Hi,

I have IKEv1 XAUTH PSK configured on Strongswan:

ikev1-psk-xauth-adm {
  version = 1
  aggressive = yes
  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
    }
  }
}
adm-pool-ipv4 {
  addrs = 192.168.255.0/24
  dns = 192.168.3.2, 192.168.3.3
  28674 = int.domain.tld
}
ike-3 {
  secret=some_secret
  id=keyid:vpn-adm
}
radius-1 {
  address = 192.168.45.10
  secret = radius_pass
  sockets = 5
}
There are 4 more groups configured in the same way (with different id and if_id, pool etc). All connections use XFRM interfaces. First connection attempt to a particular group from initiator always fails:

initiating Aggressive Mode IKE_SA XF[1] to 1.2.3.4
generating AGGRESSIVE request 0 [ SA KE No ID V V V V V V ]
sending packet: from 192.168.0.50[500] to 1.2.3.4[500] (636 bytes)
received packet: from 1.2.3.4[500] to 192.168.0.50[500] (544 bytes)
parsed AGRESSIVE response 0 [ SA KE No ID V 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_SHA1_96/PRF_HMAC_SHA1/MODP_2048
calculated HASH does not match HASH payload
generating INFORMATIONAL_V1 request 3478984288 [ HASH N(AUTH_FAILED) ]
sending packet: from 192.168.0.50[500] to 1.2.3.4[500] (92 bytes)

The same happens when vpnc is used as an initiator. Second and all next attempts to a group where one failure has already happened are successful and everything works perfectly fine from that point.

Also there are a few site-to-site tunnels configured but those are working perfectly fine from the beginning and most likely unrelated here. I'm aware of security implication of such setup but unfortunately it's not up to me.

Related issues:
Related to Bug #3394: Dynamic leftid of responder on router with multiple IPs

You shouldn't use IKEv1 anymore, and you should really never use Aggressive Mode with PSKs.

calculated HASH does not match HASH payload

No idea what causes this error, but apparently the two peers calculate the authentication hash differently.

#2 - 23.03.2020 15:52 - abcd efgh
I know that this setup is insecure but I can do nothing about that. It is a requirement to configure it this way.

The thing is that they calculate it differently only during first connection to a particular group (for example after strongSwan was restart). It doesn't matter if strongSwan, vpnc, Android native client or MacOS (which uses racoon for what I know) is used as initiator. That makes me think that it is strictly strongSwan related. It's highly unlikely that all those initiators are guilty here because they all are closed after authentication fails while strongSwan "server" keeps running and probably changes the way how this HASH is calculated (or maybe gets correct values to calculate from after first failure).

I would also like to emphasise that "first try" is not per user/client. It is per group. Example scenario, after strongSwan restart:
- connection to vpn-adm - failure
- connection to vpn-adm - success
- connection to vpn-other - failure
- connection to vpn-adm - success
- connection to vpn-other - success
- connection to vpn-other - success
etc

This behaviour is 100% reproducible.

#3 - 14.04.2020 11:07 - Tobias Brunner
- Related to Bug #3394: Dynamic leftid of responder on router with multiple IPs added

#4 - 14.04.2020 11:07 - Tobias Brunner
- Status changed from Feedback to Closed
- Assignee set to Tobias Brunner
- Resolution set to Fixed