Annexure -III

FIREWALL – TECHNICAL SPECIFICATIONS

General Requirements

i. Certified by ICSA 4.1x and EAL 4+.
ii. Internationally accepted marked/Certified like FIPS, USGV6, RoHS, UL/CUL, FCC, CE, VCCI, ISI, etc.
iii. Firewall should be either IPv6 Ready Logo certified or equivalent.
iv. Support Unlimited IP/User license.
v. Support user defined multi zone security architecture.
vi. Firewall policy must facilitate IP, Network, Port, Protocol, Application and Zone.
vii. Should facilitate to apply policy like IPS, Content filtering, Traffic shaping & policy based routing decision on any firewall policy.
viii. User authentication facilitated by services like LDAP and RADIUS.
ix. Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
x. Management access control using Profile/Role based for granular control.
xi. Support at least eight firewall domains/instants with centralized management and with each firewall domains/instances having a separate administrative control OR equivalent.

The following features should be available in the virtualized context environment:

a. Firewall
b. IPSEC and SSL VPN
c. IPS settings
d. URL Filtering settings
e. Application control settings
f. Antivirus settings
g. User and Group settings
h. Log and Reporting settings
i. support for two factor authentication

xii. Configuration backup and restore on to/from a remote system via GUI/CLI over HTTP/SSH/TFTP or equivalent.
xiii. Firmware/OS/software updates via Web UI / TFTP or equivalent and should support version roll back functionality.
xiv. All SNMP versions support (v1, v2c and v3).
xv. Rack Mountable not exceeding 4U (for single solution) with redundant power supply (populated).
xvi. The system should inherit all the standard RFC’s.

Web & Application Content Filtering System Requirements:

i. The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
ii. URL database should have at least 40+ million sites and 25+ categories.
iii. The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
iv. Should be able to block web plug-ins such as ActiveX, Java Applet, and Cookies.
v. Should be able to block individual web URL's / IP’s.

vi. The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.
vii. The solution shall allow administrators to create multiple new local URL filtering categories besides dynamic categories
viii. Should have application control feature
ix. Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, BitTorrent etc.
x. Should have minimum database of 2000 applications for application control

User Authentication

The proposed Firewall shall be able to support various form of user Authentication methods simultaneously, including:

i. Local Database entries
ii. LDAP server entries
iii. RADIUS server entries
iv. TACACS+ server entries
v. Native Windows AD (Single sign on capability)
vi. Two-factor authentication without any external Hardware.
vii. The solution shall be capable of providing Windows AD single sign-on by means of collector agents which broker between users when they log on to the AD domain and the device.
viii. The proposed appliance shall support inbuilt 2 factor authentication services and database using tokens, email and SMS.
ix. System should also have capability to identify devices (ex. Android, IPhone, Windows, etc.) & should be able to write policies on basis of device identity.
x. Should also support Authentication-based routing

IPSEC VPN Requirements:

i. The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or equivalent
ii. The proposed system shall comply/support industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules:
iii. The device shall utilize inbuilt hardware acceleration support for:
    a. IPSEC (DES, 3DES, AES) encryption/decryption
    b. SSL encryption/decryption
iv. The system shall support the following IPSEC VPN capabilities:
    a. Multi-zone VPN supports.
    b. IPSec, ESP security.
v. Supports Aggressive and Dynamic mode
vi. Support perfect forward secrecy group 1 and group 2 configuration
vii. MD5 or SHA1 authentication and data integrity.
viii. Automatic IKE (Internet Key Exchange) and Manual key exchange.
ix. Supports NAT traversal
x. Supports Extended Authentication
xi. Supports Hub and Spoke architecture
xii. Supports Redundant gateway architecture
xiii. DDNS support

Network Requirements

i. Support a minimum 10 nos. of 10/100/1000 Ethernet interfaces (copper) with at least 2 nos. of 10GbE (SFP+ multi-mode) fully populated.
ii. Support IEEE 802.1q (VLAN Tagging) and VLANs on all interfaces with at least 1024 VLANs.
iii. Automatic multiple or at least two ISP failover (condition based on ICMP, TCP or UDP protocol) as well as ISP load sharing for outbound traffic.
iv. Dynamic Routing (RIPv2, OSPF, OSPFv3, BGP4, RIPng), Static Route, Policy Based Routing, Multicast Routing.
v. Firewall throughput of at least 20 Gbps.
vi. Concurrent Sessions of at least 5 million.
vii. Should support new session per second at least 190,000
viii. Should support and IPS throughput of 5.0 Gbps or better
ix. Should support and GAV throughput of upto 2 Gbps
x. Should support and SSL VPN throughput of upto 1 Gbps
xi. Should support Site to Site VPN Tunnels up to 10,000
xii. Should support Client to Site VPN Tunnels up to 50,000
xiii. Should support End Point Protection Client up to 2000
xiv. New Sessions per second of at least 120,000.
xv. Support Firewall policies of at least 10000.
xvi. Firewall should operate in Route mode and transparent mode.
xvii. Traffic shaping/bandwidth management on a per policy basis for specific network/IP/Interface/Zone (individual or shared) and should be able to define guaranteed, burstable/maximum bandwidth per policy. Also able to set different level of priority.
xviii. Support DHCP server, DHCP client, DHCP relay, DNS client and NTP client.
xix. Support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT and IPv6 to IPv4 (vice a versa).
xx. Support both IPv4 and IPv6
xxi. The appliance should support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability.

Support IPSEC VPN with following requirements

i. Net-to-Net, Host-to-Host, Client to site, L2TP & PPTP VPN connection.
ii. 3DES, AES, DES Encryption/Decryption algorithm.
iii. MD5, SHA1, Pre-shared keys & Digital certificate based authentication.
iv. Dynamic mode (Main mode) & Aggressive mode for phase negotiation.
v. Key exchange Manual Key, IKE, PKI.
vi. Support external certificate authorities.
vii. Support commonly available IPsec VPN clients.
viii. Perfect Forward Secrecy (DH groups) (group 1 and 2 configuration)
ix. Supports at least 7000 Site to Site VPN tunnel.
x. IPsec throughput of at least 2Gbps.
xi. Support local certificate authority and able to create/renew/Delete self-signed certificate.
xii. Preloaded with third party certificate authority like VeriSign/Entrust.net/Microsoft and provide
facility to upload any other certificate authority.
xiii. ICSA certified preferred
xiv. Generate GUI based reports categorized by tunnel, group etc.
xv. Hub and spoke architecture.

xvi. Management over GUI using HTTPS or equivalent secures mechanism, SSH and console access.
xvii. NAT traversal.

Data Leak Prevention requirements:

i. Should have the ability to prevent data loss through SMTP, FTP, HTTP, HTTPS & IM
ii. Should have built in pattern database

Support SSL VPN with following requirements:

i. Should support at least 500 SSL VPN users with at least 150 users from day 1.
ii. Should support two factor authentications with LDAP, Radius and using tokens/email/SMS.
iii. Support for clientless or client based VPN in Full Tunnel and Split Tunnel mode.
iv. Should support HTTP/HTTPS proxy, FTP, RDP, SSH, VNC, SMB service access provision through portal.
v. Support on 32 bit and 64 bit OS.
vi. SSL VPN throughput at least 1Gbps.
vii. Certified by ICSA preferred.
viii. Support for all major browsers like Firefox/IE/Chrome etc. Java Script, Basic and Advanced Network Extensions.
ix. Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
x. Generate GUI based reports categorized on IP, user etc.
xi. The Firewall should support for TWO modes of SSL VPN:
xii. Web-only mode: for thin remote clients equipped with a web browser only and support web application such as: HTTP/HTTPS PROXY, FTP, SMB/CIFS, SSH, VNC, RDP
xiii. Tunnel mode, for remote computers that run a variety of client and server applications
xiv. The system shall provide SSL VPN tunnel mode that supports 32 and 64-bit Windows operating systems
xv. The proposed solution shall allow administrators to create multiple bookmarks to add to a group and make these bookmarks available for SSL-VPN users.

17. Support IPS with following requirements

i. ICSA and NSS certified preferred.
ii. IPS throughput of 5 Gbps.
iii. Anomaly detection and prevention up to layer 7 traffic including application type, SSL/TLS and must be applicable on any firewall policy.
iv. Support at least 2500 or more signatures with support for custom IPS signatures.
v. IPS signature updates must be done automatically/schedule directly over Internet and should not require reboot of the appliance.
vi. Should be able to respond to any unauthorized activity, Dos/Distributed Dos, network missuses, pre-attack probes like various types of TCP/UDP scanners etc. that originate from both inside and outside network.
vii. Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
viii. Signatures should have a severity level defined to it, so that it helps the administrator to understand and decide which signatures to enable for what traffic.
ix. Generate GUI based reports categorized by alerts, attackers, severity wise, protocol etc.

18. Web content filtering

i. Support web content filtering up to layer 7 traffic like HTTP, HTTPS, FTP, DNS, SMTP, IMAP, POP3 etc., with Application identification like IM, torrent etc., Allow/Deny traffic based on Src / Dst IP / Networks, Web URLs, Regular expressions, Web plug-ins such as ActiveX , Java Applet & Cookies, Regular file extensions, Spy wares, Ad wares, Time/Day.
ii. Should have URL database of 20 million or more for web content filtering based on categories.
iii. Data leak prevention for up to layer 7 traffic.
iv. Should provide an option to send customized Access denied message to the end user.
v. The proposed solution must block HTTP or HTTPS based anonymous proxy request available on the Internet.
vi. Support for geographical based filtering like country level TLD etc.

19. Gateway Antivirus

i. Should provide protection against viruses, worms or any other malicious content in traffic like SMTP, POP3, IMAP, HTTP/S, FTP etc. and must be configurable/applicable on specific firewall Policy.
ii. Should be able to scan the file either on the basis of flow or buffering.
iii. Should have option to respond to virus detection in several ways like delete/quarantine the file And send notification via e-mail/SMS.
iv. Antivirus signature updates must be done automatically/schedule and should not require reboot of the appliance.
v. Management over GUI using HTTPS or equivalent secures mechanism, SSH and console access.
vi. Support at least 1 million or more signatures
vii. The antivirus signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc.
viii. Support on quarantined facility on the appliance or on a remote system.
ix. Allow/Block/quarantine file type extensions
x. Generate GUI based reports categorized by virus signatures, host/user infected etc.

20. Logging and Reporting

i. Provide separate appliance or software for collection and analysis of UTM Logs and reporting
ii. Have standard report templates
iii. Support scheduling of reports
iv. Support sending of reports by email at scheduled intervals
v. Should provide standard dashboards
vi. Should be possible to offload logs from the logging and reporting appliance to other external storage for long term retention.
vii. Logging up to layer 7 traffic details (firewall policy level, denied traffic details etc.)
viii. Should provide log report in Web/GUI /dashboard based format with detailed information categorized by IP/Application/Port/Protocol etc., able to forward logs to syslog server and sending schedule reports and send via email.
ix. Log storing facility on a local disk or on to a remote system. Logs stored on the local disk must be transferable over network(scheduled) to a remote system and must be in a generic format like
x. CSV, HTML, PDF, Excel(formats) or if proprietary, must provide appropriate software/hardware to generate the report.

xi. Support configurable option for E-mail or SMS alerts (Via SMS gateway) in case of any event trigger.

xii. Should provide information of real time data transfer/bandwidth utilization of individual IP/Application/protocol/port/Interface/Zone.

21. Support and Warranty

i. 24X7 support with 4 hrs response time and 8 hours resolution time. For Hardware replacement (RMA) / resolution time should be within 48 hrs.

ii. Online upgradation of firmware/software/patches as and when required.

iii. Telephonic support with call logging mechanism should be provided on 24x7x365 basis.

iv. The bidder should provide 5 yrs comprehensive warranty for the following:

A) Subscription of all Softwares, Firmware and associated Licenses (of all features) and effective from day one.

B) Warranty for all the supplied Hardware

C) Bidder should ensure that all features of Firewall is functional without requirement of any additional procurements of H/W, S/W , Subscriptions and Licenses.

D) All the H/W replacements and delivery should be taken care by the bidder with no financial implications to NIA.

22. Other Requirements

For all requirements listed above, the necessary cables, connectors, external software media, manuals or any other hardware and software must be bundled and included with the firewall appliance.

NOTE: Below features (IPS, IPSEC VPN, SSL VPN) can be embedded in the firewall or bundled as standalone solution (separate device), which must be compatible (integrated) with the firewall appliance.

23. Installation and Configuration