① We want to add access to server from outside

— ① Give the public ip to server
    — configuring a static nat

  ② set a policy that can be DMZ since its a server most likely config. at DMZ

  — in policy source will be any since we want anyone to access server from outside & destⁿ will the public ip of the server.

② How to troubleshoot IPsec tunnel

— To troubleshoot phase 1 & phase 2 on PA we have to commands to check the configurations done on PA

commands are

{ — show vpn ike-sa
{ — show vpn ipsec-sa

run this command on both side and check the configuration and see if there is any mis configuration.

③ Vwire —

aka bump in wire

bridge traffic betn two interface.

④ Troubleshooting commands on PA.

⟶ google for more.

⑤ Wildfire —

Thread analysis cloud based tool

— When we have unknown signature on the PA and we have configured the PA in that case Wildfire will check the signature on the database to analyze the packet.

It is pretty effective against zero day.

unkn signature can be through — Data/URL/files

⑥ split brain issue in PA firewall

— when we are using one HA link that goes down then both firewall shows Active/Active mode.

so it is recommended to use two HA Link.

⑦ What is diff betn route base VPN & Policy based VPN.

— Policy based VPN – Define proxy ID, Unicast traffic.

— Route based – can run over Dynamic routing protocol over route
multicast traffic can pass through

— we prefer route based VPN