

Network Firewall Specifications			
General Requirements:		Complied (Yes/No)	Remarks, References
1	The Firewall must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth		
2	The Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 + / NDPP certified, if not the same model		
3	The Firewall should belong to a family of products that attains NSS/NIST Approved Certification and attains IPv6 Ready Phase 2 & IPv6 Certification		
4	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance		
5	The administrator authentication shall be facilitated by local database, PKI & remote server such as Radius, LDAP, AD and TACS+		
6	The Firewall system should have provision of Web Content Filter, Application Control, Antivirus systems and Intrusion Prevention in the same solution		
Networking & System Performance Requirements:			
1	The Firewall should support a minimum of 12 x GE RJ45 & 2xGE SFP & 2x10G SFP+ & 1xGE Management & 1 Console interfaces with auto sensing capacity		
2	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth		
3	Should support automatic ISP failover as well as ISP load sharing		
4	The Firewall should support Static, Policy Base, Identity based, Multicast routing and Dynamic routing for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPv6		
5	The Firewall should support Static, Policy Based, and Multicast routing		
6	The Firewall should support throughputs of 20 Gbps or better		
7	The firewall should support throughput of atleast 4Gbps of AES - IPSEC VPN and should be H/W accelerated		
8	should support concurrent session atleast 1.5Mil		
9	Should support new session per second atleast 50,000 or above		
10	Should support and IPS throughput of atleast 1000Mbps with production env. profiles or better with enterprise mix		
Firewall Requirements:			
1	The Firewall should support deployment modes as; "Route Mode" or "Transparent Mode" and support web proxy/ssl proxy		
2	The firewall shall be able to handle VoIP traffic securely with "pinhole opening" and support SIP, SCCP, MGCP and H.323 ALGs		
3	The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)		
4	The Firewall should support Inbound Port Forwarding with inbound Load Balancing if servers are running in high availability (layer 4)		
5	Should support IPv6 ACL to implement security Policy for IPv6 traffic		
6	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc		
7	Should be able to inspect HTTP and FTP traffic when these are deployed using nonstandard port(i.e when HTTP is not using standard port TCP/80)		
8	The Firewall should support deployment of Virtualization at least for 3 virtual context from the day one without any additional cost / licenses		
9	Virtual context must have all security features for use for every single firewall		
IPSEC VPN Requirements:			
1	The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or VPNC certified		
2	The proposed system shall support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional cost for license or solution for VPN client		
3	Firewall must have atleast 100SSL VPN client & 200 IPsec VPN client in Route mode from the day 1		
4	Able to create 10 or more virtual domains		
Application control			
1	Atleast 2500+ application signature must be there & it should able to understand welknown application like P2P, Voice, etc without any dependency on the ports		
2	Solution should have application throughput of atleast 2000Mbps or higher		
Threat Protection			

1	Firewall must able to scan http, https, IMAP, IMAPs, FTP, FTPs, POP, POPs, SMTP, SMTPs & MAPI protocols with AV signatures		
2	Threat prevention throughput must be atleast 600Mbps after enabling AV, Appcontrol & IPS signatures in real world/Enterprise mix scenarios		
SSL VPN Requirements			
1	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN		
2	SSL VPN must have atleast throughput of 200Mbps or higher		
3	The Firewall should support for TWO modes of SSL VPN:1.Web mode,2.Tunnel mode		
Traffic Shaping Requirements			
1	The proposed system should have integrated Traffic Shaping functionality including these features:		
2	capable of enable and disable traffic shaping per firewall policy		
3	capable of setting guarantee bandwidth and maximum bandwidth per firewall policy		
4	ability to Tag and Pass Differentiated Service tagging		
Network Intrusion Detection & Prevention System Requirements:			
1	The IPS capability shall minimally attain Internet Computer Security Association (ICSA) or equivalent		
2	Able to prevent denial of service and Distributed Denial of Service attacks on signature		
3	Supports at least 6000+ attack signature and should be automatic updates directly over the internet for the newly discovered attacks		
4	Security check updates do not require reboot of the unit		
Web & Application Content Filtering System Requirements:			
1	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules		
2	URL database should have atleast 250+ million sites and 70 + categories in 60+ languages		
3	The proposed solution should be able to enable or disable Web Filter per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS		
4	Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies		
5	Shall include Web URL block, Web keyword block, Web Exempt List		
Data Leak Prevention Requirements:			
1	Should have the ability to prevent data loss through SMTP, FTP, HTTP, HTTPS & IM and using any application		
2	Should have built in pattern database and option to configure new patterns as and when required		
Certification			
1	Proposed solution must be in a Leader quadrant of Gartner Enterprise/Network Firewall for atleast last 3 consecutive years		