strongSwan - Issue #3496

Route-based VPN - transport mode

25.06.2020 15:02 - Jiri Zendulka

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	

Description

Hello,

I would like to use transport mode in route-based IPsec but I am not succesfull so far. I use new xfrmi interface which should works for transport mode (Tunnel mode works). As you can see bellow initiator's side works OK - connection is established and installed but responder's side is established only - NOT installed. I cannot see any error in log. Is anything missing in the configuration?

Many thanks.

Responder's swanctl.conf:

```
connections {
  ipsec1 {
    local_addrs = 0.0.0.0
    remote_addrs = 0.0.0.0
    local {
      auth = psk
    }
    remote {
      auth = psk
    }
    children {
      ipsec1 {
        mode = transport
        if_id_in = 1
        if_id_out = 1
        updown = /etc/scripts/updown_xfrmi 1
        life_time = 3600
        rekey_time = 3060
        rand_time = 540
        esp_proposals = aes128-sha1,3des-sha1
        start_action = none
      }
    }
    version = 1
    rekey_time = 3060
    over_time = 540
    rand_time = 540
    keyingtries = 0
    proposals = aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
  }
}
secrets {
  ike-1 {
    secret =  "123456"
  }
}
```

Responder's status:

```
strongSwan swanctl 5.8.4
uptime: 16 minutes, since Jun 22 15:46:00 2020
worker threads: 16 total, 11 idle, working: 4/0/1/0
```

```
job queues: 0/0/0/0
jobs scheduled: 2
IKE_SAs: 0 total, 0 half-open
mallinfo: sbrk 532480, mmap 0, used 233704, free 298776
loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-default vici updown xauth-ge
neric

ipsec1: IKEv1, reauthentication every 3060s
  local:  0.0.0.0
  remote: 0.0.0.0
  local pre-shared key authentication:
    id: 192.168.7.231
  remote pre-shared key authentication:
  ipsec1: TRANSPORT, rekeying every 3060s
    local:  dynamic
    remote: dynamic
```

Responder's log:

```
2020-06-22 15:45:59 charon: 00[DMN] Starting IKE charon daemon (strongSwan 5.8.4, Linux 4.14.138,
armv7l)
2020-06-22 15:45:59 charon: 00[LIB] loaded plugins: charon nonce pubkey pem openssl kernel-netlink
 socket-default vici updown xauth-generic
2020-06-22 15:45:59 charon: 00[JOB] spawning 16 worker threads
2020-06-22 15:46:02 charon: 13[CFG] loaded IKE shared key with id 'ike-1' for: '%any'
2020-06-22 15:46:02 charon: 06[CFG] added vici connection: ipsec1
2020-06-22 15:46:25 charon: 09[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500]
 (236 bytes)
2020-06-22 15:46:25 charon: 09[ENC] parsed ID_PROT request 0 [ SA V V V V ]
2020-06-22 15:46:25 charon: 09[IKE] received DPD vendor ID
2020-06-22 15:46:25 charon: 09[IKE] received FRAGMENTATION vendor ID
2020-06-22 15:46:25 charon: 09[IKE] received NAT-T (RFC 3947) vendor ID
2020-06-22 15:46:25 charon: 09[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
2020-06-22 15:46:25 charon: 09[IKE] 192.168.7.222 is initiating a Main Mode IKE_SA
2020-06-22 15:46:25 charon: 09[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_
SHA2_256/MODP_3072
2020-06-22 15:46:25 charon: 09[ENC] generating ID_PROT response 0 [ SA V V V V ]
2020-06-22 15:46:25 charon: 09[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(160 bytes)
2020-06-22 15:46:25 charon: 06[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500]
 (524 bytes)
2020-06-22 15:46:25 charon: 06[ENC] parsed ID_PROT request 0 [ KE No NAT-D NAT-D ]
2020-06-22 15:46:25 charon: 06[ENC] generating ID_PROT response 0 [ KE No NAT-D NAT-D ]
2020-06-22 15:46:25 charon: 06[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(524 bytes)
2020-06-22 15:46:25 charon: 10[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500]
 (92 bytes)
2020-06-22 15:46:25 charon: 10[ENC] parsed ID_PROT request 0 [ ID HASH ]
2020-06-22 15:46:25 charon: 10[CFG] looking for pre-shared key peer configs matching 192.168.7.231
...192.168.7.222[192.168.7.222]
2020-06-22 15:46:25 charon: 10[CFG] selected peer config "ipsec1"
2020-06-22 15:46:25 charon: 10[IKE] IKE_SA ipsec1[1] established between 192.168.7.231[192.168.7.2
31]...192.168.7.222[192.168.7.222]
2020-06-22 15:46:25 charon: 10[IKE] scheduling rekeying in 2862s
2020-06-22 15:46:25 charon: 10[IKE] maximum IKE_SA lifetime 3402s
2020-06-22 15:46:25 charon: 10[ENC] generating ID_PROT response 0 [ ID HASH ]
2020-06-22 15:46:25 charon: 10[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(92 bytes)
2020-06-22 15:46:25 charon: 12[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500]
 (204 bytes)
2020-06-22 15:46:25 charon: 12[ENC] parsed QUICK_MODE request 1266116125 [ HASH SA No ID ID ]
2020-06-22 15:46:25 charon: 12[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
2020-06-22 15:46:25 charon: 12[ENC] generating QUICK_MODE response 1266116125 [ HASH SA No ID ID ]

2020-06-22 15:46:25 charon: 12[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(188 bytes)
2020-06-22 15:46:29 charon: 13[IKE] sending retransmit 1 of response message ID 1266116125, seq 4
```

```
2020-06-22 15:46:29 charon: 13[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(188 bytes)
2020-06-22 15:46:34 charon: 10[IKE] sending retransmit 2 of response message ID 1266116125, seq 4
2020-06-22 15:46:34 charon: 10[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(188 bytes)
2020-06-22 15:46:39 charon: 13[IKE] sending retransmit 3 of response message ID 1266116125, seq 4
2020-06-22 15:46:39 charon: 13[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(188 bytes)
2020-06-22 15:46:46 charon: 16[IKE] sending retransmit 4 of response message ID 1266116125, seq 4
2020-06-22 15:46:46 charon: 16[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(188 bytes)
2020-06-22 15:46:55 charon: 12[IKE] sending retransmit 5 of response message ID 1266116125, seq 4
2020-06-22 15:46:55 charon: 12[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500]
(188 bytes)
2020-06-22 15:47:04 charon: 07[KNL] creating delete job for CHILD_SA ESP/0xc3495a8c/192.168.7.231
2020-06-22 15:47:04 charon: 07[JOB] CHILD_SA ESP/0xc3495a8c/192.168.7.231 not found for delete
2020-06-22 15:47:05 charon: 09[IKE] giving up after 5 retransmits
```

Initiator's swanctl.conf:

```
connections {
  ipsec3 {
    local_addrs = 0.0.0.0
    remote_addrs = 192.168.7.231
    local {
      auth = psk
    }
    remote {
      auth = psk
    }
    children {
      ipsec3 {
        mode = transport
        if_id_in = 3
        if_id_out = 3
        updown = /etc/scripts/updown_xfrmi 3
        life_time = 3600
        rekey_time = 3060
        rand_time = 540
        esp_proposals = aes128-sha1,3des-sha1
        start_action = start
      }
    }
    version = 1
    rekey_time = 3060
    over_time = 540
    rand_time = 540
    keyingtries = 0
    proposals = aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
  }
}
secrets {
  ike-3 {
    secret =  "123456"
  }
```

Initiator's status:

```
strongSwan swanctl 5.8.4
uptime: 13 minutes, since Jun 25 12:44:41 2020
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 2
IKE_SAs: 1 total, 0 half-open
mallinfo: sbrk 540672, mmap 0, used 222552, free 318120
loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-default vici updown xauth-ge
neric
```

```
ipsec3: IKEv1, reauthentication every 3060s
  local:  0.0.0.0
  remote: 192.168.7.231
  local pre-shared key authentication:
    id: 192.168.7.222
  remote pre-shared key authentication:
  ipsec3: TRANSPORT, rekeying every 3060s
    local:  dynamic
    remote: dynamic

ipsec3: #1, ESTABLISHED, IKEv1, 6953c5fed8415280_i* c8509db0cc501620_r
  local  '192.168.7.222' @ 192.168.7.222[500]
  remote '192.168.7.231' @ 192.168.7.231[500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
  established 815s ago, rekeying in 2039s
  ipsec3: #1, reqid 1, INSTALLED, TRANSPORT, ESP:AES_CBC-128/HMAC_SHA1_96
    installed 815s ago, rekeying in 2169s, expires in 2785s
    in  c91619f2 (-|0x00000003),      0 bytes,     0 packets
    out c3495a8c (-|0x00000003),      0 bytes,     0 packets
    local  192.168.7.222/32
    remote 192.168.7.231/32
```

Initiator's log:

```
2020-06-25 12:44:41 charon: 00[DMN] Starting IKE charon daemon (strongSwan 5.8.4, Linux 4.14.138,
armv7l)
2020-06-25 12:44:41 charon: 00[LIB] loaded plugins: charon nonce pubkey pem openssl kernel-netlink
 socket-default vici updown xauth-generic
2020-06-25 12:44:41 charon: 00[JOB] spawning 16 worker threads
2020-06-25 12:44:43 charon: 13[CFG] loaded IKE shared key with id 'ike-3' for: '%any'
2020-06-25 12:44:43 charon: 06[CFG] added vici connection: ipsec3
2020-06-25 12:44:43 charon: 06[CFG] initiating 'ipsec3'
2020-06-25 12:44:43 charon: 06[IKE] initiating Main Mode IKE_SA ipsec3[1] to 192.168.7.231
2020-06-25 12:44:43 charon: 06[ENC] generating ID_PROT request 0 [ SA V V V V ]
2020-06-25 12:44:43 charon: 06[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(236 bytes)
2020-06-25 12:44:43 charon: 12[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (160 bytes)
2020-06-25 12:44:43 charon: 12[ENC] parsed ID_PROT response 0 [ SA V V V V ]
2020-06-25 12:44:43 charon: 12[IKE] received XAuth vendor ID
2020-06-25 12:44:43 charon: 12[IKE] received DPD vendor ID
2020-06-25 12:44:43 charon: 12[IKE] received FRAGMENTATION vendor ID
2020-06-25 12:44:43 charon: 12[IKE] received NAT-T (RFC 3947) vendor ID
2020-06-25 12:44:43 charon: 12[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_
SHA2_256/MODP_3072
2020-06-25 12:44:43 charon: 12[ENC] generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
2020-06-25 12:44:43 charon: 12[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(524 bytes)
2020-06-25 12:44:44 charon: 13[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (524 bytes)
2020-06-25 12:44:44 charon: 13[ENC] parsed ID_PROT response 0 [ KE No NAT-D NAT-D ]
2020-06-25 12:44:44 charon: 13[ENC] generating ID_PROT request 0 [ ID HASH ]
2020-06-25 12:44:44 charon: 13[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(92 bytes)
2020-06-25 12:44:44 charon: 14[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (92 bytes)
2020-06-25 12:44:44 charon: 14[ENC] parsed ID_PROT response 0 [ ID HASH ]
2020-06-25 12:44:44 charon: 14[IKE] IKE_SA ipsec3[1] established between 192.168.7.222[192.168.7.2
22]...192.168.7.231[192.168.7.231]
2020-06-25 12:44:44 charon: 14[IKE] scheduling rekeying in 2854s
2020-06-25 12:44:44 charon: 14[IKE] maximum IKE_SA lifetime 3394s
2020-06-25 12:44:44 charon: 14[ENC] generating QUICK_MODE request 1266116125 [ HASH SA No ID ID ]
2020-06-25 12:44:44 charon: 14[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(204 bytes)
2020-06-25 12:44:44 charon: 15[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (188 bytes)
```

```
2020-06-25 12:44:44 charon: 15[ENC] parsed QUICK_MODE response 1266116125 [ HASH SA No ID ID ]
2020-06-25 12:44:44 charon: 15[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
2020-06-25 12:44:44 charon: 15[IKE] CHILD_SA ipsec3{1} established with SPIs c91619f2_i c3495a8c_o
 and TS 192.168.7.222/32 === 192.168.7.231/32
2020-06-25 12:44:44 charon: 16[KNL] interface ipsec3 activated
2020-06-25 12:44:44 charon: 09[KNL] fe80::e387:a6b3:9f41:eb52 appeared on ipsec3
2020-06-25 12:44:44 charon: 15[ENC] generating QUICK_MODE request 1266116125 [ HASH ]
2020-06-25 12:44:44 charon: 15[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(76 bytes)
2020-06-25 12:44:48 charon: 09[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (188 bytes)
2020-06-25 12:44:48 charon: 09[IKE] received retransmit of response with ID 1266116125, resending
last request
2020-06-25 12:44:48 charon: 09[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(76 bytes)
2020-06-25 12:44:52 charon: 10[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (188 bytes)
2020-06-25 12:44:52 charon: 10[IKE] received retransmit of response with ID 1266116125, resending
last request
2020-06-25 12:44:52 charon: 10[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(76 bytes)
2020-06-25 12:44:58 charon: 11[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (188 bytes)
2020-06-25 12:44:58 charon: 11[IKE] received retransmit of response with ID 1266116125, resending
last request
2020-06-25 12:44:58 charon: 11[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(76 bytes)
2020-06-25 12:45:05 charon: 06[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (188 bytes)
2020-06-25 12:45:05 charon: 06[IKE] received retransmit of response with ID 1266116125, resending
last request
2020-06-25 12:45:05 charon: 06[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(76 bytes)
2020-06-25 12:45:13 charon: 16[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500]
 (188 bytes)
2020-06-25 12:45:13 charon: 16[IKE] received retransmit of response with ID 1266116125, resending
last request
2020-06-25 12:45:13 charon: 16[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500]
(76 bytes)
2020-06-25 12:55:17 sshd[2880]: Accepted keyboard-interactive/pam for root from 192.168.7.2 port 1
0783 ssh2
```

History

#1 - 25.06.2020 17:45 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

Are you f*in crazy to use IKEv1 for this? I won't even look at it closer.

#2 - 25.06.2020 20:20 - Jiri Zendulka

Is it valid configuration, isn't it? I understand that is not recommended to use IKEv1 in general. But I guess it should work anyway. IKEv2 has the same failure. Could I ask for any advice?

#3 - 26.06.2020 08:46 - Jiri Zendulka

Responder IKEv2:

```
connections {
  ipsec1 {
    local_addrs = 0.0.0.0
    remote_addrs = 0.0.0.0
    local {
      auth = psk
    }
    remote {
```

```
      auth = psk
    }
    children {
      ipsec1 {
        mode = transport
        if_id_in = 1
        if_id_out = 1
        updown = /etc/scripts/updown_xfrmi 1
        life_time = 3600
        rekey_time = 3060
        rand_time = 540
        esp_proposals = aes128-sha1,3des-sha1
        start_action = none
      }
    }
    version = 2
    rekey_time = 3060
    over_time = 540
    rand_time = 540
    keyingtries = 0
    proposals = aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
  }
}
secrets {
  ike-1 {
    secret =  "123456"
  }
}

strongSwan swanctl 5.8.4
uptime: 7 minutes, since Jun 23 09:17:03 2020
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 22
IKE_SAs: 1 total, 0 half-open
mallinfo: sbrk 557056, mmap 0, used 444304, free 112752
loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-default vici updown xauth-generic

ipsec1: IKEv2, no reauthentication, rekeying every 3060s
  local:  0.0.0.0
  remote: 0.0.0.0
  local pre-shared key authentication:
  remote pre-shared key authentication:
  ipsec1: TRANSPORT, rekeying every 3060s
    local:  dynamic
    remote: dynamic

ipsec1: #12, ESTABLISHED, IKEv2, 45c89114d6dd87f2_i 54bf5e8934cc765f_r*
  local  '192.168.7.231' @ 192.168.7.231[4500]
  remote '192.168.7.222' @ 192.168.7.222[4500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
  established 13s ago, rekeying in 2834s
  active:  IKE_MOBIKE
  ipsec1: #10, reqid 1, INSTALLED, TRANSPORT, ESP:AES_CBC-128/HMAC_SHA1_96
    installed 13s ago, rekeying in 2874s, expires in 3587s
    in  cf081651 (-|0x00000001),      0 bytes,     0 packets
    out c532e7d1 (-|0x00000001),      0 bytes,     0 packets
    local  192.168.7.231/32
    remote 192.168.7.222/32

2020-06-23 09:46:50 charon: 00[DMN] Starting IKE charon daemon (strongSwan 5.8.4, Linux 4.14.138, armv7l)
2020-06-23 09:46:50 charon: 00[LIB] loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-defa
ult vici updown xauth-generic
2020-06-23 09:46:50 charon: 00[JOB] spawning 16 worker threads
2020-06-23 09:46:53 charon: 15[CFG] loaded IKE shared key with id 'ike-1' for: '%any'
2020-06-23 09:46:53 charon: 08[CFG] added vici connection: ipsec1
2020-06-23 09:46:54 charon: 05[KNL] interface wlan1 activated
2020-06-23 09:46:54 charon: 06[KNL] interface wlan1 deactivated
2020-06-23 09:46:54 charon: 07[KNL] interface wlan1 activated
2020-06-23 09:46:57 charon: 12[KNL] interface wlan1 deactivated
2020-06-23 09:47:17 charon: 06[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)

2020-06-23 09:47:17 charon: 06[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_S
UP) N(HASH_ALG) N(REDIR_SUP) ]
2020-06-23 09:47:17 charon: 06[IKE] 192.168.7.222 is initiating an IKE_SA
```

```
2020-06-23 09:47:17 charon: 06[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MOD
P_3072
2020-06-23 09:47:17 charon: 06[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(F
RAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
2020-06-23 09:47:17 charon: 06[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500] (598 bytes)
2020-06-23 09:47:17 charon: 07[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:47:17 charon: 07[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:47:17 charon: 07[CFG] looking for peer configs matching 192.168.7.231[%any]...192.168.7.222[192.
168.7.222]
2020-06-23 09:47:17 charon: 07[CFG] selected peer config 'ipsec1'
2020-06-23 09:47:17 charon: 07[IKE] authentication of '192.168.7.222' with pre-shared key successful
2020-06-23 09:47:17 charon: 07[IKE] peer supports MOBIKE
2020-06-23 09:47:17 charon: 07[CFG] no IDr configured, fall back on IP address
2020-06-23 09:47:17 charon: 07[IKE] authentication of '192.168.7.231' (myself) with pre-shared key
2020-06-23 09:47:17 charon: 07[IKE] IKE_SA ipsec1[1] established between 192.168.7.231[192.168.7.231]...192.16
8.7.222[192.168.7.222]
2020-06-23 09:47:17 charon: 07[IKE] scheduling rekeying in 2826s
2020-06-23 09:47:17 charon: 07[IKE] maximum IKE_SA lifetime 3366s
2020-06-23 09:47:17 charon: 07[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
2020-06-23 09:47:17 charon: 07[IKE] CHILD_SA ipsec1{1} established with SPIs c82459a5_i c2e50572_o and TS 192.
168.7.231/32 === 192.168.7.222/32
2020-06-23 09:47:18 charon: 10[KNL] interface ipsec1 activated
2020-06-23 09:47:18 charon: 12[KNL] fe80::73ec:1c96:d7fb:9da7 appeared on ipsec1
2020-06-23 09:47:18 charon: 07[ENC] generating IKE_AUTH response 1 [ IDr AUTH N(USE_TRANSP) SA TSi TSr N(MOBIK
E_SUP) N(ADD_4_ADDR) ]
2020-06-23 09:47:18 charon: 07[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:47:18 charon: 05[IKE] sending address list update using MOBIKE
2020-06-23 09:47:18 charon: 05[ENC] generating INFORMATIONAL request 0 [ N(ADD_4_ADDR) ]
2020-06-23 09:47:18 charon: 05[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:47:21 charon: 09[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:47:21 charon: 09[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:47:21 charon: 09[IKE] received retransmit of request with ID 1, retransmitting response
2020-06-23 09:47:21 charon: 09[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:47:22 charon: 10[IKE] retransmit 1 of request with message ID 0
2020-06-23 09:47:22 charon: 10[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:47:26 charon: 15[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:47:26 charon: 15[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:47:26 charon: 15[IKE] received retransmit of request with ID 1, retransmitting response
2020-06-23 09:47:26 charon: 15[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:47:26 charon: 07[IKE] retransmit 2 of request with message ID 0
2020-06-23 09:47:26 charon: 07[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:47:32 charon: 16[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:47:32 charon: 16[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:47:32 charon: 16[IKE] received retransmit of request with ID 1, retransmitting response
2020-06-23 09:47:32 charon: 16[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:47:32 charon: 06[IKE] retransmit 3 of request with message ID 0
2020-06-23 09:47:32 charon: 06[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:47:39 charon: 05[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:47:39 charon: 05[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:47:39 charon: 05[IKE] received retransmit of request with ID 1, retransmitting response
2020-06-23 09:47:39 charon: 05[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:47:39 charon: 14[IKE] retransmit 4 of request with message ID 0
2020-06-23 09:47:39 charon: 14[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:47:47 charon: 09[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
```

```
2020-06-23 09:47:47 charon: 09[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:47:47 charon: 09[IKE] received retransmit of request with ID 1, retransmitting response
2020-06-23 09:47:47 charon: 09[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:47:47 charon: 11[IKE] retransmit 5 of request with message ID 0
2020-06-23 09:47:47 charon: 11[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:47:57 charon: 10[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)

2020-06-23 09:47:57 charon: 10[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_S
UP) N(HASH_ALG) N(REDIR_SUP) ]
2020-06-23 09:47:57 charon: 10[IKE] 192.168.7.222 is initiating an IKE_SA
2020-06-23 09:47:57 charon: 10[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MOD
P_3072
2020-06-23 09:47:57 charon: 10[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(F
RAG_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
2020-06-23 09:47:57 charon: 10[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500] (598 bytes)
2020-06-23 09:47:57 charon: 11[IKE] giving up after 5 retransmits
2020-06-23 09:47:57 charon: 08[KNL] interface ipsec1 deactivated
2020-06-23 09:47:57 charon: 07[KNL] fe80::73ec:1c96:d7fb:9da7 disappeared from ipsec1
2020-06-23 09:47:57 charon: 16[KNL] interface ipsec1 deleted
2020-06-23 09:48:01 charon: 14[NET] received packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)

2020-06-23 09:48:01 charon: 14[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_S
UP) N(HASH_ALG) N(REDIR_SUP) ]
2020-06-23 09:48:01 charon: 14[IKE] received retransmit of request with ID 0, retransmitting response
2020-06-23 09:48:01 charon: 14[NET] sending packet: from 192.168.7.231[500] to 192.168.7.222[500] (598 bytes)
2020-06-23 09:48:01 charon: 10[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:48:01 charon: 10[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:48:01 charon: 10[CFG] looking for peer configs matching 192.168.7.231[%any]...192.168.7.222[192.
168.7.222]
2020-06-23 09:48:01 charon: 10[CFG] selected peer config 'ipsec1'
2020-06-23 09:48:01 charon: 10[IKE] authentication of '192.168.7.222' with pre-shared key successful
2020-06-23 09:48:01 charon: 10[IKE] peer supports MOBIKE
2020-06-23 09:48:01 charon: 10[CFG] no IDr configured, fall back on IP address
2020-06-23 09:48:01 charon: 10[IKE] authentication of '192.168.7.231' (myself) with pre-shared key
2020-06-23 09:48:01 charon: 10[IKE] IKE_SA ipsec1[2] established between 192.168.7.231[192.168.7.231]...192.16
8.7.222[192.168.7.222]
2020-06-23 09:48:01 charon: 10[IKE] scheduling rekeying in 2997s
2020-06-23 09:48:01 charon: 10[IKE] maximum IKE_SA lifetime 3537s
2020-06-23 09:48:01 charon: 10[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
2020-06-23 09:48:01 charon: 10[IKE] CHILD_SA ipsec1{2} established with SPIs c18593b0_i c6b8ac75_o and TS 192.
168.7.231/32 === 192.168.7.222/32
2020-06-23 09:48:01 charon: 12[KNL] interface ipsec1 activated
2020-06-23 09:48:01 charon: 13[KNL] fe80::5c57:84f2:9b42:47b2 appeared on ipsec1
2020-06-23 09:48:01 charon: 10[ENC] generating IKE_AUTH response 1 [ IDr AUTH N(USE_TRANSP) SA TSi TSr N(MOBIK
E_SUP) N(ADD_4_ADDR) ]
2020-06-23 09:48:01 charon: 10[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:48:01 charon: 06[IKE] sending address list update using MOBIKE
2020-06-23 09:48:01 charon: 06[ENC] generating INFORMATIONAL request 0 [ N(ADD_4_ADDR) ]
2020-06-23 09:48:01 charon: 06[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (80 bytes)

2020-06-23 09:48:05 charon: 08[NET] received packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 byte
s)
2020-06-23 09:48:05 charon: 08[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE_SUP
) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-23 09:48:05 charon: 08[IKE] received retransmit of request with ID 1, retransmitting response
2020-06-23 09:48:05 charon: 08[NET] sending packet: from 192.168.7.231[4500] to 192.168.7.222[4500] (240 bytes
)
2020-06-23 09:48:05 charon: 12[IKE] retransmit 1 of request with message ID 0
```

Initiator IKEv2:

```
connections {
  ipsec3 {
    local_addrs = 0.0.0.0
    remote_addrs = 192.168.7.231
    local {
      auth = psk
    }
```

```
    remote {
      auth = psk
    }
    children {
      ipsec3 {
        mode = transport
        if_id_in = 3
        if_id_out = 3
        updown = /etc/scripts/updown_xfrmi 3
        life_time = 3600
        rekey_time = 3060
        rand_time = 540
        esp_proposals = aes128-sha1,3des-sha1
        start_action = start
      }
    }
    version = 2
    rekey_time = 3060
    over_time = 540
    rand_time = 540
    keyingtries = 0
    proposals = aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
  }
}
secrets {
  ike-3 {
    secret =  "123456"
  }
}

strongSwan swanctl 5.8.4
uptime: 34 minutes, since Jun 26 06:15:44 2020
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 2
IKE_SAs: 1 total, 1 half-open
mallinfo: sbrk 724992, mmap 0, used 562496, free 162496
loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-default vici updown xauth-generic

ipsec3: IKEv2, no reauthentication, rekeying every 3060s
  local:  0.0.0.0
  remote: 192.168.7.231
  local pre-shared key authentication:
  remote pre-shared key authentication:
  ipsec3: TRANSPORT, rekeying every 3060s
    local:  dynamic
    remote: dynamic

ipsec3: #1, CONNECTING, IKEv2, d01f77c72f91fb64_i* 91b8a53c40536cfa_r
  local  '192.168.7.222' @ 192.168.7.222[4500]
  remote '%any' @ 192.168.7.231[4500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
  active:  IKE_CERT_PRE IKE_AUTH IKE_CERT_POST CHILD_CREATE IKE_AUTH_LIFETIME IKE_MOBIKE

2020-06-26 06:51:03 charon: 00[DMN] Starting IKE charon daemon (strongSwan 5.8.4, Linux 4.14.138, armv7l)
2020-06-26 06:51:04 charon: 00[LIB] loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-defa
ult vici updown xauth-generic
2020-06-26 06:51:04 charon: 00[JOB] spawning 16 worker threads
2020-06-26 06:51:06 charon: 14[CFG] loaded IKE shared key with id 'ike-3' for: '%any'
2020-06-26 06:51:06 charon: 07[CFG] added vici connection: ipsec3
2020-06-26 06:51:06 charon: 07[CFG] initiating 'ipsec3'
2020-06-26 06:51:06 charon: 07[IKE] initiating IKE_SA ipsec3[1] to 192.168.7.231
2020-06-26 06:51:06 charon: 07[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
2020-06-26 06:51:06 charon: 07[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:51:07 charon: 15[KNL] interface wlan1 activated
2020-06-26 06:51:07 charon: 05[KNL] interface wlan1 deactivated
2020-06-26 06:51:07 charon: 06[KNL] interface wlan1 activated
2020-06-26 06:51:10 charon: 12[KNL] interface wlan1 deactivated
2020-06-26 06:51:10 charon: 14[IKE] retransmit 1 of request with message ID 0
2020-06-26 06:51:10 charon: 14[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:51:15 charon: 16[IKE] retransmit 2 of request with message ID 0
2020-06-26 06:51:15 charon: 16[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:51:21 charon: 05[IKE] retransmit 3 of request with message ID 0
2020-06-26 06:51:21 charon: 05[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
```

```
2020-06-26 06:51:28 charon: 06[IKE] retransmit 4 of request with message ID 0
2020-06-26 06:51:28 charon: 06[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:51:28 charon: 08[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500] (598 bytes)

2020-06-26 06:51:28 charon: 08[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_
SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
2020-06-26 06:51:28 charon: 08[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MOD
P_3072
2020-06-26 06:51:28 charon: 08[CFG] no IDi configured, fall back on IP address
2020-06-26 06:51:28 charon: 08[IKE] authentication of '192.168.7.222' (myself) with pre-shared key
2020-06-26 06:51:28 charon: 08[IKE] establishing CHILD_SA ipsec3{1}
2020-06-26 06:51:28 charon: 08[ENC] generating IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE
_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-26 06:51:28 charon: 08[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:51:32 charon: 09[IKE] retransmit 1 of request with message ID 1
2020-06-26 06:51:32 charon: 09[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:51:36 charon: 11[IKE] retransmit 2 of request with message ID 1
2020-06-26 06:51:36 charon: 11[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:51:42 charon: 07[IKE] retransmit 3 of request with message ID 1
2020-06-26 06:51:42 charon: 07[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:51:49 charon: 13[IKE] retransmit 4 of request with message ID 1
2020-06-26 06:51:49 charon: 13[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:51:57 charon: 15[IKE] retransmit 5 of request with message ID 1
2020-06-26 06:51:57 charon: 15[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:07 charon: 12[KNL] creating delete job for CHILD_SA ESP/0xc7d33527/192.168.7.222
2020-06-26 06:52:07 charon: 12[JOB] CHILD_SA ESP/0xc7d33527/192.168.7.222 not found for delete
2020-06-26 06:52:07 charon: 07[IKE] giving up after 5 retransmits
2020-06-26 06:52:07 charon: 07[IKE] peer not responding, trying again (2/0)
2020-06-26 06:52:07 charon: 07[IKE] initiating IKE_SA ipsec3[1] to 192.168.7.231
2020-06-26 06:52:07 charon: 07[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
2020-06-26 06:52:07 charon: 07[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:52:11 charon: 13[IKE] retransmit 1 of request with message ID 0
2020-06-26 06:52:11 charon: 13[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:52:11 charon: 15[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500] (598 bytes)

2020-06-26 06:52:11 charon: 15[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_
SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
2020-06-26 06:52:11 charon: 15[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MOD
P_3072
2020-06-26 06:52:11 charon: 15[CFG] no IDi configured, fall back on IP address
2020-06-26 06:52:11 charon: 15[IKE] authentication of '192.168.7.222' (myself) with pre-shared key
2020-06-26 06:52:11 charon: 15[IKE] establishing CHILD_SA ipsec3{2}
2020-06-26 06:52:11 charon: 15[ENC] generating IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE
_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-26 06:52:11 charon: 15[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:15 charon: 14[IKE] retransmit 1 of request with message ID 1
2020-06-26 06:52:15 charon: 14[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:20 charon: 05[IKE] retransmit 2 of request with message ID 1
2020-06-26 06:52:20 charon: 05[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:26 charon: 06[IKE] retransmit 3 of request with message ID 1
2020-06-26 06:52:26 charon: 06[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:33 charon: 08[IKE] retransmit 4 of request with message ID 1
2020-06-26 06:52:33 charon: 08[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:41 charon: 14[IKE] retransmit 5 of request with message ID 1
2020-06-26 06:52:41 charon: 14[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:50 charon: 16[KNL] creating delete job for CHILD_SA ESP/0xc12d652b/192.168.7.222
2020-06-26 06:52:50 charon: 16[JOB] CHILD_SA ESP/0xc12d652b/192.168.7.222 not found for delete
2020-06-26 06:52:51 charon: 06[IKE] giving up after 5 retransmits
2020-06-26 06:52:51 charon: 06[IKE] peer not responding, trying again (3/0)
2020-06-26 06:52:51 charon: 06[IKE] initiating IKE_SA ipsec3[1] to 192.168.7.231
2020-06-26 06:52:51 charon: 06[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
```

```
2020-06-26 06:52:51 charon: 06[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:52:55 charon: 08[IKE] retransmit 1 of request with message ID 0
2020-06-26 06:52:55 charon: 08[NET] sending packet: from 192.168.7.222[500] to 192.168.7.231[500] (674 bytes)
2020-06-26 06:52:55 charon: 09[NET] received packet: from 192.168.7.231[500] to 192.168.7.222[500] (598 bytes)

2020-06-26 06:52:55 charon: 09[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_
SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
2020-06-26 06:52:55 charon: 09[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MOD
P_3072
2020-06-26 06:52:55 charon: 09[CFG] no IDi configured, fall back on IP address
2020-06-26 06:52:55 charon: 09[IKE] authentication of '192.168.7.222' (myself) with pre-shared key
2020-06-26 06:52:55 charon: 09[IKE] establishing CHILD_SA ipsec3{3}
2020-06-26 06:52:55 charon: 09[ENC] generating IKE_AUTH request 1 [ IDi AUTH N(USE_TRANSP) SA TSi TSr N(MOBIKE
_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
2020-06-26 06:52:55 charon: 09[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:52:59 charon: 10[IKE] retransmit 1 of request with message ID 1
2020-06-26 06:52:59 charon: 10[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:53:04 charon: 11[IKE] retransmit 2 of request with message ID 1
2020-06-26 06:53:04 charon: 11[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:53:10 charon: 08[IKE] retransmit 3 of request with message ID 1
2020-06-26 06:53:10 charon: 08[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
2020-06-26 06:53:17 charon: 09[IKE] retransmit 4 of request with message ID 1
2020-06-26 06:53:17 charon: 09[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.231[4500] (336 bytes
)
```

#4 - 26.06.2020 09:55 - Tobias Brunner

> Is it valid configuration, isn't it?

I'd never consider it valid to use IKEv1 between two strongSwan instances. It makes absolutely no sense to use a horrible legacy protocol in such a scenario.

It looks like you routed the IKE packets via XFRM interface. You want to prevent that by e.g. configuring *charon.plugins.socket-default.fwmark* to an arbitrary value and then install your routes in a separate table whose routing rule excludes packets with that mark (ip rule add not fwmark <mark> table <table>).

What's your reason to use XFRM interfaces with transport mode in the first place?

#5 - 29.06.2020 11:43 - Jiri Zendulka

We use strongswan on an embedded device (industrial routers) which have a web user interface for setup. So customer doesn't edit swantcl.conf directly.

We have an idea to use route-based ipsec (xfrmi interface) for all Ipsec configurations. swactl.conf is generated by a script - all is picked from WebUI. We would like to avoid any option "policy-based" vs "route-based" IPsec on WebUI.

I think that with xfrmi interface it is possible to cover all possible configuration including very simple or legacy (ikev1) configurations. Or I am wrong? Is it any limitation of route-based IPsec in compariosn with policy-based IPsec?

Many thanks.

#6 - 29.06.2020 11:52 - Tobias Brunner

> I think that with xfrmi interface it is possible to cover all possible configuration including very simple or legacy (ikev1) configurations. Or I am wrong? Is it any limitation of route-based IPsec in compariosn with policy-based IPsec?

While you can probably do pretty much anything with both approaches, they are quite different. And don't forget that you still negotiate and install policies for route-based connections, so there might really not be any difference or advantage depending on the config (also depends on how flexible the remote peer is). You might want to read about them and really think what use cases would be better suited for one or the other (for instance, it really makes not much sense to use a route-based approach for a host-to-host transport mode connection unless you want to do fancy policy routing stuff).

#7 - 16.07.2020 10:13 - Jiri Zendulka

I am able to create a new table but I am not sure what table number should be set. Or it does not depend on it?

#8 - 16.07.2020 13:59 - Jiri Zendulka

Connections are established on both sides now. But ping does not go through... I see some dropped packets.

```
ipsec1: #2, ESTABLISHED, IKEv2, 1a90700764872159_i* 4fdd154c42bb561f_r
  local  '192.168.7.222' @ 192.168.7.222[4500]
  remote '192.168.7.100' @ 192.168.7.100[4500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
  established 290s ago, rekeying in 2556s
  ipsec1: #1, reqid 1, INSTALLED, TRANSPORT, ESP:AES_CBC-128/HMAC_SHA1_96
    installed 290s ago, rekeying in 2272s, expires in 3310s
    in  c69da689 (-|0x00000001),      0 bytes,     0 packets
    out ca82ac93 (-|0x00000001),      0 bytes,     0 packets
    local  192.168.7.222/32
    remote 192.168.7.100/32
```

xfm interface

```
ipsec1    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet6 addr: fe80::e6c2:9ebc:59f2:df3a/64 Scope:Link
          UP RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:4 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

ip route:

```
# ip route show table ipsec1
192.168.7.222 dev ipsec1 scope link
```

ip rule:

```
# ip rule show
0:      from all lookup local
219:    not from all fwmark 0x1234 lookup ipsec1
220:    from all lookup 220
32766:  from all lookup main
32767:  from all lookup default
```

strongswan.conf

```
charon {
  plugins {
    socket-default {
      fwmark = 0x1234
  }
}
```

#9 - 17.07.2020 10:05 - Jiri Zendulka

Responder:

```
...
2020-07-17 09:57:49 charon: 08[IKE] retransmit 3 of request with message ID 0
2020-07-17 09:57:49 charon: 08[NET] sending packet: from 192.168.7.100[4500] to 192.168.7.222[4500] (80 bytes)

2020-07-17 09:58:12 charon: 07[IKE] retransmit 4 of request with message ID 0
2020-07-17 09:58:12 charon: 07[NET] sending packet: from 192.168.7.100[4500] to 192.168.7.222[4500] (80 bytes)

2020-07-17 09:58:54 charon: 11[IKE] retransmit 5 of request with message ID 0
2020-07-17 09:58:54 charon: 11[NET] sending packet: from 192.168.7.100[4500] to 192.168.7.222[4500] (80 bytes)

2020-07-17 10:00:10 charon: 16[IKE] giving up after 5 retransmits
2020-07-17 10:00:10 charon: 13[KNL] interface ipsec1 deactivated
2020-07-17 10:00:10 charon: 15[KNL] fe80::27f5:e081:52cb:c844 disappeared from ipsec1
2020-07-17 10:00:10 charon: 08[KNL] interface ipsec1 deleted
```

Initiator:

```
...
2020-07-17 09:57:01 charon: 11[ENC] parsed INFORMATIONAL request 0 [ N(ADD_4_ADDR) ]
2020-07-17 09:57:01 charon: 11[IKE] received retransmit of request with ID 0, retransmitting response
2020-07-17 09:57:01 charon: 11[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.100[4500] (80 bytes)

2020-07-17 09:57:43 charon: 09[NET] received packet: from 192.168.7.100[4500] to 192.168.7.222[4500] (80 bytes
)
2020-07-17 09:57:43 charon: 09[ENC] parsed INFORMATIONAL request 0 [ N(ADD_4_ADDR) ]
2020-07-17 09:57:43 charon: 09[IKE] received retransmit of request with ID 0, retransmitting response
2020-07-17 09:57:43 charon: 09[NET] sending packet: from 192.168.7.222[4500] to 192.168.7.100[4500] (80 bytes)
```

#10 - 20.07.2020 15:58 - Tobias Brunner

Looks like the initiator can't send packets to the responder, so fix that.

#11 - 21.07.2020 11:30 - Jiri Zendulka

Could you guide me a little?

The rule table ID 219 is OK? Or should I use something like 1000X?
Should I add something like default route to route table ipsec1?
Should I add CONNMARK rule set/restore for fwmark 0x1234 to iptables -t mangle PREROUTING and OUTPUT?

Thanks.

#12 - 25.09.2020 14:04 - Jiri Zendulka

I did some progress and transport mode is established and installed on both side but ping 192.168.7.232 <--> 192.168.7.100 does not pass through the IPsec. I see icmp replies at ipsec interface but it looks that are dropped.

```
# tcpdump -i ipsec0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ipsec0, link-type RAW (Raw IP), capture size 262144 bytes
14:00:15.490939 IP 192.168.7.100 > 192.168.7.232: ICMP echo reply, id 29702, seq 0, length 64
14:00:16.491024 IP 192.168.7.100 > 192.168.7.232: ICMP echo reply, id 29702, seq 1, length 64
14:00:17.491450 IP 192.168.7.100 > 192.168.7.232: ICMP echo reply, id 29702, seq 2, length 64
14:00:18.491895 IP 192.168.7.100 > 192.168.7.232: ICMP echo reply, id 29702, seq 3, length 64
14:00:19.492308 IP 192.168.7.100 > 192.168.7.232: ICMP echo reply, id 29702, seq 4, length 64
14:00:20.492729 IP 192.168.7.100 > 192.168.7.232: ICMP echo reply, id 29702, seq 5, length 64

# ip -s link show ipsec0
25: ipsec0@eth0: <NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/none a0:f6:fd:12:7e:6e brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    3648       57       0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    0          0        0       57      0       0
```

I am lookong for a reason and I found some information about XFRMi at https://libreswan.org/wiki/Route-based_XFRMi. There is a note about xfrmi details:

```
...
ip -d link show dev  ipsec1
2: ipsec1@eth0: <NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/none 06:c7:58:c4:b2:c6 brd ff:ff:ff:ff:ff:ff promiscuity 0 minmtu 68 maxmtu 1500
    xfrm if_id 0x1 addrgenmode eui64 numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso_max_segs 65535

ip xfrm state
src 192.1.2.23 dst 192.1.3.209
    proto esp spi 0xa7c66a14 reqid 16393 mode tunnel
    replay-window 32 flag af-unspec
    output-mark 0x1
    aead rfc4106(gcm(aes)) 0xd371dde7df8be108215590f49a084d665417ad63aa1896d51c03173b85d5037d02384567 128
    encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
    if_id 0x1
src 192.1.3.209 dst 192.1.2.23
    proto esp spi 0x873318d8 reqid 16393 mode tunnel
    replay-window 32 flag af-unspec
    output-mark 0x1
    aead rfc4106(gcm(aes)) 0xbda3403de033c690a4c6c54651493bd8590042a56997ae127965e1e1f01de405843c4e55 128
    encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
    anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
```

```
ip xfrm policy
src 192.0.2.1/32 dst 0.0.0.0/0
    dir out priority 1040383 ptype main
    tmpl src 192.1.3.209 dst 192.1.2.23
        proto esp reqid 16393 mode tunnel
    if_id 0x1
src 0.0.0.0/0 dst 192.0.2.1/32
    dir fwd priority 1040383 ptype main
    tmpl src 192.1.2.23 dst 192.1.3.209
        proto esp reqid 16393 mode tunnel
    if_id 0x1
src 0.0.0.0/0 dst 192.0.2.1/32
    dir in priority 1040383 ptype main
    tmpl src 192.1.2.23 dst 192.1.3.209
        proto esp reqid 16393 mode tunnel
    if_id 0x1
...
```

And I wonder why **if_id** and **output-mark** are missing at my xfrm interface/state/policy. I do not know if it is important in this issue or not.

```
#  ip -d link show dev ipsec0
25: ipsec0@eth0: <NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/none a0:f6:fd:12:7e:6e brd ff:ff:ff:ff:ff:ff promiscuity 587356
    xfrm addrgenmode random numtxqueues 587356 gso_max_size 587356 gso_max_segs 587356
# ip xfrm state
src 192.168.7.100 dst 192.168.7.232
        proto esp spi 0xced287fa reqid 1 mode transport
        replay-window 0
        auth-trunc hmac(sha1) 0xe2edb1abfa609bdebd8baff75068081fcffbb70f 96
        enc cbc(aes) 0x7329316f583e9059acaae3594fa5a7a5
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.7.100/32 dst 192.168.7.232/32
src 192.168.7.232 dst 192.168.7.100
        proto esp spi 0xc6181cfd reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x8361d128fba32500705dc5ae37bcecbaebb188a6 96
        enc cbc(aes) 0x4aff8f2cea9637ced716e62ea75b97a3
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        sel src 192.168.7.232/32 dst 192.168.7.100/32
# ip xfrm policy
src 192.168.7.100/32 dst 192.168.7.232/32
        dir out priority 367231
        tmpl src 0.0.0.0 dst 0.0.0.0
                proto esp spi 0xced287fa reqid 1 mode transport
src 192.168.7.232/32 dst 192.168.7.100/32
        dir in priority 367231
        tmpl src 0.0.0.0 dst 0.0.0.0
                proto esp reqid 1 mode transport
```

Many Thanks.

#13 - 25.09.2020 17:23 - Tobias Brunner

> And I wonder why **if_id** and **output-mark** are missing at my xfrm interface/state/policy. I do not know if it is important in this issue or not.

It's possible your version of iproute2 can't show the interface ID. And output marks are something different, not related to XFRMi (configurable via *set_mark_in|out* in swanctl.conf).