strongSwan - Issue #2082

When Local ID 'Local IP address' and Remote ID 'some string' is used then two tunnels don't work at the same time.

09.08.2016 15:35 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.4.0	**Resolution:**	No change required

Description

Hi,

when I try to establish two ipsec connection with Local ID (IP address) / Remote ID (some string) then tunnels don't work. I am initiator.
If I use config with only one tunnel then it works.
I suspect "identity matching" in ipsec.secrets doesn't work properly in case that two tunnels are configured.

Configuration:

```
conn ipsec1
 left=10.64.0.32
 right=10.40.30.136
 rightid=@responder1
 leftauth=psk
 rightauth=psk
 leftsubnet=192.168.211.0/24
 rightsubnet=192.168.210.0/24
 leftupdown=/etc/scripts/updown
 keyexchange=ikev1
 ikelifetime=3600
 keylife=3600
 rekeymargin=540
 rekeyfuzz=100%
 keyingtries=%forever
 type=tunnel
 ike=aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
 esp=aes128-sha256,aes128-sha1,3des-sha1
 auto=start

conn ipsec2
 left=10.64.0.32
 right=10.64.0.15
 rightid=@responder2
 leftauth=psk
 rightauth=psk
 leftsubnet=192.168.213.0/24
 rightsubnet=192.168.212.0/24
 leftupdown=/etc/scripts/updown
 keyexchange=ikev1
 ikelifetime=3600
 keylife=3600
 rekeymargin=540
 rekeyfuzz=100%
 keyingtries=%forever
 type=tunnel
 ike=aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
 esp=aes128-sha256,aes128-sha1,3des-sha1
 auto=start
```

Log:

```
...
2016-08-09 13:16:17 charon: 05[NET] received packet: from 10.64.0.15[500] to 10.64.0.32[500] (76 b
ytes)
2016-08-09 13:16:17 charon: 05[ENC] invalid HASH_V1 payload length, decryption failed?
2016-08-09 13:16:17 charon: 05[ENC] could not decrypt payloads
2016-08-09 13:16:17 charon: 05[IKE] message parsing failed
2016-08-09 13:16:17 charon: 05[IKE] ignore malformed INFORMATIONAL request
2016-08-09 13:16:17 charon: 05[IKE] INFORMATIONAL_V1 request with message ID 798849831 processing
failed
2016-08-09 13:16:30 charon: 07[IKE] sending retransmit 3 of request message ID 0, seq 3
2016-08-09 13:16:30 charon: 07[NET] sending packet: from 10.64.0.32[500] to 10.64.0.15[500] (108 b
ytes)
2016-08-09 13:16:30 charon: 14[NET] received packet: from 10.64.0.15[500] to 10.64.0.32[500] (76 b
ytes)
2016-08-09 13:16:30 charon: 14[ENC] invalid HASH_V1 payload length, decryption failed?
2016-08-09 13:16:30 charon: 14[ENC] could not decrypt payloads
2016-08-09 13:16:30 charon: 14[IKE] message parsing failed
2016-08-09 13:16:30 charon: 14[IKE] ignore malformed INFORMATIONAL request
2016-08-09 13:16:30 charon: 14[IKE] INFORMATIONAL_V1 request with message ID 1506804838 processing
 failed
2016-08-09 13:16:35 charon: 16[NET] received packet: from 10.64.0.15[500] to 10.64.0.32[500] (508
bytes)
2016-08-09 13:16:35 charon: 16[IKE] received retransmit of response with ID 0, but next request al
ready sent
2016-08-09 13:16:54 charon: 13[IKE] sending retransmit 4 of request message ID 0, seq 3
2016-08-09 13:16:54 charon: 13[NET] sending packet: from 10.64.0.32[500] to 10.64.0.15[500] (108 b
ytes)
2016-08-09 13:16:54 charon: 08[NET] received packet: from 10.64.0.15[500] to 10.64.0.32[500] (76 b
ytes)
2016-08-09 13:16:54 charon: 08[ENC] invalid HASH_V1 payload length, decryption failed?
2016-08-09 13:16:54 charon: 08[ENC] could not decrypt payloads
2016-08-09 13:16:54 charon: 08[IKE] message parsing failed
2016-08-09 13:16:54 charon: 08[IKE] ignore malformed INFORMATIONAL request
2016-08-09 13:16:54 charon: 08[IKE] INFORMATIONAL_V1 request with message ID 884680444 processing
failed
```

Status:

```
Connections:
      ipsec2:  10.64.0.32...10.64.0.15  IKEv1
      ipsec2:   local:  [10.64.0.32] uses pre-shared key authentication
      ipsec2:   remote: [responder2] uses pre-shared key authentication
      ipsec2:   child:  192.168.213.0/24 === 192.168.212.0/24 TUNNEL
      ipsec1:  10.64.0.32...10.40.30.136  IKEv1
      ipsec1:   local:  [10.64.0.32] uses pre-shared key authentication
      ipsec1:   remote: [responder1] uses pre-shared key authentication
      ipsec1:   child:  192.168.211.0/24 === 192.168.210.0/24 TUNNEL
Security Associations (0 up, 2 connecting):
      ipsec1[4]: CONNECTING, 10.64.0.32[10.64.0.32]...10.40.30.136[%any]
      ipsec1[4]: IKEv1 SPIs: 91bc86673d355936_i* abeaee537e6dcc83_r
      ipsec1[4]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
      ipsec1[4]: Tasks queued: QUICK_MODE
      ipsec1[4]: Tasks active: ISAKMP_VENDOR MAIN_MODE
      ipsec2[3]: CONNECTING, 10.64.0.32[10.64.0.32]...10.64.0.15[%any]
      ipsec2[3]: IKEv1 SPIs: 61bcb95de1acaccf_i* c462fdba35749285_r
      ipsec2[3]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
      ipsec2[3]: Tasks queued: QUICK_MODE
      ipsec2[3]: Tasks active: ISAKMP_VENDOR MAIN_MODE
```

ipsec.secrets:

```
10.64.0.32 @responder1 : PSK "123456"
10.64.0.32 @responder2 : PSK "012345"
```

History

#1 - 09.08.2016 17:59 - Noel Kuntze

Jiri Zendulka wrote:

> Hi,
>
> when I try to establish two ipsec connection with Local ID (IP address) / Remote ID (some string) then tunnels don't work. I am initiator.
> If I use config with only one tunnel then it works.
> I suspect "identity matching" in ipsec.secrets doesn't work properly in case that two tunnels are configured.

That is wrong. This behaviour is by design of IKEv1. As outlined in RFC 2409,
if PSK authentication is used in IKEv1, the peer identities are determined by their IP addresses and this is what happens here.
The responder tries to authenticate the remote peer with the first secret it finds for its IP address and that is 10.64.0.32 @responder1 : PSK "123456", which obviously won't work, because the remote peer used the second secret, 10.64.0.32 @responder2 : PSK "012345".

#2 - 10.08.2016 08:32 - Jiri Zendulka

Hi Noel,

thanks for your reply...but when I manually remove local ids(local ip addresses) from ipsec.secrets then it works. Both tunnels are up.

Modified ipsec.secrets:

```
@responder1 : PSK "123456"
@responder2 : PSK "012345"
```

If I understand you correctly the "@responder" ID matching shouldn't work for IKEv1 as you mentioned above - because it is not an ip address. But it is work if I remove local IDs.

I think that problem is on initiator side only (not on responder side). On responder side is only one tunnel configured. So ID/PSK mismatch in ipsec.secrets is not possible.

The initiator side is strongswan and the responder side is openswan. When is openswan is used on both sides then it works even if local ip addresses are used as local ids.

#3 - 15.08.2016 12:50 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

> If I understand you correctly the "@responder" ID matching shouldn't work for IKEv1 as you mentioned above - because it is not an ip address. But it is work if I remove local IDs.

The PSK whose associated identities matches best is used. So if you configure the local identity with every PSK every PSK will basically match to some degree. Which is why you should only use remote identities/IPs in ipsec.secrets.

The first lookup is always based on the IP addresses (i.e. every secret that lists the local IP will match). If no PSK is found an initiator will use the configured identities for a second lookup. As responder identities can only be used if aggressive mode is used (which should never be used with PSK). However, if we find a configuration (based on the IPs) a lookup based on the configured identities is done (all matching configs are considered until a PSK is found).

> The initiator side is strongswan and the responder side is openswan. When is openswan is used on both sides then it works even if local ip addresses are used as local ids.

So? The two implementations are completely different (only the syntax of the legacy ipsec/secrets.conf format is roughly the same).

#4 - 16.08.2016 13:22 - Jiri Zendulka

Hi Tobias,

Thanks for clarification how matches in ipsec.secrets works.

You can close this issue.

#5 - 16.08.2016 14:56 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required