strongSwan - Issue #3401

Strongswan connection to CheckPoint VPN device

08.04.2020 12:16 - Alexandru Mateescu

Status: Feedback
Priority: Normal
Assignee: 
Category: 
Affected version: 5.7.2
Resolution: 

Description

hi.

Over the last 2 days i have tried to debug a connection between a Strongswan system and a CheckPoint firewall.

The IPSEC tunnels seem to be brought up both Phase 1 and 2 but the traffic is not reaching the other peer.

I can see traffic entering the tunnel yet the other party does not see any de-crypts.

the config that i have is below. My peer uses a /32 ip address for phase 2 which is in the same subnet as their public ip address.

On top of that they have a NAT on their side that converts my ip range to a static ip.

Where to look to understand what is going on here?

conn 2
  type=tunnel
  authby=secret
  left=%defaultroute # private ip of openswan instance
  leftid=x.x.x.x   #public ip of openswan instance
  leftsubnet=10.13.2.0/24  # private ip of #openswan/32 and private ip of java application instances/32
  right=a.b.c.d      # public ip of the third party network
  rightsubnet=a.b.c.e/32
  keyexchange=ikev1
  ike=aes256-sha1-modp1024!
  ikelifetime=86400s

#phase2
  esp=aes256-shal-modp1024!
  keylife=3600s
  auto=start

keyingtries=3
  dpdaction=restart
  dpddelay=10
  dpdtimeout=3600

History

#1 - 08.04.2020 13:27 - Tobias Brunner
- Status changed from New to Feedback

I can see traffic entering the tunnel yet the other party does not see any de-crypts.

So figure it out with them.