Network Debug Checklist

It's The Firewalls Fault!!!

How to NOT Blame the Firewall
Determining if the Firewall is the Problem

1) Debug Client

1	Get the source and destination IP addresses where the problem is occurring. If possible get the type of application and the port number. Also get the time of last occurance	▪ SmartTracker will give you some of this
		  ▪ Source IP,
		  ▪ Dest IP,
		  ▪ Source Port,
		  ▪ Dest Port,
		▪ Time of last occurance,
		▪ Time it last worked,
		▪ application name

2	Use traceroute to find the nearest firewall to the client	You will have to confer with a network topology diagram to confirm. ▪ LINUX: traceroute -d <ip> ▪ WIN: tracert -d <ip>
3	Use the nearest firewall to see if traffic is entering the firewall from that client. Use SmartTracker and filter on the source IP of the client. See if you can find the PORT being used by the application	Confer with the caller to see if any traffic is happening at the moment. ▪ SmartTracker - Filter on source/dest/protocol
4	Do PTT to make sure	▪ ping <DNS> ▪ ping <IP>

	you can see the client from the firewall and get to the port of the application.	▪ LINUX: traceroute -d <ip> ▪ WIN: tracert -d <ip> ▪ telnet <ip> <port>
5	Run tcpdump on client side interface and look for syn/ack bidirectional traffic from the client/server. If you see traffic, then its not a firewall problem. Although if its an intermittent problem, then you have to take further steps.	▪ ifconfig; ▪ tcpdump -X -n -i <interface e.g. eth0> (host <ip> or host <ip>) and port <port>
6	Do PTT from the firewall to the server to see if you have connectivity. Watch logs for drops	▪ ping <DNS> ▪ ping <IP> ▪ LINUX: traceroute -d <ip> ▪ WIN: tracert -d <ip> ▪ telnet <ip> <port>

2) Debug Server

1	Use traceroutee to find the nearest firewall to the server	▪ LINUX: traceroute -d <ip> ▪ WIN: tracert -d <ip>
2	Use the nearest firewall to see if traffic is entering the firewall from the CLIENT. Use SmartTracker and filter on the source IP (OR NAT IP) of the client. Filter on the port indicated by Step 1	▪ SmartTracker - Filter on source/dest/protocol
3)	Do PTT on the server to make sure you can see the server and its application	▪ ▪ ping <DNS> ▪ ping <IP> ▪ LINUX: traceroute -d <ip>

		▪ WIN: tracert -d <ip> ▪ telnet <ip> <port>
4)	Run tcpdump on server side interface and look for syn/ack bidirectional traffic from the client/server. This is to confirm that traffic is leaving the server and heading back to the client.	▪ ifconfig; ▪ tcpdump -X -n -i <interface e.g. eth0> (host <ip> or host <ip>) and port <port>

3) Debug Firewall

1	Look at basics: disk, cpu, free mem, process status, network errors	1. SmartMonitor 2. top 3. df -h 4. cpstat os -f all 5. ifconfig - look for collisions
2	Look at licensing!!!	1. cplic print
3	Look at kernel statistics	1. fw ctl pstat