# Technical Requirements

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Rack Mountable (Hardware based). |  |  |
| Central web management console |  |  |
| Supports High Availability (HA) Configurations. |  |  |
| Client Based VPN access |  |  |
| Should be able to support with high throughput to cater minimum of 200 live users. |  |  |
| Dual WAN Supported  |  |  |

# General Features

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Client based VPN access (minimum 200 Concurrent Users) |  |  |
| Identity awareness-based Firewall |  |  |
| Bandwidth Management based on:* Active Directory Users and Groups
* External Users
* Apply rules to specific devices.

Apply rules to specific websites or applications. |  |  |
| Includes integrated intrusion detection and prevention (IPS) function |  |  |
| Web Content and Application Filtering /URL Filtering |  |  |
| Able to create and set security policy definitions per AD user, role, computer, IP or MAC address, specific aspects of an application and security groups. |  |  |
| Support Software Defined Networking (SDN) |  |  |
| 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 dual stacking of IPv4 and IPv6 protocols for all firewall features. |  |  |
| Secure access to applications used in SDFC. Includes: SQL Server, VOIP, Video Conference, RDP, O365 and other web-based applications. |  |  |
| 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, mobile devices and IOTs.  |  |  |
| Policy-based traffic shaping (priority, guaranteed, maximum) For applications, user, groups, 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 |  |  |
| Provide application function control to identify, allow, block or limit usage of applications and features within them. |  |  |
| 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  |  |  |
| Supports zero trust network framework. |  |  |

# Performance

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Firewall throughput: > 17 Gbps |  |  |
| Threat Prevention throughput: > 2 Gbps |  |  |
| IPsec VPN throughput: > 9 Gbps |  |  |
| SSL VPN throughput: > 1Gbps |  |  |
| Concurrent Sessions: > 2 million |  |  |
| Support at least 200 VPN users. |  |  |
| Support at least 1 Gbps sustained throughput with all firewall and associated security features enabled. |  |  |

# Hardware Specs

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Minimum interfaces supported: 10 Gigabit RJ45, 2 SFP Ports. All ports must be compatible with the existing network equipment currently at SDFC. |  |  |
| 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 |  |  |
| NGFW throughput greater than 1GBps |  |  |
| Storage minimum 240GB SSD |  |  |

# 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 must 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. |  |  |
| Staff can use a web portal on the firewall to view VPN setups and self-guided access to the corporate intranet. |  |  |

# 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 vendor Training for 2 Staffs (Hardware vendor proprietary professional certification) |  |  |

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.) |  |  |
| **Subscription Duration: 3 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. (Documents required) |  |  |
| 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. |  |  |

Delivery, Installation and Configuration

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Vendor Comment** | **Compliance (YES/NO)** |
| Delivery: Maximum 40 days upon signing the agreement |  |  |
| Installation: Maximum 10 working days from the date of supply (main branch) |  |  |
| Should configure mainly as per the rules/policies suggested by IT department. |  |  |
| Should be installed and configured by Certified Engineers employed at the company. (Must submit certification document and employment letter stating the staff is employed at the organization. ) |  |  |
| 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 |  |  |