1. Technical Specification for WAN SWITCH FOR DC

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	02 (Two)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
Hardware Architecture	The Switch should have 24 x 10/100/1000 Base-T Ports and 4 x 1G SFP ports
	The switch should support 55Gbps switching capacity and 41.66 Mpps forwarding rate.
	Switch should have 2GB RAM and 4 GB Flash.
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.
	Switch should support minimum 80 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 8 switch in stack
	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.
	Switch should be able to support 3000 IPV4 & 1500 IPV6 routing entries from day-1
	Switch should support minimum 500 Switched Virtual Interfaces.
	The switch should support Jumbo frames of 9216 bytes
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch should support Layer 2 features, Routed Access (RIP, OSPF), Policy Based Routing, PIM Stub Multicast, PVLAN, VRRP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder from day-1
	The proposed switch should be software defined networking capable and be able to atleast integrate easily with the SDN controller from the same OEM.
	Switch shall support application visibility and traffic monitoring with minimum 16K netFlow/sflow/jflow entries.
	Switche should support both front and back beacon LEDs for easy identification of the switch being accessed.
	Switches should have hardware support to connect a Bluetooth dongle to your switch, enabling you to use this wireless interface as an IP management port interface.

High availabity & Resilliency	Switch should support redundant field replacable power supplies	
	Proposed Switch must have stacking kit and cable from day-1	
	Switch should support redundant field replacable fans.	
	Switch should support cross-stack etherchannel.	
L2 Features	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors	
	The switch should support IEEE 802.1Q VLAN encapsulation	
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence	
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability	
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.	
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN	
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth	
	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.	
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.	
	The switch should support IGMP v1, v2 Snooping	
	Switch should support IPv4 and IPv6The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.	
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.	
	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.	
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.	

	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.
	The switch should support MACSec-128
Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring.
	Support sampled NetFlow/SFlow, Switched Port Analyzer, Remote SPAN, shared NetFlow/SFlow policy, RSPAN and packet capture tool like Wireshark for troubleshooting and network visibility.
	Support Network automation with Open PnP, Containers, Python scripting, NETCONF, RESTCONF using YANG
QoS	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port.
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

2. Technical Specification for WAN SWITCH FOR DR

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	01 (One)
Environmental	Maintain International Quality Environmental Safety standard

Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
Hardware Architecture	The Switch should have 24 x 10/100/1000 Base-T Ports and 4 x 1G SFP ports
	The switch should support 55 Gbps switching capacity and 41.66 Mpps forwarding rate.
	Switch should have 2 GB RAM and 4 GB Flash.
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.
	Switch should support minimum 80 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 8 switch in stack
	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.
	Switch should be able to support 3000 IPV4 & 1500 IPV6 routing entries from day-1
	Switch should support minimum 500 Switched Virtual Interfaces.
	The switch should support Jumbo frames of 9216 bytes
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch should support Layer 2 features, Routed Access (RIP, OSPF), Policy Based Routing, PIM Stub Multicast, PVLAN, VRRP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder from day-1
	The proposed switch should be software defined networking capable and be able to atleast integrate easily with the SDN controller from the same OEM.
	Switch shall support application visibility and traffic monitoring with minimum 16K netFlow/sflow/jflow entries.
	Switche should support both front and back beacon LEDs for easy identification of the switch being accessed.
	Switches should have hardware support to connect a Bluetooth dongle to your switch, enabling you to use this wireless interface as an IP management port interface.
High availabity & Resilliency	Switch should support redundant field replacable power supplies.
	Switch should support redundant field replacable fans.
	Switch should support cross-stack etherchannel.
	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
	The switch should support IEEE 802.1Q VLAN encapsulation

L2 Features	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth
	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
	The switch should support IGMP v1, v2 Snooping
	Switch should support IPv4 and IPv6The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.
	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.
	The switch should support MACSec-128
Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring.
	Support sampled NetFlow/SFlow, Switched Port Analyzer, Remote SPAN, shared NetFlow/SFlow policy, RSPAN and packet capture tool like Wireshark for troubleshooting and network visibility.

	Support Network automation with Open PnP, Containers, Python scripting, NETCONF, RESTCONF using YANG
QoS	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port.
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

3.Technical Specification for CORE ROUTER DC AND DR

Item Description	Required Specifications
Quality	ISO 9001/9002 for a manufacturer of quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	03 (Three)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.

Hardware Architecture	The Router should have minimum 4x1G Gigabit Ethernet and 2x10G Gigabit Ethernet Port from day 1. Bidder must provide 2 x 10G Multi mode SFP+ Short Range module for each device from day 1. Module must be OEM original.
	The Router should support IPv4 Forwarding Throughput (1400Bytes) minimum 19.7 Gbps, IPsec Throughput (1400Bytes, clear text) minimum 16.9 Gbps in Non-SDWAN mode
	Number of IPsec SVTI Tunnels minimum 3900
	The router should have 400 Mbps aggregate throughput from day 1 in non-SD-WAN mode
	Router should have 8 GB DRAM from day 1 and can be upgraded to 32 GB for higher scale
	Router should have Flash storage M.2 USB 16GB from day 1 and be upgraded to 32 GB for higher scale
General Features	Number of ACLs per system minimum: 3900
	Number of IPv4 Routes: 1.6M w/ default 8GB, up to 4M w/ 32GB
	Number of IPv6 Routes: 1.5M w/ default 8GB, up to 4M w/ 32GB
	Number of Queues: 15.5K
	Number of NAT Sessions: 1.2M w/ default 8GB, up to 2M w/ 32GB & f Firewall Sessions: 512K
	Number of VRFs: 4000
High availabilty & Resilliency	The Router Should have Redundant N+1
General & Security Features	Proposed router should be Intel x86 CPU with multiple cores allocated to control plane architecture.
	The router should have Access Control Entries (ACE) feature for security with at least 70K capacity is preferable in a single device or cluster architecture.
	The router should have unique Access Control List (ACL) or unified access control feature for security with at least 3900 capacity is preferable in a single device or cluster architecture.
	Hardware-anchored Secure Boot and Secure Unique Device Identification (SUDI) support
	for Plug and Play to verify the identity of the hardware and software
	The router should support 3DES and AES encryption standards
	Should support Inline hardware-accelerated encryption for high-throughput IPsec and MACsec
	The router should support multiple level of privileges and authentication for user access, along with SSH support for secured device access

Routing Protocol	Should have IPv4, IPv6, static routes, RIP and RIPv2, OSPF, EIGRP, BGP, BGP Router Reflector, IS-IS, IGMPv3, PIM SM, SSM, RSVP, ERSPAN, IPSLA, EEM, IKE, ACL, EVC, DHCP, Frame Relay, DNS, LISP, HSRP, RADIUS, Authentication, Authorization, and Accounting (AAA), AVC, DVMRP, IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPsec, L2TPv3, BFD, IEEE 802.1ag, and IEEE 802.3ah
Encapsulations	Generic Routing Encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), High-Level Data Link Control (HDLC), and PPP over Ethernet (PPPoE)
Traffic management	Quality of Service (QoS), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Application Recognition (NBAR)
Cryptographic algorithms	Encryption: DES, 3DES, AES-128, or AES-256 (in CBC and GCM modes), Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit), Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512
Management	Support diagnostic commands and system health checks within the Router
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Comm	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

4.Technical Specification for INTERNET FIREWALL FOR

Item Description	Required Specifications

Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	02 (Two)
Environmental	Maintain International Quality Environmental Safety standard
Form Factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution. The Proposed solution should have named a Leader in the 2020 Forrester Wave for Enterprise Firewalls.
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 & malware protection, URL Filtering with application visibility/identification from day one.
	The appliance hardware should be a 12 Core CPU architecture with a hardened 64 bit operating system to support higher memory
	Support System memory 2 x 32GB
	Support Storage: 900GB SSD from day-1
	Proposed device should have redundant Hot-swappable power supply from day-1
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
Interfaces	The appliance should have 8 x RJ45, 8 x 1/10G SFP+ from day -1 and upgradeable upto 8x1/10G ports in future. Bidder must provide 4 x 10G Multi mode SFP+ Short Range module for each device from day 1. Module must be OEM original.
Performance & Scalability	Should have at least 10.0 Gbps of NGFW performance throughput includes FW, Application Visibility & IPS.
	Should have at least 10.0 Gbps of NGFW performance throughput includes FW & Application Visibility
	NG Firewall should support at least 1.5 million concurrent sessions
	NG Firewall should support at least 90,000 new connections per second or more
	NG Firewall should have 3.2 Gbps TLS throughput from day 1.
	NG Firewall should have 5.5 Gbps IPSec VPN throughput from day 1.
	NG Firewall should have at least 2000 VPN peers or more.

High-Availability Features	Firewall should support Active/active, Active/standby failover allows clustering of up to 8 chassis
	Firewall should support 802.3ad Ether-channel functionality to increase the bandwidth for a segment.
Next-Generation Firewall Featu	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.
	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously
	Firewall should support operating in routed & transparent mode
	Should support Static, RIP, OSPF, OSPFv3 and BGP
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
	Firewall should support Multicast protocols like IGMP, PIM, etc
	Should support security policies based on security group names in source or destination fields or both
	Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc.
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
	Firepower correlates all intrusion events to an impact of the attack, telling the operator what needs immediate attention. The assessment relies on information from passive device discovery, including OS, client and server applications, vulnerabilites, file processing, and connection events, etc.
	Rapid Threat Containment automates quarantine actions by the OEM Identity Services Engine.
	The solution should provide a virtual centralized Threat Visibility Monitoring & Firewall Management system for a minimum of 2 sensors from Day 1 and should be the same OEM.
	The management platform must be accessible via a web-based interface and ideally with no need for additional client software

Management Feature	Centralized configuration, logging, monitoring, and reporting are performed by the Firewall Management Center.
	The management platform must provide a highly customizable dashboard.
	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 subsequent to their authentication.
	Should support REST API for monitoring and configuration 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 management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new 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.
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.

	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

5.Technical Specification for CORE SWITCH DC and DR

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	03 (Three)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
Hardware Architecture	The Switch Should be highly performed fixed switch with wire rate Layer 2 and Layer 3 throughput on all the ports on the chassis.
	The Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch Should support minimum of 16 x 10GE SFP+ ports from day 1. Bidder must provide 6 x 10G Multi mode SFP+ Short Range module for each device from day 1. Module must be OEM original.
	The Switch Should support 10G Ethernet & 1GE Ethernet on all SFP+ access switch ports.
	Support virtual stacking for switch port scalability
	Switch should support NSF/SSO when connected in virtual stack
	The Switch should support minimum 16GB DRAM & 16GB Flash from day 1
	Dual redundant platinum rate power supply and redundant Fans from day 1
Switching Performance	The Switch should support Minimum Switching capacity 480 Gbps or more
	The Switch should support Minimum Forwarding Throughput 360 Mpps or more
Switch Layer 2 Services	Layer 2 switch ports and VLAN trunks
	IEEE 802.1Q VLAN encapsulation
	Support for up to 4094 VLANs
	The Switch should support Minimum 64,000 MAC Address
	Support minimum 9,198 bytes Jumbo frame
	Support STP, RSTP, EtherChannel/LACP, VLAN Trunking, Q-in-Q/IEEE VLAN Tunneling
	The Switch should support 32 MB of shared buffer for traffic/packet Queuing and processing
	Support Routing Protocols Static, OSPF, RIP, Policy-Based Routing/Forwarding, ECMP L3 load Balancing, Virtual redundant Routing Protocol (VRRP) from day 1

Switch Layer 3 Services	Routing protocols BGPv4, IS-IS, IS-ISv4, OSPFv3, MACsec-256 from day 1
	VRF, L3VPN, Ethernet over MPLS, H-VPLS, IPv6 on Virtual Provider Edge, Multicast VPN for network virtualization and segregation from day 1
	The proposed switch should be software defined networking capable and be able to at least integrate easily with the SDN controller from the same OEM.
	Support Minimum Up to 32,000 IPv4 Multicast routes
	Support Minimum Up to 16,000 IPv6 Multicast routes
	Support Minimum Up to 64,000 indirect + direct & Up to 80,000 host IPv4 routes
	Support Minimum Up to 32,000 indirect + direct & Up to 40,000 host IPv6 routes
	Support Minimum Up to 18,000 QoS ACL scale
	Support minimum 1,000 Switched Virtual Interfaces (SVIs)
	Support minimum 13,000 STP Virtual Ports (Port* VLANs) for PVST
	Support minimum 13,000 STP Virtual Ports (Port* VLANs) for MST
	Support minimum 120,000 flow entries for security and traffic visibility.
	The Switch should Support v4 FIB scale Total 224K
	Support Dual-stack for IPv4/IPv6 for IPv4-to-IPv6 migration.
	Support wire-speed forwarding for IPv6 networks
	NAT, VXLAN and PAT from day 1
	Support Internet Group Management Protocol (IGMP), PIM Stub etc.
	Support QoS with 802.1p Class of Service, Weighted Random Early Detection, DSCP field classification, Class-Based Weighted Fair Queuing, Shaped Round Robin scheduling or similar protocol
	Support Stateful Switchover (SSO), OS patch update resiliency and Nonstop Routing for high-availability.
	Support Bootstrap Router Protocol, Multicast Source Discovery Protocol
Security features	Support 802.1X, Router Advertisement guard, IPv6 snooping, IPv6 ND inspection, IPv6 device tracking
	Support Control Plane Policing to protect from DOS attack.
	Support visibility of encrypted traffic for analysis and troubleshooting from day 1
	Support L2 IEEE 802.1AE -128-bit security and L2 IEEE 802.1AE -256-bit security from day 1
	Support OS, Firmware/BIOS & patch authenticity as encrypted images to protect from unauthorized and modified/cracked images.

	Support OS validation during booting to protect from threats
Management features	Support SNMP, Group-based policies, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring.
	The Switch should Support SD-Access, Encrypted Traffic Analytics, and DNA Assurance
	Support sampled NetFlow/SFlow, Switched Port Analyzer, Remote SPAN, shared NetFlow/SFlow policy, RSPAN and packet capture tool like Wireshark for troubleshooting and network visibility.
	Support Network automation with Open PnP, Containers, Python scripting, NETCONF, RESTCONF using YANG
	The switch must have at least 315,790 hours Mean Time Between Failure (MTBF) for hardware reliability.
	Bidder must propose centralize management platform for configuration rollout, change, backup, troubleshooting and performance analysis feature from day 1 with required hardware and software license.
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

6.Technical Specification for WEB PROXY DC AND DR

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	02 (Two)

Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	CISCO
Platform Requirement	The solution should be a hardened Web Proxy, Threat Intelligence via Cisco Talos, Layer 4 traffic monitoring, Application Visibility and Control (AVC), Policy management, Actionable reporting, URL filtering, Third-party DLP integration via ICA and Centralized Web Management Reporting License for atleast 250 user. All the functionalities should be in a single appliance from the day 1.
	The solution should be hardware based
Hardware Architecture	The solution should have minimum two 32GB DDR4-3200 RDIMM RAM
	The solutions should have one 2.9GHz 16c 3200MHz processor
	The solution should have minimum 6 port 1G Base-T copper network interface (NICs)
	The solution should have redundant power supply from day 1
	The solution should have minimum 4.8 TB (4x1.2TB SAS) storage
	Should have min 20+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls.
	The solution should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page and creation of custom URL categories for allowing/blocking specific destinations as required by the Organisation. The solution should have facility for End User to report Mis-categorisation in URL Category.
	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.
	The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.
	When the website is blocked due to suspected malware or URL- Filters it should allow the end user to report that the webpage has been wrongly misclassified.
	The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.

Security Features	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.
	The proxy should support the functionality to configure URL feeds as custom categories
	The proxy should support the functionality to exempt URLs/Ips downloaded from the feed server
	The Proxy should supportr Multi category URLs filtering
	The solution should support HTTPS decryption from day one should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.
	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80.
	Should inspect the sensitive content through pre-defined templates, textual content inside image, cumulative content control and inspection through web channel to prevent the content from being sent over outbound web channel.
	The appliance should support at least 2 industry known Anti Malware/Anti Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and Keyloggers and as defined by the organizations policy. Please mention the antimalware engine.
	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.
	The solution should support signature based application control.
	Solution should support filtering adult content from web searches & websites on search engines like Google.
	Should simplify design and implementation of policy to ensure user compliance
	Should have ability to block anonymizer sites or proxy avoidance tools.
	The Proxy should support ability to filter YouTube Video categorization
	The proxy should support ICAP/ICAPs integration for external DLP
	The solution shall provide option to choose Multiple Antivirus engines
	The proxy should support VDI users identification

	The proxy should support TLS 1.3
	The proxy should support HTTP 2.0
	The Solution should allow admin to choose source IP as IP spoofing featurrer
	The solution should support integration with Private File rreputation and sandbox integration
	The proxy should offer ability to block files based on the file name and file types
	The proxy should offer ability to Add/Remove/Edit HTTP custom or default headers
	The proxy should offer ability to consume Authention header from downstream proxy
	The proxy should offer Office 365 or Cloud Application restriction based on the user/group header/custom headers.
	The proxy should offer ability to anonymise User information in the logs
	The proxy should allow exempting traffic from decryption and further scanning
	The proxy should offer ability to block file upload and download based on the file size
	The solution should support SOCKS4 and SOCKS5
	Solution should provide different action based on categories, protocols, file type, UDL, keyword, regular expression, User, Group, OU, Domain, IP address, etc.
	Offered solution should have real time reputation service for both IP's and URL's
	Solution must be capable of inspecting SSL traffic within the same appliance with no additional hardware required.
	Offered solution must support the real-time graphical and chart-based dashboard for the summary of WEB filtering activities.
	The frequency of updates to the master threat and URL databases should be configurable.
	Solution must not be just signatrure based security but also should have other predictive engines to provide real time checks
	The solution must be able to detect and prevent unknown exploits using behavioral technology
	The solution must be able to detect and block suspecious user agents
LDAP Support	The solution must seamlessly integrate with LDAP, Active Directory and Radius server for user authentication and authorization.
	The proposed solution should have VM based central management appliance with logging and reporting
	For VM based central manager bidder should mention the required resource
	The Support Engineers should be able to login to appliance using secure tunneling methods such as SSH/SSL for troubleshooting purposes
	The appliance should be manageable via command line using SSH and must have serial console access on appliance for emergency sceanrios

	The appliance based Solution should be provided with hardened Operating System. No need of separate OS/database for management and reporting
	Solution to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it. Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files. Solution should support to schedule reports to run on a daily, weekly, or monthly basis.
	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.
	The solution should support REST API for reporting and tracking.
	The solution should support REST API for configuration.
	The appliance should be manageable via centralized configuration manager
Administration, Management ar	The solution should support centrralized reporting and tracking feature.
	The proxy should support automatic config backup
	The proxy should allow to send logs to external server using Syslog, FTP and SCP to external SIEM/Logging server
	The solution should support centralized software upgrade
	The proxy should support 2FA for administrators for secure login to Proxies
	Solution should have drill down reporting interface
	System shall have method of notifying administrator of issues with proxy.
	The appliance should be manageable via command line using SSH
	For emergency, the appliance should have serial console access
	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it
	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.
	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.
	The appliance should provide seamless version upgrades and updates.
	The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.
	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
Manufacturer's part number	Bidder must be submitted Manufacturer Authorization Letter (MAL)

Manufacturer's part number	
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

7. Technical Specification for SERVER FARM SWITCH

Item Description	Required Specifications
Quality	ISO 9001/9002 for a manufacturer, FCC Class A/B for quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	03 (Three)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
Hardware Architecture	The Switch must be 1RU rack-mountable.
	Network Infrastructure equipment must use 240V AC power.
	Must have 2x400W AC Power Supply, Std airflow (port-side exhaust) from day1.
	Must have 4x30CFM FAN module (port-side exhaust airflow) from day1.
	All removable components (including elements such as I/O cards, Expansion Modules, power supplies, and fans) must be hot-swappable with zero disruption to traffic forwarding (Unicast or multicast).
	In the event of a PSU failure, a single power supply Must be able to support the network device.

	Must have a minimum of 24 x 10 GE SFP+ ports enabled from day 1. Bidder must provide 12 x 10G Multi mode SFP+ Short Range module for each device from day 1. Module must be OEM original.
	Should have minimum of 16GB Flash & 16GB DRAM from day1.
Performance & Scalability	Should have minimum of 480 Gbps switching bandwidth and 360 million packets per second (mpps)
	Must support Latency less than 2 microseconds.
	Must support Layer 3 from Day 1.
	Must have Line-rate traffic throughput on all ports at Layer 2.
	Must have Line-rate traffic throughput on all ports at Layer 3
	Must support a minimum of 64,000 MAC address table entries and 64,000 IPv4 hosts.
	Must support minimum 24,000 IPv4 unicast routes and 8,000 IPv4 multicast routes
	Must support minimum 4094 ACL entries
Layer 2 and Layer 3 features	Must support Layer 2 switch ports and VLAN trunks
	Must support IEEE 802.1Q VLAN encapsulation
	Must support Support for up to 4096 VLANs
	Must support Rapid Spanning Tree Protocol (RSTP): 512
	Must support Rapid Per-VLAN Spanning Tree Plus (PVRST+) (IEEE 802.1w compatible)
	Must support MSTP (IEEE 802.1s): 64 instances
	Must support EtherChannel technology (up to 24 ports per EtherChannel)
	Must support Buffer size 6 MB shared among 16 ports; 18 MB total
	Must support LACP: IEEE 802.3ad, IEEE 802.1ax
	Must support Storm control (multicast and broadcast)
	Must support Link-level flow control (IEEE 802.3x),vPC*2,Advanced PortChannel hashing based on Layer 2, 3, and 4 information
	Must support Layer 3 interfaces: Routed ports on interfaces, switch virtual interfaces (SVIs), PortChannels, and subinterfaces (total: 1024)
	Must support 24-way Equal-Cost Multipath (ECMP)
	Must support Routing protocols: Static, RIPv2, EIGRP, OSPF, and BGP
	Must support HSRP and VRRP, VRF route leaking
	Must support ACL: Routed ACL with Layer 3 and 4 options to match ingress and egress ACLs
	Must support VRF: VRF-Lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP), and VRF-aware multicast
	Must support Jumbo frame support (up to 9216 bytes)

Multicast	Must support Multicast: PIMv2, PIM Sparse Mode (PIM-SM), SSM, and BiDir
	Must support Bootstrap router (BSR), Auto-RP, and Static RP
	Must support MSDP and Anycast RP
	Must support Internet Group Management Protocol (IGMP) Versions 2 and 3
Security features	Must support Ingress ACLs (standard and extended) on Ethernet
	Must support Standard and extended Layer 3 to 4 ACLs include IPv4, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP)
	Must support VLAN-based ACLs (VACLs)
	Must support Port-based ACLs (PACLs)
	Must support Named ACLs
	Must support ACLs on virtual terminals (VTYs)
	Must support Dynamic Host Configuration Protocol (DHCP) relay
	Must support Control Plane Policing (CoPP)
	Must support multiple privilege levels for remote access
	Must support Remote Authentication Dial-In User Service (RADIUS)
	Must support AAA using RADIUS enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration
Management features	Must provide management using 10/100/1000-Mbps management or console ports
	Must have CLI-based console to provide detailed out-of-band management
	Must support RMON, Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3
	Must support AAA, AAA with RBAC, Radius for user authentication
	Must support detail buffer monitoring reports for real-time buffer usage on per port and per queue
	Must support AAA, with CHAP and PAP, DCNM, PTP (IEEE 1588) boundary clock, OHMS, ERSPAN Versions 2 and 3,MS-CHAP, RMON, XML
	Must have Switched Port Analyzer (SPAN) on physical, Port Channel, VLAN
	The switch must have at least Typical heat dissipation of 383 BTUs per hr and Maximum heat dissipation of 727 BTUs per hr
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.

Item Description	Required Specifications
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

8. Technical Specification for DHAKA BRANCH ROUTER

Item Description	Required Specifications
Quality	ISO 9001/9002 for a manufacturer of quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	02 (Three)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
Hardware Architecture	The Router should have minimum 4x1G WAN and 8x1G LAN Port from Day 1. Bidder must provide 2 x 1G Base-T module for each device from day 1. Module must be OEM original.
	The Router should support IPv4 Forwarding Throughput (1400Bytes) minimum 3.8 Gbps, IPsec Throughput (1400Bytes, clear text) minimum 1.0 Gbps in Non-SDWAN mode
	Number of IPsec SVTI Tunnels minimum 2000
	The router should have 400 Mbps aggregate throughput from Day 1 in non-SD-WAN mode
	Router should have 8 GB DRAM from day 1 and can be upgraded to 32 GB for higher scale
	Router should have Flash storage M.2 USB 16GB from day 1 and be upgraded to 32 GB for higher scale
General Features	Number of ACLs per system minimum: 3900
	Number of IPv4 Routes: 1.6M w/ default 8GB, up to 4M w/ 32GB
	Number of IPv6 Routes: 1.5M w/ default 8GB, up to 4M w/ 32GB

General Features	Number of Queues: 15.5K
	Number of NAT Sessions: 1.2M w/ default 8GB, up to 2M w/ 32GB & f Firewall Sessions: 512K
	Number of VRFs: 4000
High availabity & Resilliency	The Router Should have Single Power supply
General & Security Features	Proposed router should be Intel x86 CPU with multiple cores allocated to control plane architecture.
	The router should have Access Control Entries (ACE) feature for security with at least 70K capacity is preferable in a single device or cluster architecture.
	The router should have unique Access Control List (ACL) or unified access control feature for security with at least 3900 capacity is preferable in a single device or cluster architecture.
	Hardware-anchored Secure Boot and Secure Unique Device Identification (SUDI) support
	for Plug and Play to verify the identity of the hardware and software
	The router should support 3DES and AES encryption standards
	Should support Inline hardware-accelerated encryption for high-throughput IPsec and MACsec
	The router should support multiple level of privileges and authentication for user access, along with SSH support for secured device access
Routing Protocol	Should have IPv4, IPv6, static routes, RIP and RIPv2, OSPF, EIGRP, BGP, BGP Router Reflector, IS-IS, IGMPv3, PIM SM, SSM, RSVP, ERSPAN, IPSLA, EEM, IKE, ACL, EVC, DHCP, Frame Relay, DNS, LISP, HSRP, RADIUS, Authentication, Authorization, and Accounting (AAA), AVC, DVMRP, IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPsec, L2TPv3, BFD, IEEE 802.1ag, and IEEE 802.3ah
Security Protocol	Encryption: AES-256 (in CBC and GCM modes), Internet Key Exchange (IKE)
	Authentication: AAA, RSA (2048 bit), ESP-256-CBC, HMAC-SHA1, ECDSA (256/384 bit)
	Integrity: SHA-1, SHA-2
	Built-in end-to-end Segmentation (VPNs), ZBFW, PKI, DNS Layer Security, Security Internet
	Gateway (Umbrella, Zscaler), ALG for ZBFW
High availabity	Software redundancy with dual IOS, Box-to-Box application-level redundancy
Encapsulations	Generic Routing Encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), High-Level Data Link Control (HDLC), and PPP over Ethernet (PPPoE)

Traffic management	Quality of Service (QoS), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Application Recognition (NBAR)
Cryptographic algorithms	Encryption: DES, 3DES, AES-128, or AES-256 (in CBC and GCM modes), Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit), Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512
Management	Support diagnostic commands and system health checks within the Router
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

9. Technical Specification for BRANCH ROUTER FOR

Item Description	Required Specifications
Quality	ISO 9001/9002 for a manufacturer of quality assurance
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	30 (Thirty)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Environment:	Maintain International Quality Environmental Safety standard
	Should have multiple processor/CPU based architecture with the dedicated control plan and service plan

	Should support encrypted traffic min 350 Mbps and should provide traffic performance 50 Mbps or more from day 1
Memory	Minimum 4GB DRAM & minimum 4GB Flash
Interface	2 WAN Port (1 x Copper Gigabit Ethernet and 1 x SFP Gigabit Ethernet) with 8 x 1 GE LAN Port and future upgrade to 4 POE or 2 POE+ with module
Management	1 x console, 1 x USB 2.0 Type A port
	Should support minimum 50 Mbps IPsec performance from day 1 which can be upgrade 200 Mbps if required.
	Should support static routes, RIP and RIPv2, OSPF, BGP, IS-IS, IGMPv3, PIM SM, SSM, RSVP, ACL, AVC and BFD
	Should support LISP, Virtual Private LAN Services (VPLS), L2TPv3, MPLS & Ethernet over MPLS
Network Services	IPv4, DNS, DHCP Client, DHCP Server, DHCP relay, NAT
	IPv4, DNS, DHCP Client, DHCP Server, DHCP relay & AAA
	Should support hardware assisted VPN acceleration for crypto performance in future without any hardware change
Security	Should support DES, 3DES, VPN compliant IPSec, AES-128 or AES-256 for encryption and RSA (748/1024/2048 bit) and ECDSA (256/384 bit) as authentication protocol in future without any hardware change
	Should support PPPoE, Layer 2 Tunneling protocol version 3, Layer 2 and Layer 3 VPN, Ethernet Virtual Connections as well as IKEV2 IPSec based VPN, Crypto VPN, GRE VPN, site-to-site, dynamic multisite hub and-spoke, multisite spoke-and-spoke, remote access software based VPN over IPv4 and IPv6, multicast traffic over the VPN in future without any hardware change
	Should support hardware assisted VPN acceleration for crypto performance
	Should support dynamic failover protocols such as Virtual Router Redundancy Protocol (VRRP, RFC 2338)
Qos	Shaping, Policing, Per-flow queuing, Class-based queuing, Voice/Video/RTP QoS
	Should support modular OS on open platform with programmable and automation feature to support software defined WAN (i.e. link optimization, application visibility/detection, traffic load balancing, performance analysis for routing etc.)
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.

Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

10. Technical Specification for CORE SWITCH FOR

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA/EU
Brand	CISCO
Model	**To be mentioned by the bidder**
Quantity	02 (Two)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
Architecture	The Switch should have 24 x 10/100/1000 Base-T Ports and 4 x 1G SFP Ports
	The switch should support 56Gbps switching capacity and 40 Mpps forwarding rate.
	Switch should have 8GB RAM and 16 GB Flash.
	The switch should support 32K MAC Addresses and 4000 VLAN IDs.
	Switch should have slot/ports (excluding uplinks ports) for minimum 320 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 8 switch in stack
	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.
	Switch should be able to support 3000 IPV4 & 1500 IPV6 routing entries from day-1
	Switch should support minimum 1K Switched Virtual Interfaces.
	The switch should support Jumbo frames of 9216 bytes
	Proposed switch should be enterprise grade switch with x86 based CPU architecture

General Features	Proposed switch should have fixed uplink
	The Switch should support Layer 2 features, Routed Access (RIP, OSPF), Policy Based Routing, PIM Stub Multicast, PVLAN, VRRP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder from day-1
	The proposed switch should be software defined networking capable and be able to atleast integrate easily with the SDN controller from the same OEM.
	Switch shall support application visibility and traffic monitoring with minimum 64K netFlow/sflow/jflow entries.
	Switche should support both front and back beacon LEDs for easy identification of the switch being accessed.
	Switches should have hardware support to connect a Bluetooth dongle to your switch, enabling you to use this wireless interface as an IP management port interface.
High availabity & Resilliency	Switch should support redundant field replacable power supplies
	Proposed Switch must have stacking kit and cable from day-1
	Switch should support redundant field replacable fans.
	Switch should support cross-stack etherchannel.
L2 Features	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
	The switch should support IEEE 802.1Q VLAN encapsulation
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth
	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.

	The switch should support IGMP v1, v2 Snooping
	Switch should support IPv4 and IPv6The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.
	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.
	The switch should support MACSec-128
Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring.
	Support sampled NetFlow/SFlow, Switched Port Analyzer, Remote SPAN, shared NetFlow/SFlow policy, RSPAN and packet capture tool like Wireshark for troubleshooting and network visibility.
	Support Network automation with Open PnP, Containers, Python scripting, NETCONF, RESTCONF using YANG
QoS	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port.
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.

Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

11. Technical Specification for ACCESS SWITCH FOR

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	02 (Two)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch should have 48 x 10/100/1000 Base-T PoE+ Ports and 4 x 1G SFP Ports
	The switch should support at least 104 Gbps switching capacity and 77 Mpps forwarding rate.
	The switch should support at least 52 Gbps forwarding Bandwidth.
	Switch should have 512 MB RAM and 256 MB Flash.
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.
	The Switch should have at least 370W PoE capacity
	Switch should be able to support 500 IPV4 & 400 IPV6 routing entries from day-1
	The switch should support Jumbo frames of minimum 10,000 bytes
Redundancy and resiliency	Should support Switch port automatic recovery due to link failure/fault or network fault
	Switch should support rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances
	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
	The switch should support at least 256 VLANs
	The switch should support IEEE 802.1Q VLAN encapsulation

L2 Features	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
	The switch should support IGMP v1, v2 Snooping
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
	Support Port Security, Dynamic ARP Inspection, and IP Source Guard
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.
	Support Port-based ACLs, VLAN ACLs
	Support IPv6 ACLs
	Support Unicast Reverse Path Forwarding (RPF)
Management features	Support diagnostic commands and system health checks within the switch
	Support Remote Monitoring (RMON) software with four RMON groups (history, statistics, alarms, and events).
	support Layer 2 troubleshoot features
	Support SSHv2, Telnet, console, NTP, DNS, TFTP, DHCP
	Support RMON I and II standards
	Support SNMP v1, v2c, and v3
QoS	Support automatic configuration of QoS
	Support eight egress queues and two thresholds per port, supporting egress bandwidth control, shaping, and priority queuing so that high-priority packets are serviced ahead of other traffic
	Support flexible mechanisms for marking, classifying, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed
	Support congestion avoidance feature like SRR/SRR/similar protocol

	Support 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) classification, with marking and reclassification
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

12. Technical Specification for OTHER BRANCHES

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA/EU
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	02 (Two)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
	Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch should have 24 x 10/100/1000 Base-T PoE+ Ports and 4 x 1G SFP Ports
	The switch should support at least 55 Gbps switching capacity and 40 Mpps forwarding rate.
	The switch should support at least 25 Gbps forwarding Bandwidth.

General Features	Switch should have 512 MB RAM and 256 MB Flash.
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.
	The Switch should have at least 195W PoE capacity
	Switch should be able to support 500 IPV4 & 400 IPV6 routing entries from day-1
	The switch should support Jumbo frames of minimum 10,000 bytes
Redundancy and resiliency	Should support Switch port automatic recovery due to link failure/fault or network fault
	Switch should support rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances
	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
L2 Features	The switch should support at least 256 VLANs
	The switch should support IEEE 802.1Q VLAN encapsulation
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
	The switch should support IGMP v1, v2 Snooping
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
	Support Port Security, Dynamic ARP Inspection, and IP Source Guard
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.
	Support Port-based ACLs, VLAN ACLs
	Support IPv6 ACLs
	Support Unicast Reverse Path Forwarding (RPF)

Management features	Support diagnostic commands and system health checks within the switch
	Support Remote Monitoring (RMON) software with four RMON groups (history, statistics, alarms, and events).
	support Layer 2 troubleshoot features
	Support SSHv2, Telnet, console, NTP, DNS, TFTP, DHCP
	Support RMON I and II standards
	Support SNMP v1, v2c, and v3
QoS	Support automatic configuration of QoS
	Support eight egress queues and two thresholds per port, supporting egress bandwidth control, shaping, and priority queuing so that high-priority packets are serviced ahead of other traffic
	Support flexible mechanisms for marking, classifying, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed
	Support congestion avoidance feature like SRR/SRR/similar protocol
	Support 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) classification, with marking and reclassification
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

13. Technical Specification for OTHER BRANCHES

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA
Brand	CISCO
Model	To be mentioned by the bidder

Quantity	10 (Ten)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch should have 16 x 10/100/1000 Base-T PoE+ Ports and 2 x 1G SFP Ports
	The switch should support at least 32 Gbps switching capacity and 25 Mpps forwarding rate.
	The switch should support at least 15 Gbps forwarding Bandwidth.
	Switch should have 512 MB RAM and 256 MB Flash.
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.
	The Switch should have at least 110 W PoE capacity
	Switch should be able to support 500 IPV4 & 400 IPV6 routing entries from day-1
	The switch should support Jumbo frames of minimum 10,000 bytes
Redundancy and resiliency	Should support Switch port automatic recovery due to link failure/fault or network fault
	Switch should support rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances
	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
L2 Features	The switch should support at least 256 VLANs
	The switch should support IEEE 802.1Q VLAN encapsulation
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth

	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
	The switch should support IGMP v1, v2 Snooping
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
	Support Port Security, Dynamic ARP Inspection, and IP Source Guard
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.
	Support Port-based ACLs, VLAN ACLs
	Support IPv6 ACLs
	Support Unicast Reverse Path Forwarding (RPF)
Management features	Support diagnostic commands and system health checks within the switch
	Support Remote Monitoring (RMON) software with four RMON groups (history, statistics, alarms, and events).
	support Layer 2 troubleshoot features
	Support SSHv2, Telnet, console, NTP, DNS, TFTP, DHCP
	Support RMON I and II standards
	Support SNMP v1, v2c, and v3
QoS	Support automatic configuration of QoS
	Support eight egress queues and two thresholds per port, supporting egress bandwidth control, shaping, and priority queuing so that high-priority packets are serviced ahead of other traffic
	Support flexible mechanisms for marking, classifying, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed
	Support congestion avoidance feature like SRR/SRR/similar protocol
	Support 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) classification, with marking and reclassification
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.

Item Description	Required Specifications
Installation, Testing and Commi	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 Division.
Warranty	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.
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

14. Technical Specification for OTHER BRANCHES

Item Description	Required Specifications
Quality	ISO 9001/9002 for manufacture
Country of Origin	USA
Brand	CISCO
Model	To be mentioned by the bidder
Quantity	04 (Four)
Environmental	Maintain International Quality Environmental Safety standard
Form factor	1U Chassis Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required performance document for the proposed device.Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ in Last Three Years.
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture
	The Switch should have 8 x 10/100/1000 Base-T PoE+ Ports and 2 x 1G SFP Ports
	The switch should support at least 18 Gbps switching capacity and 12 Mpps forwarding rate.
	The switch should support at least 8 Gbps forwarding Bandwidth.
	Switch should have 512 MB RAM and 256 MB Flash.
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.
	The Switch should have at least 65 W PoE capacity
	Switch should be able to support 500 IPV4 & 400 IPV6 routing entries from day-1
	The switch should support Jumbo frames of minimum 10,000 bytes
	Should support Switch port automatic recovery due to link failure/fault or network fault

Redundancy and resiliency	Switch should support rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances
	The switch should support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors
L2 Features	The switch should support at least 256 VLANs
	The switch should support IEEE 802.1Q VLAN encapsulation
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability
	The switch should support Spanning-tree root guard to prevent other edge swicthes becoming the root bridge.
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.
	The switch should support IGMP v1, v2 Snooping
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
	Support Port Security, Dynamic ARP Inspection, and IP Source Guard
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration.
	Support Port-based ACLs, VLAN ACLs
	Support IPv6 ACLs
	Support Unicast Reverse Path Forwarding (RPF)
Management features	Support diagnostic commands and system health checks within the switch
	Support Remote Monitoring (RMON) software with four RMON groups (history, statistics, alarms, and events).
	support Layer 2 troubleshoot features
	Support SSHv2, Telnet, console, NTP, DNS, TFTP, DHCP
	Support RMON I and II standards
	Support SNMP v1, v2c, and v3
	Support automatic configuration of QoS

QoS	Support eight egress queues and two thresholds per port, supporting egress bandwidth control, shaping, and priority queuing so that high-priority packets are serviced ahead of other traffic
	Support flexible mechanisms for marking, classifying, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed
	Support congestion avoidance feature like SRR/SRR/similar protocol
	Support 802.1p class of service (CoS) and Differentiated Services Code Point (DSCP) classification, with marking and reclassification
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer Warranty.
	Bidder must be submitted Manufacturer Authorization Letter (MAL)
	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.
Installation, Testing and Comm	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 Division.
Warranty	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
	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support

Item Description	Technical Specification & Standards
Quality	ISO 9001/9002 for Manufacture
Brand	CISCO
Model	To be mentioned by the bidder
Environmental	Maintain International Quality Environmental Safety Standard
Form factor	Rack Mountable with Rack Mounting Kit
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Manufacture should be Gratner Leader in Year of 2020/2021.
Architecture	The Appliance should have 6 port 1G Base-T copper network interface (NICs), RJ-45
	Security Intelligence
	URL filtering
	Dynamic Content Analysis (DCA)
	HTTPS inspection
	Advanced Malware Protection
	Layer 4 Traffic Monitor

General Features	Cloud-based threat analysis
	Malware Infection
	Data Breach Protection
	Behavioral Analysis
	Anomaly Detection
	Application Visibility and Control (AVC)
	Data Loss Prevention
	Remote Browser Isolation
	Roaming-User Protection
	Centralized Management and Reporting
Manufacturer's warranty	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. OEM should have local office & RMA

Firepower Management Center Hardware Req.	
RAM	32 GB
HDD	320 GB
CPU	8 Core Virtual CPU
VMware Virtual Hardware Ver	VMware vSphere Hypervisor (ESXi)