NATIONAL CENTRE FOR SUSTAINABLE COASTAL MANAGEMENT
Ministry of Environment and Forests (MoEF)
Koodal Building, Anna University Campus
Chennai – 600025

Specification for Firewall (Quantity required: 1No)

Supply, Installation, testing, commissioning, Advance replacement and training for Security Firewall with 3year warranty subscription - 1no (24/7 Support)

S.No	Related Services	Technical Description for Firewall
1	General Requirements:	The Firewall should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, 600Mbps throughput etc.
		Appliance should be rack mountable
		The platform must use a hardened OS.
		The platform should use hardware that is optimized for firewall, IPSec and SSL
		Appliance should support for Active – Active connections. It should not depend upon any 3rd party alliance with high availability
		Licensing should be a per device and not user/IP based (should support unlimited users)
		Firewall Architecture should be on multiple tiers (firewall module, logging & policy management server, and the GUI/WebUI Console)
		The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.
		The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols
		The firewall should all the multicast traffic to pass through the firewall system
		The firewall should support multicast tunnels
		The firewall system should have a provision to handle the bandwidth management, if the same is required in future
		The firewall should support IPv6 and IPV4 functionality
		Firewall should work on software blade architecture
		Firewall should be processor based
2	Technical, Interface and Connectivity	The platform must be supplied with atleast 6nos. of 10/100/1000Mbps,
		The platform should support VLAN tagging (IEEE 802.1q)
		The firewall should support ISP link load sharing
		The firewall interfaces have to support the unnumbered IP address
		The platform must be supplied with atleast 6nos. of 10/100/1000Mbps
		Support a minimum of 1000 VLAN’s
		Integrated Multi site management

2	and Connectivity Requirements	Built in storage capacity of 250 G B minimum for storing logs.
		Power Input of 100 – 230V (50-60Hz)
		Encryption support of AES 128-256 bit, 3DES 56-168 bit, Trible data DES
		Integrated certificate authority (X.509)
		Should support 200 or more with globally support protocols.
		Should support star & mesh topology for VPN usage
		Should support an integrated IPS
3	Intrusion Prevention System	Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related DNS cache poisoning, FTP bounce, improper commands
		Signature-based, behavioral, and protocol anomaly, IPS should be an integrated system with firewall
		Encryption support of AES 128-256 bit, 3DES 56-168 bit, Trible data DES, Integrated certificate authority (X.509), Should support 200 or more with globally support protocols, Should support star & mesh topology for VPN usage and Should support an integrated IPS
4	Performance Requirements	The box should be capable of upgrading to new versions/products in case a new feature is released by the OEM.
		The Firewall may support at least 1.2 Million
		The Firewall may support at least 30,000 connections per second processing.
		The Firewall should support throughputs of minimum 5 Gbps
		The appliance should support integrated IPS throughputs of minimum 250 Mbps
5	Firewall Filtering Requirements	The Firewall should also support the standard Layer 3 mode of configuration with Interface IP's. It should be possible to protect the firewall policies from being compromised.
		The Firewall must provide state engine support for all common protocols
		The Firewall must provide NAT functionality, including dynamic and static NAT translations
		The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type
		The Firewall should be able to filter traffic even if the packets are fragmented.
		All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, mime, s/mime, Lotus Notes, MS-Exchange etc
		The Firewall should support database related filtering and should have support for Oracle, MS-SQL, and Oracle SQL-Net.
		The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications
		Support for Filtering TCP based applications
		Support basic inspection by working as a proxy for HTTP, FTP & SMTP traffic
		Should support CLI & GUI based access to the firewall modules
		Local access to firewall modules should support role based access
		Integrated IPS should support hybrid attack detection/prevention with multiple attack protections methods, like Protocol Anomaly, Signature-Based, Day-Zero Protection, etc
		Integrated IPS should protect setup against vulnerabilities in the applications of the protected systems by carrying out deep packet inspection

		Firewall should have option to run as full fledged UTM if required, including AV, Anitispam, URL filtering, & Application Control
6	Firewall Logging and Monitoring Requirements:	The Firewall must send log information to an external log server via an encrypted connection
		The Firewall administration software must provide a means of viewing, filtering and managing the log data
		The Firewall logs must contain information about the firewall policy rule that triggered the log
		The Firewall must provide at a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall
		Support to log in detail all connections which are blocked
		Support to log in detail all connections which go through the Firewall
		Firewall should have an option to save filters
		Log solution should have an option to search for using search strings
		Provision to report all successful connections inbound
		Provision to report all successful connections outbound
		Provision to report traffic levels for inbound & outbound destinations
		Support to generate performance statistics on real-time basis
		Capability to produce reports which measure usage
7	Administration/ Management Requirements:	Dedicated management system and real-time logs system should be provided and the management should a software and not a hardware
		The Firewall administration station must provide a means for exporting the firewall rules set and configuration to a text file.
		Any changes or commands issued by an authenticated user should be logged to a database.
		The Firewall must send SNMP traps to Network Management Servers (NMS) in response to System failures.
		Automatic synchronization ability of rules on multiple firewalls and the management servers at DC & DR sites
		Provision to generate automatic mail alerts
		Provision to send alerts to multiple recipients
		The Firewall must not support any non-secure means of access to the Firewall.
		Support for role based administration of firewall
		Management module should support Role-based approval, Self-approval & Emergency bypass with password)
		Only approved policies can be installed & email notification on installation of policies.
		Should be capable of comparing different policies installed verses new policy intended to apply.
		Management server should give a full view on all changes to objects and rules to generate an audit log for any forensic/ compliance needs.
8	User Authentication Requirements	Support for user authentication at the firewall system for the different TCP/IP applications, like HTTP, SMTP, Telnet & RSH
		Support for integration with the RSA Secure ID as the strong user authentication mode
		Should support machine based authentication for user access across the firewall
		Should support clientless authentication for user access across the firewall
9	URL Filtering Requirements	Should support category based filtering.
		Should support minimum of atleast 90 predefined categories.
		White listing based on IP’s & URL’s.
		Black listing based on IP’s & URL’s.
		Exceptions based on network objects defined.

		Notification of Custom messages or URL redirection.
		Should provide Centralized, daily updates.
		Should support atleast 25 million-plus URLs
10	Web Server Security:	Should offer protection for web servers using separate web security modules
		Should support Malicious code protection.
		Should monitor Web communication for potential executable code
		Blocks malicious executable code from reaching a target host.
		Should be capable of doing real-time security decisions based on session and application information, and protects Web communication even when it spans multiple TCP segments
		Should Identify buffer overflow, heap overflows, and other malicious executable code attacks on Web servers and other applications without the need of signatures
		Should detect malicious executable code within Web communications by identifying existence potential for malicious behavior