Netwrok Firewall Specifications

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

	Firewall must able to scan http, https, IMAP, IMAPs, FTP, FTPs, POP, POPs, SMTP, SMTPs & MAPI protocols with AV signatures		
	Threat prevention throughput must be atleast 600Mbps after enabling AV, Appcontrol & IPS signatures in real world/Enterprise mix scenarios		
SSL VPN Requirements			
	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN		
	SSL VPN must have atleast throughput of 200Mbps or higher		
	The Firewall should support for TWO modes of SSL VPN:1.Web mode,2.Tunnel mode		
Traffic Shaping Requirements			
	The proposed system should have integrated Traffic Shaping functionality including these features:		
	capable of enable and disable traffic shaping per firewall policy		
	capable of setting guarantee bandwidth and maximum bandwidth per firewall policy		
	ability to Tag and Pass Differentiated Service tagging		
Network Intrusion Detection & Prevention System Requirements:			
	The IPS capability shall minimally attain Internet Computer Security Association (ICSA) or equivilent		
	Able to prevent denial of service and Distributed Denial of Service attacks on signature		
	Supports at least 6000+ attack signature and should be automatic updates directly over the internet for the newely discovered attacks		
	Security check updates do not require reboot of the unit		
Web & Application Content Filtering System Requirements:			
	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules		
	URL database should have atleast 250+ million sites and 70 + categories in 60+ languages		
	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		
	Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies		
	Shall include Web URL block, Web keyword block, Web Exempt List		
Data Leak Prevention Requirements:			
	Should have the ablity to prevent data loss through SMTP, FTP, HTTP, HTTPS & IM and using any application		
	Should have built in pattern database and option to configure new patterns as and when required		
Certification			
	Proposed solution must be in a Leader quadrant of Gartner Enterprise/Network Firewall for alteast last 3 consecutive years		
	Warranty		
	5 years 24x7 onsite comprehensive warranty from the OEM.(Bidder should attach OEM Authorization letter (MAF) for hardware devices and back to back support commitment letter from the OEM along with technical bid for this particular tender enquiry, without which bid is liable to be rejected.)		