VPN Troubleshooting

VPN Problems

Links & Infos

IKEv2

Internet Key Exchange Protocol Version 2 (IKEv2)

https://tools.ietf.org/html/rfc5996

Check Point Probleme mit IKEv2

Site to Site using IKEv2 fails with "None of the traffic selectors match the conection"

https://support.checkpoint.com/results/sk/sk157473

How do I change the local id for an IKEv2 IPsec VPN?

https://community.checkpoint.com/t5/Remote-Access-VPN/How-do-I-change-the-local-id-for-an-IKEv2-IPsec-VPN/m-p/14786

Unauthorized VPN access to internal networks via IKEv2 tunnel (CVE-2019-8456)

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk149892

IKEv2 negotiation for Site-to-Site VPN tunnel with 3rd party peer fails if IKEv2 SA payload contains more than 8 proposals

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112139

When Check Point peer is initiator of IKEv2 negotiation, FQDN not being sent

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108817

Debugging IKEv2 on Check Point

Link

What is the IKEView Utility ?

https://support.checkpoint.com/results/sk/sk30994

How to collect a debug for VPN issues

https://support.checkpoint.com/results/sk/sk180488

Debugging Description

- Use Ike debug to validate and understand how both devices are negotiating the parameters

disable acceleration if you can:

```
fwaccel off
vpn debug trunc ALL=5
ike debug trunc
ike debug on TDERROR_ALL_ALL=5
```

Get the file ***$FWDIR/log/legacy_ikev2.xmll*** and check the proposal for both side.
Read the file ***$FWDIR/log/vpnd.elg*** and try to find any inconsistencies.

- IKE is the same for all players, the problem is configuration. Many times, the devices try to send parameters differently of what you expect they do.
- Check Point firewalls try to summarize the networks inside the encryption domain, this is called supernetting.
  It will try to summarize at maximum possible and will send that summarization in place of original one.
  If you have two subnets /24 it will try to send a /23.
- Route based VPN is more flexible than domain based and you can have both configured.
  Use it if you can.
- There's a new version for ikeview.exe capable to read *$FWDIR/log/ikev2.xmll*. (
  https://support.checkpoint.com/results/sk/sk30994)
  Check on support center and if possible use its the best tool to troubleshoot VPN problems on Check Point side.
- Disable debug after all

```
fwaccel on
vpn debug off
```

Revision #12
Created 27 February 2021 08:14:23
Updated 25 August 2023 08:48:15 by Peter Baumann