strongSwan - Bug #3394

Dynamic leftid of responder on router with multiple IPs

04.04.2020 02:28 - abcd efgh

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.9.0		
Affected version:	5.8.2	**Resolution:**	Fixed

Description

I have a configuration (among others):

ikev1-psk-xauth-adm {
version = 1
aggressive = yes
local_addrs = IP1,IP2
proposals = aes256-sha1-modp2048,aes256-sha1-modp1024
rekey_time = 0s
pools = adm-pool-ipv4
fragmentation = yes
dpd_delay = 30s
dpd_timeout = 90s
if_id_in=99
if_id_out=99
local-1 {
auth = psk
}
remote-1 {
id = keyid:vpn-adm
auth = psk
}
remote-2 {
auth = xauth-eap
}
children {
ikev1-psk-xauth {
local_ts = 192.168.3.0/24, 192.168.4.0/24
rekey_time = 0s
dpd_action = clear
mode = tunnel
esp_proposals =
aes192gcm16-aes128gcm16-prfsha256-ecp256-modp3072,aes192-sha256-ecp256-modp3072,aes256-sha1-modp1024,default
}
}
}

IP1 and IP2 are IPs provided by 2 separate ISPs. They are configured on separate network cards and they have their default gateways in separate routing tables.
I can establish connection with any of those 2 IPs but only once. After that I have no more choice. I can't establish tunnel with IP other than used in first successful attempt. Let's say I restarted strongswan, loaded configuration, connected successfully via IP1 and disconnected. Then my attempts via IP2 return:

initiating Aggressive Mode IKE_SA CONN[1] to IP2
generating AGGRESSIVE request 0 [SA KE No ID V V V V V V]
sending packet: from 192.168.0.115[500] to IP2[500] (676 bytes)
received packet: from IP2[500] to 192.168.0.234[500] (580 bytes)
parsed AGGRESSIVE response 0 [SA KE No ID V V V V NAT-D NAT-D HASH]
received XAuth vendor ID
received DPD vendor ID
received FRAGMENTATION vendor ID

received NAT-T (RFC 3947) vendor ID
selected proposal: IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
IDir 'IP1' does not match to 'IP2'
generating INFORMATIONAL_V1 request 2630440824 [N(INVAL_ID)]
sending packet: from 192.168.0.234[500] to IP2[500] (56 bytes)
establishing connection 'CONN' failed

I thought that responder would set its id to the IP2 but it apparently isn't. I will still be able to connect via IP1. The same would happen if I started with IP2 (then connection via IP1 would fail because resopnder would retrun IP2 as its id).

Is it expected behavior or my configuration is wrong? Should I create separate set of connections with id in local-1? I would prefer to have one definition per connection that would work with both IPs.

I'm aware that IKEv1 with XAUTH in aggressive mode is not secure. This strongswan instance serves multiple site-site VPNs using IKEv2 and modern set of algorithms but unfortunately a few legacy connections must remain available as well. I'm not calling shots here.

Related issues:

Related to Issue #3380: First connection attempt always fail (per group)	**Closed**

Associated revisions

Revision b8f02fc4 - 07.05.2020 15:05 - Tobias Brunner

ikev1: Store fallback identity (IP address) on IKE_SA's auth-cfg

The other auth-cfg object is shared via peer-cfg, so we must not
modify it. It's only stored to simplify memory management.

Fixes #3394.

Revision 1665a4e0 - 07.05.2020 15:05 - Tobias Brunner

ikev1: Use actual local identity as initiator or aggressive mode responder

If none is configured, there is a fallback to the IP address, which is
not stored on the static auth config, but is set on the IKE_SA.

Fixes #3394.

History

#1 - 04.04.2020 02:29 - abcd efgh

s/192.168.0.115/192.168.0.234/

#2 - 06.04.2020 10:11 - Tobias Brunner

- Category changed from configuration to ikev1

- Status changed from New to Feedback

> Is it expected behavior or my configuration is wrong?

Yes, it's completely wrong as (1) you are using IKEv1 and (2) and even worse you are using Aggressive Mode with PSKs.

Anyway, read the logs on the responder to see what it does.

> I'm not calling shots here.

Then I'd advice you to quit in protest.

#3 - 07.04.2020 11:37 - abcd efgh

Log from the responder shows connection that is only half open and therefore deleted:

kwi 07 11:18:13 router-ubuntu charon[148614]: 09[NET] received packet: from INITIATOR_IP[500] to IP2[500] (676 bytes)
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[ENC] parsed AGGRESSIVE request 0 [SA KE No ID V V V V V V]
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] received XAuth vendor ID

kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] received DPD vendor ID
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] received Cisco Unity vendor ID
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] received FRAGMENTATION vendor ID
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] received NAT-T (RFC 3947) vendor ID
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] INITIATOR_IP is initiating a Aggressive Mode IKE_SA
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[IKE] INITIATOR_IP is initiating a Aggressive Mode IKE_SA
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[CFG] selected proposal:
IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[CFG] looking for XAuthInitPSK peer configs matching IP2...KEY_ID_HERE]
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[CFG] selected peer config "vpn-adm"
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[ENC] generating AGGRESSIVE response 0 [SA KE No ID V V V V NAT-D NAT-D HASH]
kwi 07 11:18:13 router-ubuntu charon[148614]: 09[NET] sending packet: from IP2[500] to INITIATOR_IP[500] (580 bytes)
kwi 07 11:18:13 router-ubuntu charon[148614]: 12[NET] received packet: from INITIATOR_IP[500] to IP2[500] (56 bytes)
kwi 07 11:18:13 router-ubuntu charon[148614]: 12[IKE] queueing INFORMATIONAL_V1 request as tasks still active
kwi 07 11:18:17 router-ubuntu charon[148614]: 12[IKE] sending retransmit 1 of response message ID 0, seq 1
kwi 07 11:18:17 router-ubuntu charon[148614]: 12[NET] sending packet: from IP2[500] to INITIATOR_IP[500] (580 bytes)
kwi 07 11:18:24 router-ubuntu charon[148614]: 13[NET] sending packet: from IP2[500] to INITIATOR_IP[500] (580 bytes)
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[NET] received packet: from INITIATOR_IP[500] to IP2[500] (676 bytes)
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[ENC] parsed AGGRESSIVE request 0 [SA KE No ID V V V V V V]
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] received XAuth vendor ID
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] received DPD vendor ID
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] received Cisco Unity vendor ID
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] received FRAGMENTATION vendor ID
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] received NAT-T (RFC 3947) vendor ID
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[IKE] INITIATOR_IP is initiating a Aggressive Mode IKE_SA
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[CFG] selected proposal:
IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[CFG] looking for XAuthInitPSK peer configs matching KEY_ID_HERE]
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[CFG] selected peer config "vpn-adm"
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[ENC] generating AGGRESSIVE response 0 [SA KE No ID V V V V NAT-D NAT-D HASH]
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[NET] sending packet: from IP2[500] to INITIATOR_IP[500] (580 bytes)
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 12[NET] received packet: from INITIATOR_IP[500] to IP2[500] (56 bytes)
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 12[IKE] sending retransmit 1 of response message ID 0, seq 1
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 12[NET] sending packet: from IP2[500] to INITIATOR_IP[500] (580 bytes)
kwi 07 11:18:44 router-ubuntu ipsec[148614]: 06[NET] sending packet: from IP2[500] to INITIATOR_IP[500] (580 bytes)
kwi 07 11:18:44 router-ubuntu ipsec[148614]: 08[JOB] deleting half open IKE_SA with INITIATOR_IP after timeout

I tried to trim the log but there might be some leftovers from other connections left.
Unfortunately I can't find a reason why would responder set IP1 as its ID in this scenario. Initiator correctly connects via IP2 and resopnder seems to be sending packets via IP2 too.
Please advise.

#4 - 07.04.2020 17:28 - Tobias Brunner

- Tracker changed from Issue to Bug

- Assignee set to Tobias Brunner

- Target version set to 5.9.0

- Resolution set to Fixed

I think the problem is that the first time the config is checked and no local identity is found, the IP address is used and stored in the referenced object, which is refcounted and shared by other connections. Besides that that's not thread-safe, it causes this particular problem. I pushed a fix for that to the *3394-ikev1-ip* branch.

#5 - 07.04.2020 20:59 - abcd efgh

Thank you.
I applied https://github.com/strongswan/strongswan/commit/cd1d65ce297ecbc5f835ac79e8f641c54e707e76.patch to the Ubuntu package (5.8.2-1ubuntu3) and tested it. The result is that I can connect only via IP2 now. All connections initiated via IP2 work properly. Every connection attempt via IP1 returns:

calculated HASH does not match HASH payload
generating INFORMATIONAL_V1 request 3478984288 [HASH N(AUTH_FAILED)]

To me it looks like the root cause of this issue may be the same as #3380. The patch made behavior described in #3380 different. After applying it connection via IP1 always fail and connection via IP2 is always established (before applying patch only connections via IP that had first successful tunnel ESTABLISHED worked).

#6 - 08.04.2020 13:16 - Tobias Brunner

> Every connection attempt via IP1 returns:

As far as I can tell, strongSwan always uses the contents of the ID payload (sent or received) directly when calculating the auth hash. So unless a peer sends a different value in the ID payload than it uses when calculating the hash, this should work. I don't really see why it should otherwise (even if there was an option to hard-code a specific remote identity, which is not exchanged in IKEv1, the authentication would fail anyway when the received identity is compared to the configuration). So check your client config.

#7 - 08.04.2020 14:00 - abcd efgh

This is a strongswan config that I use as a client to test this scenario:

```
conn "XF"
keyexchange=ikev1
ikelifetime=1440m
keylife=60m
aggressive=yes
ike=aes256-sha256-modp2048,aes256-sha1-modp2048,aes256-sha1-modp1024
esp=aes192gcm16-aes128gcm16-prfsha256-ecp256-modp3072,aes192-sha256-ecp256-modp3072,aes256-sha1-modp1024
xauth=client
left=192.168.0.234
leftid=keyid:vpn-adm
leftsourceip=%config
leftauth=psk
rightauth=psk
leftauth2=xauth
right=IP1
rightid=IP1
rightsubnet=0.0.0.0/0
xauth_identity=MY_LOGIN
auto=add
```

As you see I set rightid to the IP address that I'm connecting to (right and rightid both have the same value set). I see the same result when using vpnc as a client with config:

```
IPSec gateway IP1
IPSec ID vpn-adm
IPSec secret KEY
Xauth username MY_LOGIN
Xauth password MY_PASSWORD
```

Both strongswan and vpnc clients fail with the same reason.

#8 - 08.04.2020 16:51 - Tobias Brunner

> As you see I set rightid to the IP address that I'm connecting to (right and rightid both have the same value set).

As I said, *rightid* is irrelevant for strongSwan when verifying or generating the HASH payload (the value of the ID payload is used, so both should use the same value). Perhaps the wrong PSK is selected.

#9 - 08.04.2020 18:45 - abcd efgh

Thank you for clarification.

PSK is the same for both IPs. It is configured this way on responder:

```
ike-7 {
secret=SECRET_ADM
id=keyid:vpn-adm
}
ike-8 {
secret=SECRET_USERS
id=keyid:vpn-users
}
```

There are other secrets configured as well for site-to-site tunnels which have secret, id-1 (IP1 or IP2) and id-2 (remote endpoint IP address) set.

The clinet has ipsec.secrets:

IP1 : PSK "SECRET_ADM"
IP2 : PSK "SECRET_ADM"
MY_LOGIN : XAUTH "MY_PASSWORD"

The same PSK for both IP is set on purpose. The main idea is that client can connect using both IPs using exactly the same credentials including group id, PSK and XAUTH.

So if rightid is irrelevant for strongSwan when verifying or generating the HASH payload and PSK is supposed to be the same for both IPs... it should work, but doesn't. In responder logs I see that

kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[CFG] looking for XAuthInitPSK peer configs matching KEY_ID_HERE]
kwi 07 11:18:26 router-ubuntu ipsec[148614]: 09[CFG] selected peer config "vpn-adm"

which seems correct and from there PSK that matches id=keyid:vpn-adm should be used. If I understand this correctly.

#10 - 09.04.2020 10:18 - Tobias Brunner

> There are other secrets configured as well for site-to-site tunnels which have secret, id-1 (IP1 or IP2) and id-2 (remote endpoint IP address) set.

You shouldn't use the local IP address as identity. For IKEv1, there is a fallback for PSK lookups that's based solely on the IP addresses, which will find any PSK that lists the local IP address (matching a single identity is enough, any additional identity is only relevant for a best match).

With the patch, this fallback will now be used (due to this check: source:src/libcharon/sa/ikev1/phase1.c#L159) as no local identity is known anymore when looking up the PSK initially (it is now not stored on the static config anymore). This also explains what was going on in regards to #3380. Only after (incorrectly) storing the identity derived from the IP address on the config the first time was the correct PSK selected (i.e. not the one found based on the IP addresses). I pushed a fix to the branch. As a workaround, don't configure the local IP for any of the secrets.

#11 - 09.04.2020 20:06 - abcd efgh

After applying both patches from 3394-ikev1-ip branch and amending configuration the way you advised (I removed local IP from all the secrets) everything works as I wanted. Clients can connect via both IPs using the same set of credentials. First connection also works.
Your patches and advise fix both this issue and #3380.

Thank you very much for prompt responses, detailed explanations and patches.

#12 - 14.04.2020 11:07 - Tobias Brunner

- Related to Issue #3380: First connection attempt always fail (per group) added

#13 - 07.05.2020 14:59 - Tobias Brunner

- Status changed from Feedback to Closed