**strongSwan - Issue #3413**

Problems with Checkpoint R77.30 end2end VPN with NAT

17.04.2020 18:13 - Jorge Rovira

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Tobias Brunner</td>
</tr>
<tr>
<td>Category:</td>
<td>interoperability</td>
</tr>
<tr>
<td>Affected version</td>
<td>5.8.4</td>
</tr>
<tr>
<td>Resolution:</td>
<td>No change required</td>
</tr>
</tbody>
</table>

**Description**

Hi,

We are having some problems in order to establish an end2end Ipsec tunnel (with NAT, 10.0.2.2 is an internal IP in our network interface - external ip google connects using NAT) from our strongSwan swanctl 5.6.2 running in a Google Cloud VM on Ubuntu 18.04.4 to a Checkpoint R77.30.

Here the current config on the strongSwan:

```bash
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup
  # charondebug="ike 2, knl 3, cfg 0"
uniqueids=no
strictcrlpolicy=no
conn &default
  authby=psk
type=tunnel
keyexchange=ikev2
  # pfs=yes
# Misc timeouts settings
dpdaction=restart
dpddelay=300s
dpdtimeout=60s
auto=start
  # reauth=no
  # rekey=no
  # modeconfig = push
# Phase 1
#  ike=aes256-sha256-modp4096!
#  ike lifetim e=24h
# Phase 2
#  esp=aes256-sha256-modp4096!
#  lifetime=1h
ike=aes256gcm16-aes256gcm12-aes128gcm12-aes128gcm12-sha256-shal-modp2048-modp4096-modp1024,aes256-
aes128-sha256-shal-modp2048-modp4096-modp1024,3des-shal-modp1024!
esp=aes128gcm12-aes128gcm12-aes256gcm12-aes256gcm12-modp2048-modp4096-modp1024,aes128-aes256-shal-
sha256-modp2048-modp4096-modp1024,aes128-shal-modp2048,aes128-shal-modp1024,3des-shal-modp1024,aes
128-aes256-shal-sha256,aes128-shal,3des-shal!
# NOTE %defaultroute, don't put public ip here
conn c1
  left=%defaultroute
  leftid=45.142.214.54
  *leftsourceip=%config*
  right=35.227.30.42
  rightsubnet=10.1.0.5/32
  rightid=35.227.30.42

We are expecting virtual IP from the Checkpoint R77.30 --> leftsourceip=%config ---- It is expecting virtual ip

With this configuration we see:

07.05.2020
The logs show:

11[IKE] 200.7.90.6 is initiating an IKE_SA
11[IKE] local host is behind NAT, sending keep alives
11[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(MULT_AUTH) ]
11[NET] sending packet: from 10.0.2.2[500] to 200.7.90.6[500] (440 bytes)
15[NET] received packet: from 200.7.90.6[4500] to 10.0.2.2[4500] (300 bytes)
15[ENC] parsed IKE_AUTH request 1 [ IDi AUTH N(CRASH_DET) SA Ti TsR N(INIT_CONTACT) N(ESP_TFC_PAD _N) N(NON_FIRST_FRAG) ]
15[CFG] looking for peer configs matching 10.0.2.2[any]...200.7.90.6[200.7.90.6]
15[CFG] selected peer config 'c1'
15[IKE] authentication of '200.7.90.6' with pre-shared key successful
15[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
15[IKE] authentication of '[right public IP address]' (myself) with pre-shared key
15[IKE] IKE_SA c1[3] established between 10.0.2.2[right side public IP address]...200.7.90.6[200.7 .90.6]
15[IKE] scheduling reauthentication in 9992s
15[IKE] maximum IKE_SA lifetime 10532s
15[IKE] expected a virtual IP request, sending FAILED_CP_REQUIRED
15[IKE] configuration payload negotiation failed, no CHILD_SA built
15[IKE] failed to establish CHILD_SA, keeping IKE_SA

On the checkpoint R77.30 we are not seeing the SA proposal nor TSi or TSr

Is there something we need to consider on the StrongSwan configuration or the Checkpoint R77.30 configuration in order to make sure we can pass phase 2?
The other side Checkpoint R77.30 is claiming they don't have an option to enable virtual IP. Is there something we are missing. Every help we can get is welcomed.

Thanks!

History

#1 - 20.04.2020 18:20 - Tobias Brunner
- Description updated
- Status changed from New to Feedback

leftsourceip is a client option, it makes no sense as responder (see VirtualIP for details).

#2 - 28.04.2020 19:07 - Jorge Rovira

Tobias Brunner wrote:

leftsourceip is a client option, it makes no sense as responder (see VirtualIP for details).

Thanks!

#3 - 28.04.2020 19:24 - Tobias Brunner
- Status changed from Feedback to Closed
- Assignee set to Tobias Brunner
- Resolution set to No change required

7/5/2020