strongSwan - Issue #3415

Strongswan on AWS s2s VPN with Fortinet

18.04.2020 06:56 - Eric F

Status:	Closed		
Priority:	Normal		
Assignee:	Noel Kuntze		
Category:	configuration		
Affected version:	5.7.2	**Resolution:**	No feedback

Description

Problem: No proposal chosen error in log, indicates possible mismatch.

Topology:
internal host-----AWS VPN NAT instance----AWS internet GW-----Internet-site2siteVPN-----Fortinet SG----external hosts

Strongswan 5.7 running on AWS VPN NAT instance, internal IP 172.31.1.250, public IP 18.x.x.x
Site to site VPN needs to be formed between AWS VPN NAT instance and Fortinet SG over the internet

Strongswan config on AWS side:

```
conn VPN
keyexchange=ikev2
authby=secret
type=tunnel
left=172.31.1.250
leftid=18.x.x.x
leftsubnet=172.31.1.0/24,172.31.2.0/24,172.31.3.0/24
right=138.x.x.x
rightsubnet=138.x.x.x
ike=aes128-sha256-modp2048          #Phase 1 integrity check algos
esp=aes128-sha256-modp2048          #Phase 2 Encryption algos
ikelifetime=86400s
lifetime=3600s
auto=start
fragmentation=yes
mobike=no
```

Strongswan log:
sending packet: from 172.31.1.250[500] to 138.x.x.x[500] (36 bytes)
charon: 05[NET] received packet: from 138.x.x.x [500] to 172.31.1.250[500] (518 bytes)
charon: 05[ENC] parsed IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N((40002)) N(FRAG_SUP) V V V]
charon: 05[IKE] no IKE config found for 172.31.1.250...x.x.x.x, sending NO_PROPOSAL_CHOSEN

Fortinet config
Local Peer IP: 138.x.x.x
Remote Peer IP: 18.x.x.x

Encryption Domain:
TS1 local-ip 138.x.x.x/32
TS1 remote-ip 172.31.1.0/24
TS2 local-ip 138.x.x.x/32
TS2 remote-ip 172.31.1.0/24
TS3 local-ip 138.x.x.x/32
TS3 remote-ip 172.31.2.0/24
TS4 local-ip 138.x.x.x/32
TS4 remote-ip 172.31.2.0/24
TS5 local-ip 138.x.x.x/32
TS5 remote-ip 172.31.3.0/24
TS6 local-ip 138.x.x.x/32
TS6 remote-ip 172.31.3.0/24

Phase 1 Parameters:

IKE Main Mode & V2
authentication-method pre-shared-keys
dh-group group14
authentication-algorithm sha-256
encryption-algorithm aes-128-cbc
lifetime-seconds 86400

Phase 2 Parameters:
protocol esp
authentication-algorithm hmac-sha-256-128
encryption-algorithm aes-128-cbc
lifetime-seconds 3600
PFS Yes, group14

History

#1 - 20.04.2020 12:54 - Noel Kuntze

- Category set to configuration

- Status changed from New to Feedback

- Assignee set to Noel Kuntze

Please provide the output of ipsec statusall.
Be aware that fortinet devices do **not** support several subnets per side per CHILD_SA, PSK authentication is insecure, using auto=start is unreliable and fragmentation=yes probably does not do what you think it does.

#2 - 25.09.2020 11:16 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to No feedback