05.568: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM3  New State = IKE_R_MM4

*Oct  4 03:26:05.604: ISAKMP (0:134217732): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) MM_KEY_EXCH
*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM4  New State = IKE_R_MM5

*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1): processing ID payload. message ID = 0
*Oct  4 03:26:05.604: ISAKMP (0:134217732): ID payload
        next-payload : 8
        type         : 1
        address      : 172.16.0.3
        protocol     : 0
        port         : 0
        length       : 12
*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1):: peer matches PSK-Profile0 profile
*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1):Found ADDRESS key in keyring PSK-Key0
*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1):Unable to copy name into saved_grpname
*Oct  4 03:26:05.604: ISAKMP:(0:4:SW:1): processing HASH payload. message ID = 0
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = 0, sa = 643568AC
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):SA authentication status:
        authenticated
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.16.0.22 remote 172.16.0.3 remote port 500
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):SA authentication status:
        authenticated
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):SA has been authenticated with 172.16.0.3
*Oct  4 03:26:05.608: ISAKMP: Trying to insert a peer 172.16.0.22/172.16.0.3/500/,  and inserted s
uccessfully 6548C174.
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):IKE_DPD is enabled, initializing timers
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM5  New State = IKE_R_MM5

*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):SA is doing pre-shared key authentication using id type ID
_IPV4_ADDR
*Oct  4 03:26:05.608: ISAKMP (0:134217732): ID payload
        next-payload : 8
        type         : 1
        address      : 172.16.0.22
        protocol     : 17
        port         : 500
        length       : 12
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Total payload length: 12
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_KEY_EXCH
*Oct  4 03:26:05.608: ISAKMP: set new node -605736967 to QM_IDLE
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Sending NOTIFY RESPONDER_LIFETIME protocol 1
        spi 1698331192, message ID = -605736967
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) MM_KEY_EXCH
```

```
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):purging node -605736967
*Oct  4 03:26:05.608: ISAKMP: Sending phase 1 responder lifetime 4200

*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Oct  4 03:26:05.608: ISAKMP:(0:4:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:26:05.648: ISAKMP (0:134217732): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) QM_IDLE
*Oct  4 03:26:05.648: ISAKMP: set new node -407740897 to QM_IDLE
*Oct  4 03:26:05.648: ISAKMP:(0:4:SW:1): processing HASH payload. message ID = -407740897
*Oct  4 03:26:05.648: ISAKMP:(0:4:SW:1): processing SA payload. message ID = -407740897
*Oct  4 03:26:05.648: ISAKMP:(0:4:SW:1):Checking IPSec proposal 0
*Oct  4 03:26:05.648: ISAKMP: transform 1, ESP_3DES
*Oct  4 03:26:05.648: ISAKMP:   attributes in transform:
*Oct  4 03:26:05.648: ISAKMP:      authenticator is HMAC-SHA
*Oct  4 03:26:05.648: ISAKMP:      group is 2
*Oct  4 03:26:05.648: ISAKMP:      encaps is 1 (Tunnel)
*Oct  4 03:26:05.648: ISAKMP:      SA life type in seconds
*Oct  4 03:26:05.648: ISAKMP:      SA life duration (basic) of 3600
*Oct  4 03:26:05.648: ISAKMP:(0:4:SW:1):atts are acceptable.
*Oct  4 03:26:05.648: insert of map into mapdb AVL failed, map + ace pair already exists on the ma
pdb
*Oct  4 03:26:05.672: ISAKMP:(0:4:SW:1): processing NONCE payload. message ID = -407740897
*Oct  4 03:26:05.672: ISAKMP:(0:4:SW:1): processing KE payload. message ID = -407740897
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1): processing ID payload. message ID = -407740897
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1): processing ID payload. message ID = -407740897
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1): asking for 1 spis from ipsec
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1):Node -407740897, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1):Old State = IKE_QM_READY  New State = IKE_QM_SPI_STARVE
*Oct  4 03:26:05.700: ISAKMP: received ke message (2/1)
*Oct  4 03:26:05.700: ISAKMP: Locking peer struct 0x6548C174, IPSEC refcount 1 for for stuff_ke
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1): Creating IPSec SAs
*Oct  4 03:26:05.700:         inbound SA from 172.16.0.3 to 172.16.0.22 (f/i)  0/ 0
        (proxy 10.0.3.1 to 172.16.0.22)
*Oct  4 03:26:05.700:         has spi 0x813C88C9 and conn_id 0 and flags 23
*Oct  4 03:26:05.700:         lifetime of 3600 seconds
*Oct  4 03:26:05.700:         has client flags 0x0
*Oct  4 03:26:05.700:         outbound SA from 172.16.0.22 to 172.16.0.3 (f/i) 0/0
        (proxy 172.16.0.22 to 10.0.3.1)
*Oct  4 03:26:05.700:         has spi -897009016 and conn_id 0 and flags 2B
*Oct  4 03:26:05.700:         lifetime of 3600 seconds
*Oct  4 03:26:05.700:         has client flags 0x0
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:26:05.700: ISAKMP:(0:4:SW:1):Node -407740897, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPL
Y
*Oct  4 03:26:05.704: ISAKMP:(0:4:SW:1):Old State = IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2
*Oct  4 03:26:05.704: ISAKMP: Locking peer struct 0x6548C174, IPSEC refcount 2 for from create_tra
nsforms
*Oct  4 03:26:05.704: ISAKMP: Unlocking IPSEC struct 0x6548C174 from create_transforms, count 1
*Oct  4 03:26:05.748: ISAKMP (0:134217732): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) QM_IDLE
*Oct  4 03:26:05.748: ISAKMP:(0:4:SW:1):deleting node -407740897 error FALSE reason "QM done (awai
t)"
*Oct  4 03:26:05.748: ISAKMP:(0:4:SW:1):Node -407740897, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Oct  4 03:26:05.748: ISAKMP:(0:4:SW:1):Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLE
TE
*Oct  4 03:26:15.608: ISAKMP: set new node -886545912 to QM_IDLE
*Oct  4 03:26:15.608: ISAKMP:(0:4:SW:1):Sending NOTIFY DPD/R_U_THERE protocol 1
        spi 1698331216, message ID = -886545912
*Oct  4 03:26:15.608: ISAKMP:(0:4:SW:1): seq. no 0x3C70A723
*Oct  4 03:26:15.608: ISAKMP:(0:4:SW:1): sending packet to 172.16.0.3 my_port 500 peer_port 500 (R
) QM_IDLE
*Oct  4 03:26:15.608: ISAKMP:(0:4:SW:1):purging node -886545912
```

```
*Oct  4 03:26:15.608: ISAKMP:(0:4:SW:1):Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALIVE
*Oct  4 03:26:15.608: ISAKMP:(0:4:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

*Oct  4 03:26:15.612: ISAKMP (0:134217732): received packet from 172.16.0.3 dport 500 sport 500 Gl
obal (R) QM_IDLE
*Oct  4 03:26:15.612: ISAKMP: set new node 1717308230 to QM_IDLE
*Oct  4 03:26:15.612: ISAKMP:(0:4:SW:1): processing HASH payload. message ID = 1717308230
*Oct  4 03:26:15.612: ISAKMP:(0:4:SW:1): processing NOTIFY DPD/R_U_THERE_ACK protocol 1
        spi 0, message ID = 1717308230, sa = 643568AC
*Oct  4 03:26:15.612: ISAKMP:(0:4:SW:1): DPD/R_U_THERE_ACK received from peer 172.16.0.3, sequence
 0x3C70A723
*Oct  4 03:26:15.612: ISAKMP:(0:4:SW:1):deleting node 1717308230 error FALSE reason "Informational
 (in) state 1"
*Oct  4 03:26:15.612: ISAKMP:(0:4:SW:1):Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
*Oct  4 03:26:15.612: ISAKMP:(0:4:SW:1):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
```

StrongSwan config

```
conn ipsectest
        left=172.16.0.3
        right=172.16.0.22
        leftauth=psk
        rightauth=psk
        aggressive=no
        auto=ignore
        keyexchange=ikev1
        compress=no
        type=tunnel
        margintime=540s
        ike=3des-sha1-modp1024!
        ikelifetime=4200s
        esp=3des-sha1-modp1024!
        lifetime=3600s

conn ipsectest$0
        leftsubnet=10.0.3.1/32[47/%any]
        rightsubnet=172.16.0.22/32[47/%any]
        auto=route
        keyingtries=1
        also=ipsectest
```

Cisco config

```
...
interface Tunnel0
 ip address 10.4.4.1 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 60
 ip nhrp cache non-authoritative
 keepalive 10 3
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel path-mtu-discovery
 tunnel protection ipsec profile NHRPProfile
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/0
 description INTERNET (UNSAFE)
 ip address 172.16.0.22 255.255.255.0
 duplex full
 speed 100
```

```
 media-type rj45
 crypto map CM0
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 10 5 periodic
crypto isakmp profile PSK-Profile0
   keyring PSK-Key0
   match identity address 0.0.0.0
crypto ipsec optional retry 60
!
!
crypto ipsec transform-set TS0 esp-3des esp-sha-hmac
crypto ipsec transform-set TS-null esp-null esp-sha-hmac
!
crypto ipsec profile NHRPProfile
 set transform-set TS0
 set pfs group2
 set isakmp-profile PSK-Profile0
!
!
crypto dynamic-map DYNMAP0 10
 set transform-set TS0
 set pfs group1
 set isakmp-profile PSK-Profile0
 match address 102
!
crypto map CM0 1 ipsec-isakmp dynamic DYNMAP0
...
```

Associated revisions

Revision 3713d302 - 04.10.2016 10:25 - Tobias Brunner

Merge branch 'ikev1-rekey-deletion'

Sends a DELETE when rekeyed IKE_SAs are deleted. This fixes issues with peers (e.g. Cisco) that continue to send DPDs on the old SA and then delete all SAs if no response is received. But since the DELETE could get dropped this might not fix the issue in all cases.

Also, when terminating an IKE_SA DELETES for all CHILD_SAs are now sent before sending one for the IKE_SA and destroying it.

Fixes #2090.

Revision f15c85a4 - 17.02.2017 11:37 - Tobias Brunner

ikev1: Respond to DPDs for rekeyed IKE_SAs

Some devices always use the oldest IKE_SA to send DPDs and will delete all IKE_SAs when there is no response. If uniqueness is not enforced rekeyed IKE_SAs might not get deleted until they expire so we should respond to DPDs.

References #2090.

History

#1 - 24.08.2016 09:41 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to ikev1

- Status changed from New to Feedback

I think this issue has recently been discussed on the dev mailing list (see my response here). Please try if the patch in the *ikev1-rekey-deletion* branch helps.

#2 - 24.08.2016 14:52 - Alexander Velkov

Hi Tobias,

> Please try if the patch in the *ikev1-rekey-deletion* branch helps.

I tried out your fix in the *ikev1-rekey-deletion* branch. It seems to be OK.

Great, thank you!

StrongSwan logs:

```
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-19 reauthenticating IKE_SA ipsectest$0[2]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-19 initiating Main Mode IKE_SA ipsectest$0[3] to 172.16.0.22
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-19 generating ID_PROT request 0 [ SA V V V V V ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-19 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (1
72 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-23 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
100 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-23 parsed ID_PROT response 0 [ SA V ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-23 received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-23 generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-23 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (2
44 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-21 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
304 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-21 parsed ID_PROT response 0 [ KE No V V V V NAT-D NAT-D ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-21 received Cisco Unity vendor ID
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-21 received DPD vendor ID
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-21 received unknown vendor ID: 88:6a:8d:03:de:c4:bb:55:c0:54:e
7:48:79:ba:d8:ab
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-21 received XAuth vendor ID
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-21 generating ID_PROT request 0 [ ID HASH ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-21 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (6
8 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-26 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
68 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-26 parsed ID_PROT response 0 [ ID HASH ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-26 IKE_SA ipsectest$0[3] established between 172.16.0.3[172.16
.0.3]...172.16.0.22[172.16.0.22]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-26 scheduling reauthentication in 3660s
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-26 maximum IKE_SA lifetime 4200s
Aug 24 12:44:54 GWUZC info  charon: [ 1658] NET-24 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
92 bytes)
Aug 24 12:44:54 GWUZC info  charon: [ 1658] ENC-24 parsed INFORMATIONAL_V1 request 2107877428 [ HASH N((24576)
) ]
Aug 24 12:44:54 GWUZC info  charon: [ 1658] IKE-24 received (24576) notify
Aug 24 12:45:04 GWUZC info  charon: [ 1658] NET-07 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
92 bytes)
Aug 24 12:45:04 GWUZC info  charon: [ 1658] ENC-07 parsed INFORMATIONAL_V1 request 610431433 [ HASH N(DPD) ]
Aug 24 12:45:04 GWUZC info  charon: [ 1658] ENC-07 generating INFORMATIONAL_V1 request 3270500423 [ HASH N(DPD
_ACK) ]
Aug 24 12:45:04 GWUZC info  charon: [ 1658] NET-07 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (9
2 bytes)
Aug 24 12:45:14 GWUZC info  charon: [ 1658] NET-28 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
92 bytes)
Aug 24 12:45:14 GWUZC info  charon: [ 1658] ENC-28 parsed INFORMATIONAL_V1 request 2102790097 [ HASH N(DPD) ]
Aug 24 12:45:14 GWUZC info  charon: [ 1658] ENC-28 generating INFORMATIONAL_V1 request 3160458992 [ HASH N(DPD
_ACK) ]
```

#3 - 24.08.2016 17:44 - Tobias Brunner

> > Please try if the patch in the *ikev1-rekey-deletion* branch helps.
>
> I tried out your fix in the *ikev1-rekey-deletion* branch. It seems to be OK.

I don't see a DELETE getting sent for the old IKE_SA after the rekeying in your log (there should be one now instead of only IKE_SA ipsectest$0[.] state change: REKEYING => DESTROYING as seen before).

#4 - 24.08.2016 19:36 - Alexander Velkov

> I don't see a DELETE getting sent for the old IKE_SA after the rekeying in your log (there should be one now instead of only IKE_SA ipsectest$0[.] state change: REKEYING => DESTROYING as seen before).

Right, I noticed that the state of the old IKE SA printed with *ipsec statusall* keeps to be REKEYING for several minutes. The ISAKMP_DELETE task stays in the queue but does not get activated for some reason. After about 10 minutes, the Cisco sends a DELETE for the SA and it gets then removed correctly.

StrongSwan logs when rekeying:

```
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 reauthenticating IKE_SA ipsectest$0[1]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 queueing ISAKMP_VENDOR task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 queueing ISAKMP_CERT_PRE task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 queueing MAIN_MODE task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 queueing ISAKMP_CERT_POST task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 queueing ISAKMP_NATD task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 activating new tasks
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12   activating ISAKMP_VENDOR task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12   activating ISAKMP_CERT_PRE task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12   activating MAIN_MODE task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12   activating ISAKMP_CERT_POST task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12   activating ISAKMP_NATD task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 sending XAuth vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 sending DPD vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 sending Cisco Unity vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 sending NAT-T (RFC 3947) vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 sending draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 initiating Main Mode IKE_SA ipsectest$0[3] to 172.16.0.22
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 IKE_SA ipsectest$0[3] state change: CREATED => CONNECTING
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-12 generating ID_PROT request 0 [ SA V V V V V ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-12 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (1
72 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 IKE_SA ipsectest$0[1] state change: ESTABLISHED => REKEYING
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 activating new tasks
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-12 nothing to initiate
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-14 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
100 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-14 parsed ID_PROT response 0 [ SA V ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-14 received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-14 reinitiating already active tasks
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-14   ISAKMP_VENDOR task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-14   MAIN_MODE task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-14 generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-14 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (2
44 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-13 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
304 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-13 parsed ID_PROT response 0 [ KE No V V V V NAT-D NAT-D ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-13 received Cisco Unity vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-13 received DPD vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-13 received unknown vendor ID: 88:6a:8d:03:cb:72:b2:af:c2:5d:c
b:6d:e1:96:b6:26
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-13 received XAuth vendor ID
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-13 reinitiating already active tasks
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-13   ISAKMP_VENDOR task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-13   MAIN_MODE task
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-13 generating ID_PROT request 0 [ ID HASH ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-13 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (6
8 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-15 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
68 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-15 parsed ID_PROT response 0 [ ID HASH ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-15 IKE_SA ipsectest$0[3] established between 172.16.0.3[172.16
.0.3]...172.16.0.22[172.16.0.22]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-15 IKE_SA ipsectest$0[3] state change: CONNECTING => ESTABLISH
ED
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-15 scheduling reauthentication in 3660s
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-15 maximum IKE_SA lifetime 4200s
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-15 activating new tasks
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-15 nothing to initiate
Aug 24 17:21:41 GWUZC info  charon: [ 1525] NET-02 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
92 bytes)
Aug 24 17:21:41 GWUZC info  charon: [ 1525] ENC-02 parsed INFORMATIONAL_V1 request 215523396 [ HASH N((24576))
```

```
 ]
Aug 24 17:21:41 GWUZC info  charon: [ 1525] IKE-02 received (24576) notify
Aug 24 17:21:51 GWUZC info  charon: [ 1525] IKE-22 queueing ISAKMP_DELETE task
Aug 24 17:21:51 GWUZC info  charon: [ 1525] IKE-22 activating new tasks
Aug 24 17:21:51 GWUZC info  charon: [ 1525] IKE-22 nothing to initiate
...
Aug 24 17:30:40 GWUZC info  charon: [ 1525] NET-20 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
84 bytes)
Aug 24 17:30:40 GWUZC info  charon: [ 1525] ENC-20 parsed INFORMATIONAL_V1 request 911589833 [ HASH D ]
Aug 24 17:30:40 GWUZC info  charon: [ 1525] IKE-20 received DELETE for IKE_SA ipsectest$0[1]
Aug 24 17:30:40 GWUZC info  charon: [ 1525] IKE-20 deleting IKE_SA ipsectest$0[1] between 172.16.0.3[172.16.0.
3]...172.16.0.22[172.16.0.22]
Aug 24 17:30:40 GWUZC info  charon: [ 1525] IKE-20 IKE_SA ipsectest$0[1] state change: REKEYING => DELETING
Aug 24 17:30:40 GWUZC info  charon: [ 1525] IKE-20 IKE_SA ipsectest$0[1] state change: DELETING => DESTROYING
...
```

#5 - 25.08.2016 10:27 - Tobias Brunner

```
Aug 24 17:21:51 GWUZC info  charon: [ 1525] IKE-22 queueing ISAKMP_DELETE task
Aug 24 17:21:51 GWUZC info  charon: [ 1525] IKE-22 activating new tasks
Aug 24 17:21:51 GWUZC info  charon: [ 1525] IKE-22 nothing to initiate
```

Ah, I see. In state IKE_REKEYING no tasks were activated. I pushed another patch to the branch that changes that.

#6 - 25.08.2016 12:33 - Alexander Velkov

> I pushed another patch to the branch that changes that.

OK - It looks good! Below you can find the rekeying logs with the latest patches from the *ikev1-rekey-deletion* branch.

```
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 reauthenticating IKE_SA ipsectest$0[1]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 queueing ISAKMP_VENDOR task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 queueing ISAKMP_CERT_PRE task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 queueing MAIN_MODE task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 queueing ISAKMP_CERT_POST task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 queueing ISAKMP_NATD task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 activating new tasks
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15   activating ISAKMP_VENDOR task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15   activating ISAKMP_CERT_PRE task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15   activating MAIN_MODE task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15   activating ISAKMP_CERT_POST task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15   activating ISAKMP_NATD task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 sending XAuth vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 sending DPD vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 sending Cisco Unity vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 sending NAT-T (RFC 3947) vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 sending draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 initiating Main Mode IKE_SA ipsectest$0[2] to 172.16.0.22
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 IKE_SA ipsectest$0[2] state change: CREATED => CONNECTING
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-15 generating ID_PROT request 0 [ SA V V V V V ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-15 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (1
72 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 IKE_SA ipsectest$0[1] state change: ESTABLISHED => REKEYING
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 activating new tasks
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-15 nothing to initiate
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-02 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
100 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-02 parsed ID_PROT response 0 [ SA V ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-02 received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-02 reinitiating already active tasks
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-02   ISAKMP_VENDOR task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-02   MAIN_MODE task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-02 generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-02 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (2
44 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-16 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
304 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-16 parsed ID_PROT response 0 [ KE No V V V V NAT-D NAT-D ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-16 received Cisco Unity vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-16 received DPD vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-16 received unknown vendor ID: 88:6a:8d:03:6b:4d:f3:06:5c:74:6
2:0e:df:b2:e2:6d
```

```
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-16 received XAuth vendor ID
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-16 reinitiating already active tasks
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-16   ISAKMP_VENDOR task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-16   MAIN_MODE task
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-16 generating ID_PROT request 0 [ ID HASH ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-16 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (6
8 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-14 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
68 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-14 parsed ID_PROT response 0 [ ID HASH ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-14 IKE_SA ipsectest$0[2] established between 172.16.0.3[172.16
.0.3]...172.16.0.22[172.16.0.22]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-14 IKE_SA ipsectest$0[2] state change: CONNECTING => ESTABLISH
ED
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-14 scheduling reauthentication in 3660s
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-14 maximum IKE_SA lifetime 4200s
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-14 activating new tasks
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-14 nothing to initiate
Aug 25 10:22:46 GWUZC info  charon: [ 1541] NET-19 received packet: from 172.16.0.22[500] to 172.16.0.3[500] (
92 bytes)
Aug 25 10:22:46 GWUZC info  charon: [ 1541] ENC-19 parsed INFORMATIONAL_V1 request 615417581 [ HASH N((24576))
 ]
Aug 25 10:22:46 GWUZC info  charon: [ 1541] IKE-19 received (24576) notify
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01 queueing ISAKMP_DELETE task
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01 activating new tasks
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01   activating ISAKMP_DELETE task
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01 deleting IKE_SA ipsectest$0[1] between 172.16.0.3[172.16.0.
3]...172.16.0.22[172.16.0.22]
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01 sending DELETE for IKE_SA ipsectest$0[1]
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01 IKE_SA ipsectest$0[1] state change: REKEYING => DELETING
Aug 25 10:22:56 GWUZC info  charon: [ 1541] ENC-01 generating INFORMATIONAL_V1 request 3531622837 [ HASH D ]
Aug 25 10:22:56 GWUZC info  charon: [ 1541] NET-01 sending packet: from 172.16.0.3[500] to 172.16.0.22[500] (8
4 bytes)
Aug 25 10:22:56 GWUZC info  charon: [ 1541] IKE-01 IKE_SA ipsectest$0[1] state change: DELETING => DESTROYING
```

#7 - 25.08.2016 15:49 - Tobias Brunner

> I pushed another patch to the branch that changes that.

OK - It looks good! Below you can find the rekeying logs with the latest patches from the *ikev1-rekey-deletion* branch.

OK, that looks like the expected behavior. As I wrote in the email I referenced, the relatively short delay (10s) between the rekeying and the DELETE could theoretically be problematic, but lets see how it pans out in the log run.

#8 - 25.08.2016 17:45 - Alexander Velkov

> the relatively short delay (10s) between the rekeying and the DELETE could theoretically be problematic, but lets see how it pans out in the log run.

I can imagine, like in my case (where the Cisco kept using the old SA for DPDs) that very strict DPD times could tear down the tunnel during the 10s delay. But that would be a very strange setup anyway.

Is there actually a specification for the default behavior when a new SA has been established - is the new SA to be used immediately instead of the old one or we keep using the old SA until it expires? For me, it makes sense to immediately use the new SA. The old SA could be kept for some time for packets using the old SA ... and then we would not even need DELETE messages at all.

#9 - 25.08.2016 18:57 - Tobias Brunner

> the relatively short delay (10s) between the rekeying and the DELETE could theoretically be problematic, but lets see how it pans out in the log run.

> I can imagine, like in my case (where the Cisco kept using the old SA for DPDs) that very strict DPD times could tear down the tunnel during the 10s delay. But that would be a very strange setup anyway.

More problematic is probably that the Cisco box might not receive the DELETE (it is an unconfirmed INFORMATIONAL message, sent once) and does therefore keep using the old IKE_SA, which would result in the same issue if it keeps sending DPDs (but delaying the delete until the SA expires locally does not necessarily prevent that from happening - unless, it expires first on the Cisco box).

By the way, setting *uniqueids=no* should avoid the deletion 10 seconds after the rekeying (it should get deleted then when it eventually expires).

> Is there actually a specification for the default behavior when a new SA has been established - is the new SA to be used immediately instead of the old one or we keep using the old SA until it expires? For me, it makes sense to immediately use the new SA. The old SA could be kept for some time for packets using the old SA ... and then we would not even need DELETE messages at all.

No, rekeying is not really standardized. There is an old ID that also discusses Phase 1 rekeying. One problem is that in our implementation there is a strong relationship between CHILD_SAs and IKE_SAs, which for IKEv1 is not necessarily the case. In fact, CHILD_SAs could theoretically exist without an IKE_SA between two peers, the IKE_SA would then e.g. only be created to manage/rekey the CHILD_SAs. Section 3.4.1 covers multiple concurrent IKE_SAs and says:

```
When there is more than one phase 1 SA between peers, it is
recommended that the oldest SA be used for subsequent traffic
requiring phase 1 SAs. This allows full use of the keying material
generated and reduces race conditions. It also means that no special
expiration conditions are required when the phase 1 SAs expire by
traffic or other usage dependent expirations only, as the old SA
will eventually expire on its own due to usage.
```

This seems to be what the Cisco box is doing (even though it apparently sends DPDs on both SAs). This makes not that much sense to me as the point of a rekeying is to create new keying material, so using the newest SA would make way more sense than the oldest one. However, the author of the ID partly explains his reasoning in section 3.3.1, which is something that we definitely don't do. What's particularly unfortunate is that the Cisco box deletes all IKE and CHILD_SAs if there is no response on the old one even if there is an active new one (at least it looks like DPDs are successfully exchanged on it). For a discussion of DELETE notifies see section 3.4.3.

#10 - 26.08.2016 12:41 - Alexander Velkov

Thank you very much for the information you provided!

> What's particularly unfortunate is that the Cisco box deletes all IKE and CHILD_SAs if there is no response on the old one even if there is an active new one (at least it looks like DPDs are successfully exchanged on it).

I tried out the same with a newer Version of Cisco (16.x), and it still does the same SA deletions. I would say, this is bug at Cisco.

#11 - 05.09.2016 14:24 - Alexander Velkov

Hi Tobias,

> By the way, setting *uniqueids=no* should avoid the deletion 10 seconds after the rekeying (it should get deleted then when it eventually expires).

I tried that out and it works, but I didn't find the documentation for *uniqueids* in the *strongswan.conf* docu. I remember seeing it there some versions ago, but I can't seem to find it now anymore. *uniqueids* is to be defined globally for all conns, is there a way to have the same functionality per connection ?

Is the *ikev1-rekey-deletion* branch going to be merged to *master*? I have tunnels running well with the patches in the branch for a longer time. The changes in the branch make DPD work with Cisco right.

Thank you.

#12 - 05.09.2016 14:40 - Tobias Brunner

- Target version set to 5.5.1

> > By the way, setting *uniqueids=no* should avoid the deletion 10 seconds after the rekeying (it should get deleted then when it eventually expires).
>
> I tried that out and it works, but I didn't find the documentation for *uniqueids* in the *strongswan.conf* docu.

It's not an option in strongswan.conf but the config setup section of ipsec.conf.

> *uniqueids* is to be defined globally for all conns, is there a way to have the same functionality per connection ?

Yes, if you use the swanctl.conf backend the setting can be specified per connection (*connections.<conn>.unique*).

> Is the *ikev1-rekey-deletion* branch going to be merged to *master*?

Yes, these patches will be included in the next release. Thanks for testing them.

#13 - 04.10.2016 10:26 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

#14 - 10.02.2017 19:29 - Alexander Velkov

Tobias Brunner wrote:

> By the way, setting *uniqueids=no* should avoid the deletion 10 seconds after the rekeying (it should get deleted then when it eventually expires).

I had an issue with an IKEv1 tunnel to a Cisco recently. I needed to add another tunnel on the StrongSwan peer that required setting *uniqueids=no*. This brought me to the DPD topic again, so I repeated my tests and found another issue.

So, there is this behaviour on the Cisco that it may perform its DPD message exchange using its old still valid IKE_SA even though there is a new IKE_SA after re-keying. Such DPD messages are dropped on the StrongSwan peer because the relevant Child_SAs have been 'adopted' to the re-keyed IKE_SA. Is that right ? This leads to the DPD timeout on the Cisco, which then tries to regenerate the IPsec tunnel (as can be seen in the previous posts).

There is an additional funny behaviour here. In case, traffic IS flowing through the tunnel, then there is no connection break - no DPD messages get exchanged, no DPD timeout on the Cisco, everything is fine. It seems that traffic through the tunnel other than DPDs selects the right SA.

But the problem is that if there is NO traffic through the tunnel and the Cisco sends DPD messages using the 'wrong' IKE_SA, then I have the tunnel re-creation. Because of *uniqueids=no* the old IKE_SA is not removed after 10s and the Cisco (*crypto isakmp keepalive 10 5 periodic*) get's stuck in the DPD timeout problem again every time re-keying is happening.

#15 - 13.02.2017 12:05 - Tobias Brunner

> I needed to add another tunnel on the StrongSwan peer that required setting *uniqueids=no*.

Could you avoid that by using different identities for the second tunnel?

> Such DPD messages are dropped on the StrongSwan peer because the relevant Child_SAs have been 'adopted' to the re-keyed IKE_SA. Is that right?

No, this has nothing to do with the CHILD_SAs. However, in state IKE_REKEYING we currently don't activate DPD tasks. So I guess even if the old IKE_SA is still there and it processes DPD requests it won't reply to them (you should see a pile up of DPD tasks in ipsec statusall on that IKE_SA). Please check if the commit in the *2090-ikev1-rekeyed-dpd* branch fixes the problem.

> There is an additional funny behaviour here. In case, traffic IS flowing through the tunnel, then there is no connection break - no DPD messages get exchanged, no DPD timeout on the Cisco, everything is fine. It seems that traffic through the tunnel other than DPDs selects the right SA.

Traffic is flowing through IPsec SAs (ESP) not the IKE_SAs. And if there is traffic on the IPsec SAs there are usually no DPDs sent via IKE as it is assumed the other peer is alive.

#16 - 13.02.2017 14:59 - Alexander Velkov

> Could you avoid that by using different identities for the second tunnel?

This was not possible, because it was a connection to a Cisco with thousands of peers connected. Changing the configuration was not an option.

> Please check if the commit in the *2090-ikev1-rekeyed-dpd* branch fixes the problem.

OK, that seems to fix it. I've tested with the latest patch from the *2090-ikev1-rekeyed-dpd* and *uniqueids=no* and there are now no issues with DPDs.

```
... - tunnel is UP for 60 min, now rekeying

Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 25     : initiating Main Mode IKE_SA cisco-v4ikev1$0[10] to 17
```

```
2.16.0.22
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 25     : IKE_SA cisco-v4ikev1$0[10] state change: CREATED => C
ONNECTING
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 25     : generating ID_PROT request 0 [ SA V V V V V V ]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: NET 25     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (196 bytes)
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 25     : IKE_SA cisco-v4ikev1$0[5] state change: ESTABLISHED =
> REKEYING
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 25     : activating new tasks
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 25     : nothing to initiate
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: NET 32     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (100 bytes)
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 32     : parsed ID_PROT response 0 [ SA V ]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 32     : received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 32     : reinitiating already active tasks
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 32     :   ISAKMP_VENDOR task
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 32     :   MAIN_MODE task
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 32     : generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: NET 32     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (244 bytes)
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: NET 30     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (304 bytes)
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 30     : parsed ID_PROT response 0 [ KE No V V V V NAT-D NAT-D
 ]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 30     : received Cisco Unity vendor ID
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 30     : received DPD vendor ID
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 30     : received unknown vendor ID: 88:6a:8d:03:13:45:89:b3:7
4:f1:b2:38:23:41:83:01
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 30     : received XAuth vendor ID
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 30     : reinitiating already active tasks
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 30     :   ISAKMP_VENDOR task
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 30     :   MAIN_MODE task
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 30     : generating ID_PROT request 0 [ ID HASH ]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: NET 30     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (68 bytes)
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: NET 05     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (68 bytes)
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: ENC 05     : parsed ID_PROT response 0 [ ID HASH ]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 05     : IKE_SA cisco-v4ikev1$0[10] established between 172.16
.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 05     : IKE_SA cisco-v4ikev1$0[10] state change: CONNECTING =
> ESTABLISHED
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 05     : scheduling reauthentication in 3660s
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 05     : maximum IKE_SA lifetime 4200s
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 05     : activating new tasks
Feb 13 13:05:23 GWUZ info  charon  [ 1775]: IKE 05     : nothing to initiate
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: ENC 12     : parsed INFORMATIONAL_V1 request 822383562 [ HASH N(DP
D) ]
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: IKE 12     : queueing ISAKMP_DPD task
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: IKE 12     : activating new tasks
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: IKE 12     :   activating ISAKMP_DPD task
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: ENC 12     : generating INFORMATIONAL_V1 request 3111186434 [ HASH
 N(DPD_ACK) ]
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: NET 12     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (92 bytes)
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: IKE 12     : activating new tasks
Feb 13 13:05:33 GWUZ info  charon  [ 1775]: IKE 12     : nothing to initiate
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: NET 20     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (92 bytes)
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: ENC 20     : parsed INFORMATIONAL_V1 request 948004548 [ HASH N(DP
D) ]
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: IKE 20     : queueing ISAKMP_DPD task
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: IKE 20     : activating new tasks
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: IKE 20     :   activating ISAKMP_DPD task
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: ENC 20     : generating INFORMATIONAL_V1 request 2329133885 [ HASH
 N(DPD_ACK) ]
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: NET 20     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (92 bytes)
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: IKE 20     : activating new tasks
Feb 13 13:05:43 GWUZ info  charon  [ 1775]: IKE 20     : nothing to initiate

# ipsec statusall
...
Security Associations (2 up, 0 connecting):
cisco-v4ikev1$0[10]: ESTABLISHED 7 minutes ago, 172.16.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
```

```
cisco-v4ikev1$0[10]: IKEv1 SPIs: 493d67d060973999_i* 7dad2a1e134489b3_r, pre-shared key reauthentication in 53
 minutes
cisco-v4ikev1$0[10]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
cisco-v4ikev1$0{14}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cb55a0c8_i b1dc0cb8_o
cisco-v4ikev1$0{14}:  3DES_CBC/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 33 minutes
cisco-v4ikev1$0{14}:   10.0.0.0/16 === 192.168.101.0/24
cisco-v4ikev1$0[5]: REKEYING, 172.16.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
cisco-v4ikev1$0[5]: IKEv1 SPIs: 59c4da51f1c7f6dd_i* 7dad2a1ea0ff9944_r
cisco-v4ikev1$0[5]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024

... - after 10 min, the old IKE_SA is removed

Feb 13 13:14:20 GWUZ info  charon  [ 1775]: ENC 32     : parsed INFORMATIONAL_V1 request 984029729 [ HASH N(DP
D) ]
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: IKE 32     : queueing ISAKMP_DPD task
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: IKE 32     : activating new tasks
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: IKE 32     :   activating ISAKMP_DPD task
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: ENC 32     : generating INFORMATIONAL_V1 request 3438999273 [ HASH
 N(DPD_ACK) ]
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: NET 32     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (92 bytes)
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: IKE 32     : activating new tasks
Feb 13 13:14:20 GWUZ info  charon  [ 1775]: IKE 32     : nothing to initiate
Feb 13 13:14:23 GWUZ info  charon  [ 1775]: NET 05     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (84 bytes)
Feb 13 13:14:23 GWUZ info  charon  [ 1775]: ENC 05     : parsed INFORMATIONAL_V1 request 3084960910 [ HASH D ]
Feb 13 13:14:23 GWUZ info  charon  [ 1775]: IKE 05     : received DELETE for IKE_SA cisco-v4ikev1$0[5]
Feb 13 13:14:23 GWUZ info  charon  [ 1775]: IKE 05     : deleting IKE_SA cisco-v4ikev1$0[5] between 172.16.0.3
[172.16.0.3]...172.16.0.22[172.16.0.22]
Feb 13 13:14:23 GWUZ info  charon  [ 1775]: IKE 05     : IKE_SA cisco-v4ikev1$0[5] state change: REKEYING => D
ELETING
Feb 13 13:14:23 GWUZ info  charon  [ 1775]: IKE 05     : IKE_SA cisco-v4ikev1$0[5] state change: DELETING => D
ESTROYING
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: NET 06     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (92 bytes)
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: ENC 06     : parsed INFORMATIONAL_V1 request 3602214163 [ HASH N(D
PD) ]
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: IKE 06     : queueing ISAKMP_DPD task
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: IKE 06     : activating new tasks
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: IKE 06     :   activating ISAKMP_DPD task
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: ENC 06     : generating INFORMATIONAL_V1 request 1988787773 [ HASH
 N(DPD_ACK) ]
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: NET 06     : sending packet: from 172.16.0.3[500] to 172.16.0.22[5
00] (92 bytes)
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: IKE 06     : activating new tasks
Feb 13 13:14:30 GWUZ info  charon  [ 1775]: IKE 06     : nothing to initiate
Feb 13 13:14:40 GWUZ info  charon  [ 1775]: NET 08     : received packet: from 172.16.0.22[500] to 172.16.0.3[
500] (92 bytes)
Feb 13 13:14:40 GWUZ info  charon  [ 1775]: ENC 08     : parsed INFORMATIONAL_V1 request 1862044441 [ HASH N(D
PD) ]
Feb 13 13:14:40 GWUZ info  charon  [ 1775]: IKE 08     : queueing ISAKMP_DPD task
Feb 13 13:14:40 GWUZ info  charon  [ 1775]: IKE 08     : activating new tasks
Feb 13 13:14:40 GWUZ info  charon  [ 1775]: IKE 08     :   activating ISAKMP_DPD task
Feb 13 13:14:40 GWUZ info  charon  [ 1775]: ENC 08     : generating INFORMATIONAL_V1 request 3464591 [ HASH N(
DPD_ACK) ]
...

# ipsec statusall
...
Security Associations (1 up, 0 connecting):
cisco-v4ikev1$0[10]: ESTABLISHED 10 minutes ago, 172.16.0.3[172.16.0.3]...172.16.0.22[172.16.0.22]
cisco-v4ikev1$0[10]: IKEv1 SPIs: 493d67d060973999_i* 7dad2a1e134489b3_r, pre-shared key reauthentication in 50
 minutes
cisco-v4ikev1$0[10]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
cisco-v4ikev1$0{14}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cb55a0c8_i b1dc0cb8_o
cisco-v4ikev1$0{14}:  3DES_CBC/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying in 30 minutes
cisco-v4ikev1$0{14}:   10.0.0.0/16 === 192.168.101.0/24
```

And if there is traffic on the IPsec SAs there are usually no DPDs sent via IKE as it is assumed the other peer is alive.

OK, that makes sense, although that sounds like the *on-demand* parameter in the Cisco config. In this case it is *periodic*, so that's not what the Cisco does. My config - *crypto isakmp keepalive 10 5 periodic*

```
Cisco config:
```

```
...
Router(config)# crypto isakmp keepalive seconds [retries] [periodic | on-demand]
   • periodic (Optional) specifies the that DPD messages are sent at regular intervals.
   • on-demand (Optional) specifies DPD retries are sent on demand. This is the default behavior.
...
```

Tobias, thanks for the quick reply and the fix!

#17 - 13.02.2017 16:18 - Tobias Brunner

> Please check if the commit in the *2090-ikev1-rekeyed-dpd* branch fixes the problem.

OK, that seems to fix it. I've tested with the latest patch from the *2090-ikev1-rekeyed-dpd* and *uniqueids=no* and there are now no issues with DPDs.

OK, thanks for testing. Will be included in the next release.

> And if there is traffic on the IPsec SAs there are usually no DPDs sent via IKE as it is assumed the other peer is alive.

OK, that makes sense, although that sounds like the *on-demand* parameter in the Cisco config. In this case it is *periodic*, so that's not what the Cisco does. My config - *crypto isakmp keepalive 10 5 periodic*

So the Cisco did send DPDs in that scenario (traffic flowing)? Perhaps due to the inbound traffic they considered the peer alive and just removed the old IKE_SA and kept on using the new one. But didn't they send DPDs on all IKE_SAs anyway? (i.e. shouldn't they consider the peer alive if there is traffic on any SA - IKE or IPsec - even if no traffic is currently tunneled and only DPDs on the new SA get a reply...) Or do they only send DPDs on one SA (the oldest)?

#18 - 13.02.2017 17:34 - Alexander Velkov

> So the Cisco did send DPDs in that scenario (traffic flowing)? Perhaps due to the inbound traffic they considered the peer alive and just removed the old IKE_SA and kept on using the new one. But didn't they send DPDs on all IKE_SAs anyway? (i.e. shouldn't they consider the peer alive if there is traffic on any SA - IKE or IPsec - even if no traffic is currently tunneled and only DPDs on the new SA get a reply...). Or do they only send DPDs on one SA (the oldest)?

I am not sure.

The Cisco that I have tested on is a test-machine. I think I made sure that there is no traffic through the tunnel, unless I explicitly generate it. The IOS version is an older one (12.x), and it looks to me that the DPD setting *periodic* is not applied and it uses the default *on-demand*.

I made multiple tests with traffic and without traffic in the tunnel coming from either the Cisco or from the StrongSwan peer to the other site. In case I produced traffic myself from any side then the tunnel is rekeying without any problems even if I stopped producing traffic for example 2 min after rekeying (with *uniqueids=no* having two IKE_SAs - one REKEYING and one in ESTABLISHED states) and forcing DPDs to be exchanged.
In case I didn't produce any traffic at all, then the Cisco always failed with DPD timeouts although it had just established a new IKE_SA and Child_SAs before which does not seem to be right. I think that in this case the Cisco used the old IKE_SA for its DPDs, although StrongSwan was replying (maybe on the wrong but Valid one).

#19 - 14.02.2017 10:12 - Tobias Brunner

> The IOS version is an older one (12.x), and it looks to me that the DPD setting periodic is not applied and it uses the default on-demand.

I guess that's possible. The docs mention 12.3(7)T as introduction point for the *periodic/on-demand* keywords. But wouldn't you get an error message if you tried to use an unknown option for a command?

> In case I didn't produce any traffic at all, then the Cisco always failed with DPD timeouts although it had just established a new IKE_SA and Child_SAs before which does not seem to be right. I think that in this case the Cisco used the old IKE_SA for its DPDs, although StrongSwan was replying (maybe on the wrong but Valid one).

This still seems strange. If we'd assume the *on-demand* option applies, the Cisco shouldn't send any DPDs if there is no traffic from its end. Because according to the documentation it only sends DPDs in that mode if it had IPsec traffic ready to be sent to the peer (OK, maybe that traffic check isn't that accurate and gets triggered by other traffic too or it checks the peer for other reasons too). Anyway, I guess replying to DPDs on rekeyed SAs should work around the issue.