# **Requirements Specification**

Firewall Appliance for Main Office located at Male’ – Qty 1

IMPORTANT:

* Given in the sheet are the functionalities and features to be in the submitting solutions. Should there be a feature limited to a specific brand, an alternative solution may be provided and mentioned in the vendor comments column, to avoid being disqualified from the bid.
* All proposals without a fully filled checklist sheet, will be disqualified. A dash (-) must be written, in **Vendor Comment** column, should there be no comments to be made. In the **Compliance (YES/NO)** column, no field should be left unattended.
* Specified are the minimum requirements. Submitting a solution higher than the recommendation will not disqualify the bid.

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Hardware-based appliance and rack mountable |  |  |
| Support High Availability Configuration (Active-Active, Active-Passive) |  |  |
| Support stateful protocol filtering, deep packet inspection, and detection of attacks within the payload. |  |  |
| The proposed firewall solution must be extensible to accommodate the growing needs of our work place and keep up with higher throughput requirements to cater a minimum of 250 live users (either on premises or through remote sites) |  |  |
| Provide a centralized web management console. |  |  |

# General Features

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Client based VPN access (minimum 50 Concurrent Users) |  |  |
| Identity awareness-based Firewall |  |  |
| Intrusion Prevention System (IPS) |  |  |
| Web Content and Application Filtering /URL Filtering |  |  |
| Bandwidth Management (minimum requirements given below)Active Directory Users and GroupsExternal UsersApply rules to specific devicesApply rules to specific websites or applications |  |  |
| Able to create security policy definitions per Microsoft Active Directory user, role, computer name, IP address or MAC address specific aspects of an application and security groups to identify, block or limit usage of applications and widgets like instant messaging, social networking, video streaming, VoIP, games, etc. |  |  |
| Appliance reporting and retain log for minimum 1 year before rewriting |  |  |
| Networking: All internet-based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, NAT Functions etc. |  |  |
| User Authentication through AD, Local and LDAP |  |  |
| FQDN support and should support Mix mode deployment (bridge and gateway mode) |  |  |
| Support Software Defined Networking (SDN) |  |  |
| Support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions |  |  |
| Provide secure access to diverse applications that reside in the data centers (i.e. SQL Server, VoIP, Streaming video, video conferencing, Remote Desktop Services, web-based line of business applications, etc.) |  |  |
| Enable secure remote access to authorized resources from inside and outside of the networks |  |  |
| Zone-based network segmentation and zone protection; DDoS protection against flooding of new sessions |  |  |
| VOIP traffic filtering |  |  |
| Authenticate external users and external devices like laptop and mobile devices (foreign devices to AGO LAN) |  |  |
| Policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, per user group, per tunnel etc. |  |  |
| Able to support agentless integration with Microsoft Active Directory and facilitate Microsoft AD user and group integration within the firewall. |  |  |
| Web and Application filtering |  |  |
| Able to deliver consistent controls to all users, regardless of location or device type. |  |  |
| Provide application function control to identify, allow, block or limit usage of applications and features within them |  |  |
| Must include integrated intrusion detection and prevention (IPS) function  |  |  |
| Identity-based enforcement of the organization’s policies over new evasive, web-based communication technologies (i.e. social media, web mail and popular remote access applications, P2P application sharing, etc.) |  |  |
| Integrated Web security gateway to protect from legacy, emerging/unknown, dynamic and scripted Web Malware |  |  |
| Automatically prevent web-based attacks, including phishing links in emails, phishing sites, HTTP-based command-and-control, and pages that carry exploit kits |  |  |
| Detect in-process credential phishing |  |  |
| Support Multi-Networks  |  |  |

# Performance and Capacities

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Firewall throughput: > 17 Gbps |  |  |
| Threat Prevention throughput: > 2 Gbps |  |  |
| IPsec VPN throughput: > 7 Gbps |  |  |
| SSL VPN throughput: > 1Gbps |  |  |
| Concurrent Sessions: > 2 Million |  |  |
| Support a minimum of 250 VPN users |  |  |
| Support at least 1 Gbps sustained throughput with all firewall and associated security features enabled |  |  |

# Hardware Specification

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Minimum interfaces supported: 8 Port 10/100/1000 Base-T RJ45, 2 SFP. All ports must be compatible with the existing network equipment currently at our work place |  |  |
| Management I/O: 10/100/1000 out-of-band management port, (2) 10/100/1000, high availability, (1) RJ-45 console port, (1) USB Type C (optional) |  |  |
| Rack mountable |  |  |
| Storage minimum 240GB SSD |  |  |
| Memory or RAM 16GB |  |  |

# Threat Prevention

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Able to determine if an unknown traffic is a threat or not |  |  |
| Able to detect and prevent protocol misuse, malware communications, tunneling attempts and generic attack types without signatures |  |  |
| Detect and block unsanctioned peer to peer traffic |  |  |
| The Proposed Solution (Firewall, IPS, Application Control, URL Filtering, Anti-Virus & Anti-Bot, Sandboxing) should support for Active – Active connections without a dependency on a 3rd party product or appliance |  |  |
| Ability to see all unknown traffic on all ports in one management location |  |  |

# VPN

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Client VPN Based Solution, authentication to work network via users’ Active Directory Credentials |  |  |
| The hardware platform & NGFW with integrated SSL VPN application has to be from the same OEM |  |  |
| VPN users’ activity monitoring, logging and reporting. Must be able to view the activity logs of users via the management console |  |  |

# Bandwidth Management

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Load balancing between multiple WAN connections if required |  |  |
| Fair usage policy on reaching data quota, or an alternative for the same |  |  |
| Traffic shaping by network address criteria like MAC address or IP address of users/devices, AD users/group firewall users or other properties of client server protocols, or an alternative for the same |  |  |
| Traffic shaping of HTTP connections by URL or SSL connections by server certificate subject |  |  |
| Scheduling filters for particular day or week period |  |  |

# Monitoring and Reporting Systems

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Able to report events via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution |  |  |
| Support the creation of custom log messages and provide system variable placeholders mechanism to make this use case possible |  |  |
| Store logs for a period of 1-year minimum |  |  |
| Push notifications for:* Up/Down of interface
* Hardware Failure
* Critical Service failure (eg: VPN)
 |  |  |
| Generate reports of (user based wherever appropriate)* Bandwidth usage
* Application Usage
* Accessed websites
* VPN Usage
* Time spends in our networks
* Internet usage, real time bandwidth, accessed areas or servers, approved requests, rejected requests
* Requests made via firewall to high risk applications and blocked applications
* Intrusion attacks with source IP, destination IP or port must be available.
 |  |  |

Training

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| On the job training on system installation, administration and management |  |  |
| Should offer Certified Training for 3 Staff |  |  |

Licenses / Subscription

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Subscriptions to be made for all features at once. All feature subscriptions should be included. (Payments to be made for all features at once, for every successive subscription as well. This includes subscriptions for both appliances and the features that require subscriptions.) |  |  |
| VPN support/subscriptions for 250 users (minimum) |  |  |
| Subscription Duration: 2 years |  |  |

Support and maintenance

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Should have support center in Male’ and should have international support direct from original equipment manufacturer |  |  |
| Provide a documentation for installation, operation, use, and administration of the whole solution |  |  |
| Warranty: Minimum 2-year parts and replacement |  |  |
| Support: Minimum 3-year Onsite support |  |  |
| The vendor must be an authorized partner for the solution(s) they propose (documentation required). Vendor must also be able to provide on-site support when requested. |  |  |

Firewall Appliance for Regional Branch in Addu City Hithadhoo – Qty 1

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Firewall Throughput must be more than 2 Gbps |  |  |
| The VPN AES 128 throughput should be more than 100 Mbps |  |  |
| Should Support Leased Line Connection |  |  |
| Same brand as the main appliance |  |  |
| Encryption of data shared between the appliance at the main office and the branch appliance |  |  |

Delivery, Installation and Configuration

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Delivery: Maximum 30 days upon signing the agreement |  |  |
| Installation: Maximum 10 working days from the date of supply (main branch) |  |  |
| Costs for installation of branch firewall to be borne by the vendor |  |  |
| Should configure mainly as per the rules set in the existing firewall solution at our work network |  |  |
| Should be installed and configured by Certified Engineers employed at the company. (Please attach Certificates, National ID/Work Visa) |  |  |
| Installation engineers should be onsite for the duration of the configuration and migration |  |  |
| Rack mounting and cabling |  |  |
| Migration from existing firewall to the new solution to be completely done by the winning vendor |  |  |
| Update appliances to latest stable firmware |  |  |
| Configure application control policies |  |  |
| Configure AV and Web filtering policies |  |  |
| Configure antispam policies |  |  |
| Configure IPS policies |  |  |
| Configure Malware protection policies |  |  |
| Network segregation and routing configuration |  |  |
| Configure traffic shaping and ISP WAN load balancing |  |  |
| Configure remote access connectivity policies |  |  |
| Firewall monitoring, logging and alert configuration |  |  |
| NAT configuration and DMZ configuration |  |  |
| Creation of configuration documentation |  |  |