# RFP: Supply, Installation and Commissioning of Hardware and Software for CSE

## Annexure #3

## Network & Security Appliances

| Item# | Item | Qty/LOT |
|---|---|---|
| | **Network Equipment** | |
| 1 | Router | 3 Units |
| 2 | Access Switch | 10 Units |
| 3 | 10GbE Layer 3 switch | 5 Units |
| 4 | 10GBASE-T Copper Module | 30 Units |
| 5 | 10GBASE-SR SFP Module | 150 Units |
| 6 | 25GBASE-SR SFP Module | 10 Units |
| 7 | Optical Cable | 1 LOT |
| 8 | Patched Cable (CAT6) | 1 LOT |
| | | |
| | **Security Appliances** | |
| 9 | Firewall Type-1 | 2 Units |
| 10 | Firewall Type-2 | 2 Units |
| 11 | Firewall-Palo Alto | 1 Units |
| | | |
| | | |

# Network & Security Appliances

| 1. Router | | | | |
|---|---|---|---|---|
| **SL** | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 3 (Three) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety standard | | |
| 8 | Enclosure Type | Rack mountable maximum 1 RU | | |
| 9 | Industry Certifications and Evaluations | The proposed solution must be positioned as a Leader in the Wired and Wireless LAN Access Infrastructure for the last two consecutive years. | | |
| 10 | Part No | Bidder should submit BOQ of the proposed device including the details' part number. The bidder should submit the required performance document for the proposed device. | | |
| 11 | Router Processor Type | High-performance multi-core processors | | |
| 12 | General / Functional Requirement | WAN architecture should have centralized control plane architecture. Or Routers should use high performance multi core processors structure. | | |
| | | The device must operate independently of the underlying transport layer, facilitating flexible use of diverse connectivity options such as MPLS, internet, and point-to-point links between locations. | | |
| | | It should support various last mile connectivity i.e. ethernet, T1/E1, ADSL, 4G LTE. WAN controller architecture will be horizontally scalable and will allow to add up to 3000 wan edge devices on WAN. | | |
| | | It should build secure overlay network on any transport and will allow to create various topology like Hub & spoke, full mesh, partial mesh. | | |

| | | | | |
|---|---|---|---|---|
| | | 13WAN controllers should provide key wan capabilities like WAN edge device authentication on wan network, secure control communication with edge device, building overlay network as per requirement like hub & spoke, full mesh etc., best path computation, link performance computation based on latency, loss and jitter, traffic load balancing on secure overlay network based on policy, build and apply various policies and control from central locations like change in topology, applying ACL, QoS, centralize monitoring and management. | | |
| | | WAN edge device should perform actual data forwarding based on control communication from centralize controller. | | |
| | | It should build secure IPsec network between locations for secure communication and allow various last mile connectivity. | | |
| 13 | DRAM | Should have at least DRAM 2GB, preferred 8GB. | | |
| 14 | Hardware Capacity | The proposed device must provide a minimum throughput of 15 Gbps in 1400-byte packets while operating in SD-WAN mode and at least 12 Gbps (preferred 19Gbps) in non-SD-WAN mode. | | |
| 15 | Flash Memory | Integrated Min. 4 GB (installed), preferred 8 GB Flash Memory from day 1. | | |
| 16 | Interfaces | The router must have a minimum of 2x 10Gb SFP+ and 4x 1Gb Ethernet WAN ports from day one. | | |
| | | Mention out of band ports for management. | | |
| 17 | Security hardware | Hardware-based cryptography acceleration (IPsec) | | |
| 18 | Security | Should have Up to 4.3 Gbps of IPsec Internet Mix (IMIX) traffic in SDWAN mode min.5900 & Non SDWAN mode 3000 tunnels, 3900 tunnels preferred. | | |
| | | Router should have minimum support IPV4 1M and IPV6 200K routes from day 1. Number of ACL 3900, Number of Firewall concurrent session 500K, VRF 2000 from day 1.<br><br>Preferred: IPV4 1.5 M and IPV6 1.4 M routes from day 1. Number of ACL 3900, Number of Firewall session 511K, VRF 3900 from day 1. | | |
| | | Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1. | | |
| | | WAN should support end to end segmentation with different routing table per segment and it should be possible to create per segment topology on WAN like HUB & Spoke, full mesh, partial mesh, point to point. | | |
| | | It should be possible to create minimum 4 segments from day-1 | | |
| | | Should support ACL for IPv4 and IPv6, Time based ACL | | |

| | | | | |
|---|---|---|---|---|
| | | Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers like Amazon and Azure and they should able to connect on WAN like any other branch location" | | |
| 19 | Interface support | Minimum: Support connectivity LAN, WAN and 4G/LTE.<br><br>Preferred: Support Gigabit Ethernet, T1/E1, Channelized E1/T1, FXO, 4G/LTE Service Card | | |
| 20 | Supporting Protocols | At least support the following protocols:<br>IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse dense Mode, Resource Reservation Protocol (RSVP), Internet Key Exchange (IKE), Access Control Lists (ACL), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS,RADIUS Authentication, Authorization, and Accounting (AAA), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah<br><br>Router supported advanced protocols along with the mentioned minimum supported ones is preferred. | | |
| 21 | Encapsulations | Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC) and PPP over Ethernet. | | |
| 22 | Expansion Slots | Should have min. 1 Shared module & 1 NIM Module slots from day 1. | | |
| 23 | High Availability & supported Protocol | Support On-Line Insertion (OIR) for Network Interfaces Modules to reduce downtime during fault/repair/upgrade | | |
| | | Redundant power Supply from day 1 | | |

| | | | | |
|---|---|---|---|---|
| | | At least support the following protocols:<br><br>Supported protocol IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), Resource Reservation Protocol (RSVP), Internet Key Exchange (IKE), Access Control Lists (ACL), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS,RADIUS Authentication, Authorization, and Accounting (AAA), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah, SNMP, NTP.<br><br>Router supported advanced protocols along with the mentioned minimum supported ones is preferred. | | |
| | | | | |
| 24 | Management | Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed | | |
| | | Should support Telnet and SSH | | |
| | | Support application performance monitoring. Bidder has to provide all necessary advance license and aggregate throughput should be 2GB from day 1. | | |
| | | Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability from day 1. | | |
| | | Bidder should propose all the necessary hardware, software & license and the entire solution should be offered from single OEM | | |
| 25 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |
| 26 | Manufacturer's part number | Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty | | |
| | | Bidder should submit the required performance document for the proposed device. If the additional accessories are essential, Bidder will provide by this additional accessory according to the proposed model | | |

| | | | | |
|---|---|---|---|---|
| 27 | Installation, Testing and Commissioning | Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network functional and shall provide respective documentation to IT Department | | |
| 28 | Warranty & Support Services | Manufacturer's warranty part number should be mentioned, minimum 3 (three) years warranty for OEM technical solution support. Patch & New Software Upgrade, RMA replacement should be provided for this unit from the date of commissioning. Manufacturer should have local office & Local Depo in Bangladesh | | |

| **2. Access Switch** | | | | |
|---|---|---|---|---|
| | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 10 (Ten) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety standard | | |
| 8 | Enclosure Type | Rack mountable maximum 1 RU | | |
| 9 | Industry Certifications and Evaluations | The proposed solution must be positioned as a Leader in the Wired and Wireless LAN Access Infrastructure for the last two consecutive years. | | |
| 10 | Part No | Bidder should submit BOQ of the proposed device including the details' part number. The bidder should submit the required performance document for the proposed device. | | |
| 11 | General Features | Should have minimum 24 x 1 GE and 4 SFP+ uplink ports from Day one | | |
| | | Flash memory : Minimum 256MB | | |
| | | DRAM: Minimum 512MB | | |
| 12 | Performance | Switching capacity - minimum Up to 128 Gbps | | |
| | | Forwarding Bandwidth : 64 Gbps | | |
| | | Forwarding rate : 95 Mpps | | |
| | | Number of MAC addresses : Minimum 16,000 | | |
| | | Number of STP instances : mentioned by the bidder | | |
| | | Number of SPAN sessions : mentioned by the bidder | | |

| | | | | |
|---|---|---|---|---|
| 13 | Management | Mention out of band ports for management. | | |
| | | Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed | | |
| | | Should support Telnet and SSH | | |
| | | Bidder should propose all the necessary hardware, software & license and the entire solution should be offered from single OEM | | |
| 14 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |
| 15 | Manufacturer's part number | Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty | | |
| | | Bidder should submit the required performance document for the proposed device. If the additional accessories are essential, Bidder will provide by this additional accessory according to the proposed model | | |
| 16 | Installation, Testing and Commissioning | Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network functional and shall provide respective documentation to IT Department | | |
| 17 | Warranty & Support Services | Manufacturer's warranty part number should be mentioned, minimum 3 (three) years warranty for OEM technical solution support. Patch & New Software Upgrade, RMA replacement should be provided for this unit from the date of commissioning. Manufacturer should have local office & Local Depo in Bangladesh | | |

**3. 10GbE Layer 3 switch**

| SL | Item or Related Service | Technical Specification and Standards | Bidder's Response | Reference Document Name and Page No |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 5 (Five) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety standard | | |
| 8 | Enclosure Type | Rack mountable maximum 1 RU | | |

| | | | | |
|---|---|---|---|---|
| 9 | Industry Certifications and Evaluations | The proposed solution must be positioned as a Leader in the Wired and Wireless LAN Access Infrastructure for the last two consecutive years. | | |
| 10 | Part No | Bidder should submit BOQ of the proposed device including the details' part number. The bidder should submit the required performance document for the proposed device. | | |
| 11 | Architecture | Should be highly performed fixed switch with wire rate Layer 2 and Layer 3 throughput on all the ports on the chassis. | | |
| | | Should have minimum of 24x 1/10/25G and 4 x 40/100G transceiver-based ports from Day 1. | | |
| | | Dual redundant AC power supply and redundant Fans from day 1. | | |
| | | Switch should have stacking/virtual chassis feature from Day 1 | | |
| 12 | Switching Performance | Minimum Switching capacity 2 Tbps or more | | |
| | | Minimum Forwarding Throughput 480 Mpps or more. | | |
| 13 | Switch Layer 2 Services | Layer 2 switch ports and VLAN trunks | | |
| | | IEEE 802.1Q VLAN encapsulation | | |
| | | Support for up to 4000 VLANs | | |
| | | Minimum 80,000 MAC Address | | |
| | | Support minimum 9216 bytes Jumbo frame | | |
| | | Switch should have minimum 4 GB DRAM but 16 GB DRAM & Flash are preferred. | | |
| | | Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, Flow control, Jumbo frame, 802.1D, 802.1w, 802.1s, Jumbo frames, 802.3ad, private vlan . | | |
| | | Switch Should have minimum support of Layer 2, Routed Access (RIP, , OSPFv3 – Up to 40000 routes),PBR, PIM-SM,PIM-DM, VRRP, QoS,802.1X, Macsec.<br><br>Switch supported advanced services along with the mentioned minimum supported ones is preferred. | | |
| | | Must have at least 13 MB, preferred 30 MB of shared buffer for traffic/packet Queuing and processing. | | |
| 14 | Switch Layer 3 Services | Switch should support industry standard routing protocols like BGP, OSPF, IS-IS, RIP, Static, ECMP, LISP, VXLAN, PIM, SSM, DVMRP, BFD, VRF aware BFD etc. | | |
| 15 | | | | |
| | | | | |
| | | | | |
| | | Support minimum 4000 L3 VLAN Interfaces or Switched Virtual Interfaces | | |

| | | | | |
|---|---|---|---|---|
| | | Minimum 256,000 flow entries for security and traffic visibility. | | |
| | | Support Dual-stack for IPv4/IPv6 for IPv4-to-IPv6 migration. | | |
| | | Switch should support RFC 7252 (CoAP). | | |
| | | Switch should support VRF, MPLS, Policy based routing | | |
| | | Switch should support 8 queues per port | | |
| | | Switch should support IPv4 and IPv6 QoS classification and policing | | |
| | | Switch should support priority queuing, DSCP, traffic shaping, WRED | | |
| 16 | Security features | Switch should support at least 802.1x for user authentication and authorization, Guest VLAN assignment, MAC based authentication. Dynamic vlan assignment support along with these is preferred. | | |
| | | | | |
| | | Support L2 IEEE 802.1AE -256-bit security from day 1. | | |
| | | Switch should support Encrypted Traffic Analytics (ETA)* feature from day 1. | | |
| | | Switch should support Policy-based Automation & Assurance for Wired & Wireless from day 1. | | |
| | | Switch should have unique secure identity so that its authenticity and origin can be confirmed with OEM. Switch BIOS, software image should be cryptographically signed to ensure integrity and switch should not boot with modified software regardless of user's privilege level. | | |
| | | Switch should able to integrate with NetFlow based campus visibility and threat detection solution and should able to support threat detection within encrypted traffic | | |
| 17 | Management | Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed | | |
| | | Should support Telnet and SSH | | |
| | | Bidder should propose all the necessary hardware, software & license and the entire solution should be offered from single OEM | | |
| 18 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |
| 19 | Manufacturer's part number | Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty | | |
| | | Bidder should submit the required performance document for the proposed device. If the additional accessories are essential, Bidder will provide by this additional accessory according to the proposed model | | |

| | | | | |
|---|---|---|---|---|
| 20 | Installation, Testing and Commissioning | Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network functional and shall provide respective documentation to IT Department | | |
| 21 | Warranty & Support Services | Manufacturer's warranty part number should be mentioned, minimum 3 (three) years warranty for OEM technical solution support. Patch & New Software Upgrade, RMA replacement should be provided for this unit from the date of commissioning. Manufacturer should have local office & Local Depo in Bangladesh | | |

| **4. 10GBASE-T Copper Module** | | | | |
|---|---|---|---|---|
| **SL** | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 30 (Thirty) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety Standard | | |
| 8 | Part No | Bidder Must submit BOQ of proposed device including the details part numbers. The bidder should submit the required performance document for the proposed device. | | |
| 9 | Product Description | IEEE 802.3an, 802.3ab, 802.3u Standard Supported | | |
| | | Data rates should be supported by the module: 100M/1G/10Gbps from Day 1 | | |
| | | Should support copper cabling of link lengths up to 30 meters with 10Gbps speed | | |
| 10 | Originality | Bidder should propose OEM original SFP Module | | |
| | | The transceiver must be of the same brand as per the proposed network devices | | |

| | | | | |
|---|---|---|---|---|
| 11 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |

| 5. 10GBASE-SR SFP Module | | | | |
|---|---|---|---|---|
| **SL** | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 150 (One hundred Fifty) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety Standard | | |
| 8 | Part No | Bidder Must submit BOQ of proposed device including the details part numbers. The bidder should submit the required performance document for the proposed device. | | |
| 9 | Product Description | IEEE 802.3ae 10GBASE Multimode standard | | |
| | | Multimode SFP+ module from Day 1 | | |
| | | Multimode fiber links up to 300 meters | | |
| 10 | Originality | Bidder should propose OEM original SFP Module | | |
| | | The transceiver must be of the same brand as per the proposed network devices | | |
| 11 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |

| 6. 25GBASE-SR SFP Module | | | | |
|---|---|---|---|---|
| **SL** | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 10 (Ten) Units | | |

| | | | | |
|---|---|---|---|---|
| 7 | Environmental | Maintain International Quality Environmental Safety Standard | | |
| 8 | Part No | Bidder Must submit BOQ of proposed device including the details part numbers. The bidder should submit the required performance document for the proposed device. | | |
| 9 | Product Description | IEEE 802.3ae 10GBASE Multimode standard | | |
| | | Multimode supported SFP+ module from Day 1 | | |
| | | Multimode fiber links up to 300 meters | | |
| 10 | Originality | Bidder should propose OEM original SFP Module | | |
| | | The transceiver must be of the same brand as per the proposed network devices | | |
| 11 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |

**7. Optical Cable**

| SL | Qty | Technical Specification and Standards | Bidder's Response | Reference Document Name and Page No |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1 | 30-qty | LC/LC Multi-mode OM4 2 Fiber 15m Cable | | |
| 2 | 40-qty | LC/LC Multi-mode OM4 2 Fiber 5m Cable | | |
| 3 | 60-qty | LC/LC Multi-mode OM4 2 Fiber 3m Cable | | |
| 4 | 65-qty | LC/LC Multi-mode OM4 2 Fiber 2m Cable | | |

**8. Patched Cable (CAT6A/7 or higher)**

| SL | Qty | Technical Specification and Standards | Bidder's Response | Reference Document Name and Page No |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1 | 40-qty | Patched Cable (CAT6)-1 meter | | |
| 2 | 85-qty | Patched Cable (CAT6)-2 meter | | |
| 3 | 85-qty | Patched Cable (CAT6)-3 meter | | |
| 4 | 55-qty | Patched Cable (CAT6)-5 meter | | |
| 5 | 35-qty | Patched Cable (CAT6)-15 meter | | |

# Security Appliances

| 9. Firewall Type-1 | | | | |
|---|---|---|---|---|
| | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 2 (Two) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety standard | | |
| 8 | Enclosure Type | Rack mountable maximum 1 RU | | |
| 9 | Industry Certifications and Evaluations | The proposed solution must be positioned as a Leader in the Network Firewall Infrastructure for the last two consecutive years. Gartner certification is preferred. | | |
| 10 | Part No | Bidder Must submit BOQ of proposed device including the details part numbers. The bidder should submit the required performance document for the proposed device. | | |
| 11 | Hardware Architecture | The appliance based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance. The solution should provide with next-generation firewall, Next-Generation IPS, URL Filtering a malware protection with application visibility/identification from day 1 | | |
| | | The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory. 64 GB preferred. | | |
| | | The appliance should support have 8 x 1GE Copper and 8 x 1/10GE SFP+ ports from day 1 | | |
| | | The appliance should support a network module slot for future expansion | | |
| | | The appliance should have 4 x 10GE SFP+ supported Multimode Module from day one. All the SFP should be OEM original SFP Module. | | |
| | | The proposed firewall solution should have at least 12 core CPU. | | |
| | | The proposed firewall should have at least 900 GB of storage from day 1. | | |

| | | | | |
|---|---|---|---|---|
| | | Should support Active-Active, Active-Standby & Clustering high availability from day one | | |
| 12 | Performance & Scalability | Must have at least 17 Gbps Next Generation Intrusion Prevention system (IPS) Throughput | | |
| | | Must have at least 17 Gbps Firewall with (AVC) Throughput | | |
| | | NG Firewall Must support at least 2 million concurrent sessions with AVC | | |
| | | NG Firewall Must support at least 130,000 connections per second with AVC | | |
| | | NG Firewall Must support at least 8 Gbps IPSec VPN Throughput (1024B TCP w/Fastpath) | | |
| | | NG Firewall Must support at least Maximum VPN Peers 3,000 or more. | | |
| | | NG Firewall Must support TLS minimum 4.5 Gbps | | |
| | | NG firewall should have minimum 2 Virtual firewall/Virtual Domains/Security Context | | |
| | | NG Firewall Must have integrated redundant hot-swappable power supply and redundant hot-swappable FANs tray/ modules | | |
| 13 | NGFW Features | Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. This feature is extremely important for organization to build capabilities to identify internal attacks and malicious connections. Bidder must propose next-generation firewall with intrusion prevention system (IPS), malware and Spyware protection and application detection feature. | | |
| | | Firewall Must support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, zones, vlan, etc | | |
| | | Must support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance. Each instance Must have its own OS & can shutdown/restart an instance when needed | | |
| | | Firewall Must support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat which must be from day 1 (not in license based). | | |
| | | Firewall Must support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality | | |
| | | The solution Must support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6 | | |
| | | The solution Must support Multicast protocols like IGMP, PIM, etc | | |
| | | Must support capability to integrate with other security solutions to receive contextual information like security group tags/names | | |

| | | | | |
|---|---|---|---|---|
| | | Must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. | | |
| | | Must be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. | | |
| | | Must be capable of detecting and blocking IPv6 attacks. | | |
| | | Must support more than 30,000 (excluding custom signatures) IPS signatures or more. Must support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy | | |
| | | Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist | | |
| | | Must support at-least 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and Must be able to create 60 or more application categories for operational efficiency | | |
| | | The Appliance OEM must have its own threat intelligence analysis center and Must use the global footprint of security deployments for more comprehensive network protection. | | |
| | | The detection engine Must support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.) | | |
| | | The detection engine Must support the capability of detecting variants of known threats, as well as new threats | | |
| | | The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. | | |
| | | Must support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly | | |
| | | Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance. Bidder can propose multiple appliance / higher chassis to meet the solution requirement. | | |
| | | Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP | | |

| | | | | |
|---|---|---|---|---|
| 14 | Management | The management platform must be accessible via a web-based interface and ideally with no need for additional client software. The management platform should have capability to manage 10 devices from day 1. | | |
| | | The Management Center should be virtualized, supporting type-1 hypervisors such as VMware. no hardware or platform software considerations necessary. | | |
| | | The management platform must provide a highly customizable dashboard. | | |
| | | The management platform must provide centralized logging and reporting functionality. | | |
| | | The management platform must be capable of integrating third-party vulnerability information into threat policy adjustment routines and automated tuning workflows. | | |
| | | The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators after their authentication. | | |
| | | Should support troubleshooting techniques like Packet tracer and capture. | | |
| | | Should support REST API for monitoring and config programmability. | | |
| | | The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. | | |
| | | The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG). | | |
| | | The centralized management platform must not have any limit in terms of handling logs per day. Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one. | | |
| | | The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. | | |
| | | The management platform support running on-demand and scheduled reports. | | |
| | | The management platform must risk reports like advanced malware, attacks and network. | | |
| | | The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. | | |
| 15 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |
| 16 | Manufacturer's part number | Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty | | |

| | | | | |
|---|---|---|---|---|
| | | Bidder should submit the required performance document for the proposed device. If the additional accessories are essential, Bidder will provide by this additional accessory according to the proposed model | | |
| 17 | Installation, Testing and Commissioning | Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network functional and shall provide respective documentation to IT Department | | |
| 18 | Warranty & Support Services | Manufacturer's warranty part number should be mentioned, minimum 3 (three) years warranty for OEM technical solution support. Patch & New Software Upgrade, RMA replacement should be provided for this unit from the date of commissioning. Manufacturer should have local office & Local Depo in Bangladesh | | |

| **10. Firewall Type-2** | | | | |
|---|---|---|---|---|
| **SL** | **Item or Related Service** | **Technical Specification and Standards** | **Bidder's Response** | **Reference Document Name and Page No** |
| | **1** | **2** | **3** | **4** |
| 1 | Quality | ISO 9001/9002 for manufacturer for quality assurance | | |
| 2 | Brand | To be mentioned by the bidder | | |
| 3 | Model | To be mentioned by the bidder | | |
| 4 | Country of Origin | To be mentioned by bidder | | |
| 5 | Country of Manufacture | To be mentioned by the bidder | | |
| 6 | Quantity | 2 (Two) Units | | |
| 7 | Environmental | Maintain International Quality Environmental Safety standard | | |
| 8 | Enclosure Type | Rack mountable maximum 1 RU | | |
| 9 | Industry Certifications and Evaluations | The proposed solution must be positioned as a Leader in the Network Firewall Infrastructure for the last two consecutive years. Gartner certification is preferred. | | |
| 10 | Part No | Bidder Must submit BOQ of proposed device including the details part numbers. The bidder should submit the required performance document for the proposed device. | | |
| 11 | Hardware Architecture | The appliance based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance. The solution should provide with next-generation firewall, Next-Generation IPS, URL Filtering a malware protection with application visibility/identification from day 1 | | |

| | | | | |
|---|---|---|---|---|
| | | The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory and should support a minimum of 32GB DRAM. | | |
| | | The appliance should support at least 8 x 1G Copper ports, 2 x 1G SFP ports, and 2x10G SFP+ ports from day 1. | | |
| | | The appliance should have 2 x 10GE SFP+ supported Multimode Module from day one. All the SFP should be OEM original SFP Module. | | |
| | | The proposed firewall solution should have at least one 16-core Intel CPU. | | |
| | | The proposed firewall should have at least 200 GB of storage from day 1. | | |
| | | Should support Active-Standby high availability fron day one. | | |
| 12 | Performance & Scalability | Must have at least 4.8 Gbps Next Generation Intrusion Prevention system (IPS) Throughput | | |
| | | Must have at least 5.2 Gbps Firewall with (AVC) Throughput | | |
| | | NG Firewall Must support at least 600K concurrent sessions with AVC | | |
| | | NG Firewall Must support at least 28,000 new connections per second with AVC | | |
| | | NG Firewall Must support at least 2.4 Gbps IPSec VPN Throughput (1024B TCP w/Fastpath) | | |
| | | NG Firewall Must support at least Maximum VPN Peers 800 or more. | | |
| | | NG Firewall Must support TLS minimum 1.4 Gbps | | |
| 13 | NGFW Features | Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. This feature is extremely important for organization to build capabilities to identify internal attacks and malicious connections. Bidder must propose next-generation firewall with intrusion prevention system (IPS), malware and Spyware protection and application detection feature. | | |
| | | Firewall Must support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, zones, vlan, etc | | |
| | | Must support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance. Each instance Must have its own OS & can shutdown/restart an instance when needed | | |
| | | Firewall Must support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat which must be from day 1 (not in license based). | | |

| | | | | |
|---|---|---|---|---|
| | | Firewall Must support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality | | |
| | | The solution Must support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6 | | |
| | | The solution Must support Multicast protocols like IGMP, PIM, etc | | |
| | | Must support capability to integrate with other security solutions to receive contextual information like security group tags/names | | |
| | | Must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. | | |
| | | Must be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. | | |
| | | Must be capable of detecting and blocking IPv6 attacks. | | |
| | | Must support more than 30,000 (excluding custom signatures) IPS signatures or more. Must support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy | | |
| | | Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist | | |
| | | Must support at-least 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and Must be able to create 60 or more application categories for operational efficiency | | |
| | | The Appliance OEM must have its own threat intelligence analysis center and Must use the global footprint of security deployments for more comprehensive network protection. | | |
| | | The detection engine Must support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.) | | |
| | | The detection engine Must support the capability of detecting variants of known threats, as well as new threats | | |
| | | The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. | | |
| | | Must support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly | | |

| | | | | |
|---|---|---|---|---|
| | | Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance. Bidder can propose multiple appliance / higher chassis to meet the solution requirement. | | |
| | | Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP | | |
| 14 | Manufacturer Authorization | Bidder must submit Manufacturer Authorization from the OEM | | |
| 15 | Manufacturer's part number | Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty | | |
| | | Bidder should submit the required performance document for the proposed device. If the additional accessories are essential, Bidder will provide by this additional accessory according to the proposed model | | |
| 16 | Installation, Testing and Commissioning | Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network functional and shall provide respective documentation to IT Department | | |
| 17 | Warranty & Support Services | Manufacturer's warranty part number should be mentioned, minimum 3 (three) years warranty for OEM technical solution support. Patch & New Software Upgrade, RMA replacement should be provided for this unit from the date of commissioning. Manufacturer should have local office & Local Depo in Bangladesh | | |

**11. Firewall-Palo Alto**

| SL | Qty | Technical Specification and Standards | | Bidder's Response | Reference Document Name and Page No |
|---|---|---|---|---|---|
| | 1 | 2 | | 3 | 4 |
| 1 | 1-qty | **Palo Alto PA1410** | | | |
| | | PAN-1RU-RACK-KIT-4POST | Palo Alto Networks 4-Post rack mount kit for 1U PA-1400 | | |
| | | PAN-PWR-C13-C14 | Power cord for PDU with IEC-60320 C13 and IEC-60320 C14 cord ends,15A, 250V max, 10ft | | |
| | | PAN-PWR-450W-AC | PA-1400 450W spare power supply | | |
| | | PAN-SFP-PLUS-SR | SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant | | |
| | | PAN-PA-1410-BND-CORESEC-3YR | PA-1410, Core Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, DNS Security and SD-WAN ), 3 years | | |
| | | PAN-SVC-PREM-1410-3YR | PA-1410, Premium support, 3 years (36 months) term. | | |
| | | PAN-PA-1410-GP-3YR | PA-1410, GlobalProtect subscription, for one (1) device 3 years (36 months) term. | | |