VPN debug cheat sheet

Misconfiguration troubles, start here

Phase 1/2 properties mismatch

VPN Communities -> Dbl click on the community -> Encryption,Hash,DH Group should MATCH those on VPN peer .
Be careful with IP addressing (no overlap) !
Encryption domain traffic IPs should be a reversed copy of each other between peers .
a) Manage Network Objects -> Dbl click on the remote peer firewall -> Topology -> VPN Domain -> Manually defined ;
b) Do the same but for the properties of the firewall you are logged in ;
c) Security Rules - > Add new Rule (make sure nothing overlaps with rules before it) -> If you want VPN tunnel initiated from both sides - put remote and local networks in the same rule as both source and destination .

… Still on Security Rules

If it is the 1st VPN tunnel on the firewall make sure IPsec protocols are allowed from VPN peer: **ESP, IKE**
- Advisable to exclude IKE from encrypted services : VPN Communities -> Dbl click -> Advanced -> Excluded Services -> Add- > IKE

On Communities

Star - Satellite VPN peers can communicate with each other only via Center gateway, if it allows this
Meshed - VPN peers are equal and can communicate with each other directly

Preshared Key

Make sure it is the same on both peers. VPN communities -> Dbl click ->Advanced Settings -> Use Only Shared Secret ...

Disable NAT inside VPN tunnel

Community -> Advanced Settings -> Disable NAT inside VPN community

Don't forget - Policy install on every change

By Yuri Slobodyanyuk, yuri@yurisk.info

Cont: Configs are ok – enter the debug …

SmartView Tracker - 1st aid, short stay. " No valid SA" just states the obvious - tunnel is down, but not why.

SSH into the module, don't waste your time with GUI

See statistics about existing tunnels

Phase 1 SAs that are up
#**vpn tu**
1
Phase 2 SAs that are up
#**vpn tu**
2

One SA in each direction !

Delete stale tunnels
#**vpn shell**
shell> **delete IKE peer** <IP address of peer>
shell> **delete IPSEC peer** <IP address of peer>

Is VPN daemon listening at all ?
#**ps aux | grep vpnd | grep -v grep**
Look for port 500

Are VPN initiation packets from the peer even reaching my firewall?
#**fw monitor** -e ' accept host(<IP of VPN peer>) and port(500) ; '

Let's get our hands dirty! Log the whole VPN establishment process.
#**vpn debug trunc**
#**vpn debug debug on**
#**vpn debug ikeon**

Now try initiate some interesting traffic.If one of the firewall interfaces is in the encryption domain , do the magic:
ping <IP of remote net> **-I** <local interface IP in encryption domain>
vpn debug ikeoff
vpn debug off
Download to your PC file $**FWDIR/log/ike.elg**
Open it with *IKEVIEWER.EXE* which you download from Checkpoint.com .
Have fun looking at the mysteries of the VPN creation .

By Yuri Slobodyanyuk, yuri@yurisk.info