# Firewall Troubleshooting

(Checkpoint Specific)

For typical connectivity issues where a firewall is in question follow these steps to eliminate any issues relating to the firewall.

**Firewall**

1. From the distant device run traceroute command and ping (if allowed).
2. On firewall try to ping the device and look for an arp entry
    a. "***arp –a \| grep x.x.x.x***"
3. Look at SmartView Tracker, SmarLogs, or run the zdebug command to see if it is being dropped. (***fw ctl zdebug drop \| grep x.x.x.x***)
4. Do an "ip route get" on firewall or traceroute to see routing
    a. "***ip route get x.x.x.x***"
    b. "***traceroute x.x.x.x***"
5. Run tcpcump on the interface and look for the device
    a. "***tcpdump –I eth0 host x.x.x.x"***
6. Fw monitor command to see what is traversing the firewall interfaces/virtual machines of the firewall
    a. ***fw monitor –e 'accept host(x.x.x.x);'***

**ClusterXL**

1. Verify cluster status from SmartView Monitor or command line
    a. "***cphaprob stat***" to show cluster status
    b. "***cpstat ha***" – show high availability state
    c. "***cphaprob –a if***" to show interfaces monitored
    d. "***cphaprob -ia list***" to see detailed cluster info/status
    e. Look in smartview Tracker for details sorting on "information" section
    f. "***fw ctl pstat***" command to see sync status

**VPN**

1. For VPN connections look at SmarView Monitor or VPN TU command to look for VPN connection details.
2. Enable IKE debugging to look at Phase one and Phase two details
3. Run fw monitor command with vpn tagging switches for different positions in the firewall chain to see what's occurring at each VM
    ***a. fw monitor -pi +vpn -pO -vpn -e "host(x.x.x.x), accept;"***

**VPN DEBUGGING INSTRUCTIONS*:***

*From the command line ( if cluster, active member )*

- *vpn debug on*
- *vpn debug ikeon*
- *vpn tu*

*Select the option to delete IPSEC+IKE SAs for a given peer (gw)*
*Try the traffic to bring up the tunnel*

- *vpn debug ikeoff*
- *vpn debug off*

***Log Files are***

- *$FWDIR/log/ike.elg*
- *$FWDIR/log/vpnd.elg*

***COMMON MESSAGES:***

*According to the Policy the Packet should not have been decrypted*

- *The networks are not defined properly or have a typo*
- *Make sure VPN domains under gateway A are all local to gateway A*
- *Make sure VPN domains under gateway B are all local to gateway B*

***Wrong Remote Address***

- *Verify remote address*

***Failed to match proposal***

- *sk21636 – cisco side not configured for compression*

***No response from peer***

- *Check encryption domains.*
- *remote end needs a decrypt rule*
- *remote firewall not setup for encryption*
- *something is blocking communication between VPN endpoints*
- *Check UDP 500 and protocol 50*

***No Valid SA***

- *Both ends need the same definition for the encryption domain.*
- *sk19243 – (LAST OPTION) use debedit objects_5_0.c, then add subnets/hosts in users.def*
- *Likely phase2 settings cisco might say 'no proxy id allowed"*
- *Disable NAT inside VPN community*
- *Support Key exchange for subnets is properly configured*
- *Make sure firewall external interface is in public IP in general properties*

***No Proposal chosen***

- *sk19243 – usually caused when a peer does not agree to VPN Domain or subnet mask*
- *make sure that encryption and hash match as well in Phase 2 settings*

***Cannot Identify Peer (to encryption connection)***

- *sk22102 – rules refer to an object that is not part of the local firewalls encryption domain may have overlapping encryption domains*
- *2 peers in the same domain*
- *sk18972 – explains overlapping*

***Invalid ID***

- *sk25893 – Gateway: VPN-> VPN Advanced, Clear "Support key exchange for subnets", Install policy*

***Authentication Failure***

***Payload Malformed***

- *check pre shared secrets*

***RESPONDER-LIFETIME***

- *As seen in ike debugs, make sure they match on both ends*

***Invalid Certificate***

- *sk17106 – Remote side peer object is incorrectly configured*
- *sk23586 – nat rules are needed*
- *sk18805 – multiple issues, define a static nat, add a rule, check time*
- *sk25262 – port 18264 has problems*
- *sk32648 – port 18264 problems v2*
- *sk15037 – make sure gateway can communicate with management*

***No Valid CRL***

- *sk32721 – CRL has expired, and module can't get a new valid CRL*

***Add Negotiation***

- *FW-1 is handling more than 200 key negotiations at once*
- *Set maximum concurrent IKE connections*

***FW MONITOR NOTES***

- *packet comes back i I o O*
- *packet will be ESP between o and O*

***BASIC STUFF TO CHECK IN THE CONFIGURATION:***

***VPN domains***

- *Setup in the topology of an item*
- *Using topology is recommended, but you must define*
- *Looking for overlap, or missing networks.*
- *Check remote and local objects.*

***Encryption Domains***

- *Your firewall contains your networks*
- *Their firewall contains their networks*

***Rule Setup***

- *You need a rule for the originator.*
- *Reply rule is only required for 2 way tunnel*

***Preshared secret or certificate***

- *Make sure times are accurate*

***Security rulebase***

- *make sure there are rules to allow the traffic*

***Address Translation***

- *Be aware that this will affect the Phase 2 negotiations*
- *Most people disable NAT in the community*

***Community Properties***
***Tunnel management, Phase1 Phase2 encryption settings***
***Link selection***

***Routing***

- *Make sure that the destination is routed across the interface that you want it to encrypt on*
- *you need IP proto 50 and 51 for IPSEC related traffic and port 500 UDP for IKE*
- *netstat -rn and look for a single valid default route*
- *Smartview Tracker Logs*

***TRADITIONAL MODE NOTES***

- *encryption happens when you hit explicit rule*
- *rules must be created*

***SIMPLIFIED MODE NOTES***

- *VPN Communities*
- *Encryption happens at rule 0*
- *rules are implied*

***CHECKLIST***

- *Define encryption domains for each site*
- *Define firewall workstation objects for each site*
- *Configure the gateway objects for the correct encryption domain*
- *Configure the extranet community with the appropriate gateways and objects*
- *Create the necessary encryption rules.*
- *Configure the encryption properties for each encryption rule.*
- *Install the security Policy*

***IKE PACKET MODE QUICK REFERENCE***

*- > outgoing*

*< – incoming*

***PHASE 1 (MAIN MODE)***

*1 > Pre shared Secrets, Encryption & hash Algorithms, Auth method, initiator cookie (clear text)*

*2 < agree on one encryption & hash, responder cookie (clear text)*

*3 > random numbers sent to prove identity (if it fails here, reinstall)*

*4 < random numbers sent to prove identity (if it fails here, reinstall)*

*5 > authentication between peers, peers ip address, certificates exchange, shared secrets, expired certs, time offsets*

*6 < peer has agreed to the proposal and has authenticated initiator, expired certs, time offsets*

***PHASE 2 (QUICK MODE)***

*1 > Use a subnet or a host ID, Encryption, hash, ID data*

*2 < agrees with it's own subnet or host ID and encryption and hash*

*3 > completes IKE negotiation*