Common errors of IPSec Site-to-Site VPN

Srividya Anantapatnaikuni - 2021-07-08 - 0 Comments - in IPSec

Introduction: In this article, we will see the common errors found in establishing the site-to-site ipsec vpn tunnel and its possible reasons.

To view the ipsec logs, run the command `show log vpn ipsec`

The required configuration for a successful connection is explained in these articles:

https://docs.vyos.io/en/crux/configuration/vpn/site2site_ipsec.html

https://support.vyos.io/en/kb/articles/ipsec-site-to-site-vpn-2

Successful connection:

```
charon: 13[ENC] parsed QUICK_MODE response 3604205383 [ HASH SA No KE
ID ID ]
charon: 13[CFG] selected proposal:
ESP:AES_CBC_128/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ
charon: 13[IKE] CHILD_SA peer-10.2.0.15-tunnel-vti{6} established
with SPIs c0655070_i cf008f0e_o and TS 0.0.0.0/0 === 0.0.0.0/0
```

Errors:

Phase 1 Proposal mismatch

Initiator:

```
charon: 13[ENC] parsed INFORMATIONAL_V1 request 1303032223 [
N(NO_PROP) ]
charon: 13[IKE] received NO_PROPOSAL_CHOSEN error notify
```

Responder:

```
charon: 09[CFG] received proposals:
IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
charon: 09[CFG] configured proposals:
IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
charon: 09[IKE] no proposal found
```

Check if the configured encryption, hash and dh group values are the same between the

peers.

Phase 1 Pre-Shared Key Mismatch

```
charon: 13[ENC] invalid HASH_V1 payload length, decryption failed?
charon: 13[ENC] could not decrypt payloads
charon: 13[IKE] message parsing failed
charon: 13[IKE] ignore malformed INFORMATIONAL request
charon: 13[IKE] INFORMATIONAL_V1 request with message ID 3296715938
processing failed
```

Phase 1 Identifier Mismatch

```
charon: 07[ENC] parsed INFORMATIONAL_V1 request 1394373082 [ HASH
N(AUTH_FAILED)]
charon: 07[IKE] received AUTHENTICATION_FAILED error notify
```

The authentication id/remote-id configured in the initiator should match the remote-id/id of the responder respectively.

Aggressive/Main Mode mismatch:

Initiator:

```
charon: 05[IKE] initiating Aggressive Mode IKE_SA peer-10.30.0.2-
tunnel-vti[2] to 10.30.0.2
charon: 05[ENC] generating AGGRESSIVE request 0 [ SA KE No ID V V V V
V ]
charon: 05[NET] sending packet: from 10.30.0.1[500] to 10.30.0.2[500]
(360 bytes)
charon: 09[NET] received packet: from 10.30.0.2[500] to
10.30.0.1[500] (56 bytes)
charon: 09[ENC] parsed INFORMATIONAL_V1 request 1915047113 [
N(AUTH_FAILED) ]
charon: 09[IKE] <peer-10.30.0.2-tunnel-vti|2> received
AUTHENTICATION_FAILED error notify
```

Responder:

```
charon: 06[IKE] 10.30.0.1 is initiating a Aggressive Mode IKE_SA
charon: 15[IKE] Aggressive Mode PSK disabled for security reasons
charon: 15[ENC] generating INFORMATIONAL_V1 request 1240365724 [
N(AUTH_FAILED) ]
```

Phase 2 Proposal Mismatch

Initiator:

```
charon: 12[ENC] parsed INFORMATIONAL_V1 request 3790314576 [ HASH
```

```
N(NO_PROP) ]
charon: 12[IKE] received NO_PROPOSAL_CHOSEN error notify
```

Responder:

```
charon: 05[CFG] received proposals:
ESP:AES_CBC_256/HMAC_SHA2_256_128/MODP_1024/NO_EXT_SEQ
charon: 05[CFG] configured proposals:
ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ
charon: 05[IKE] no matching proposal found, sending
NO_PROPOSAL_CHOSEN
```

PFS mismatch also sends a similar error message.

If you face any other issue, collect logs and open a ticket in the support portal or raise a query in our forum.

```
sudo swanctl -P
sudo swanctl -L
sudo ip x sa show
sudo ip x policy show
sudo ip -s l
sudo ip a
sudo ip rule show
sudo ip r
sudo ip r show table 220
sudo journalctl /usr/lib/ipsec/charon > /tmp/charon.log
```