|| यतो धर्मस्ततो जयः ||

Maharashtra National Law University, Aurangabad

NIT No.: MNLUA/Admin/NIT/2023/02
CORRIGENDUM
Date: 03.06.2023

Due to changes in Technical specifications suggested by our technical expert team, the tender submission date is extended as per following table:

Tender Reference Number	MNLUA/ARC22-23/OFC
Due Date & Time/Submission End Date	09 /06/2023 17:00pm
Tender Opening Date (Technical Bid)	12/06/2023 11.00 am
Name, Address & Contact No. of Tenderer	The Registrar, Maharashtra National Law University, PaithanRoad, Kanchanwadi campus, Aurangabad - 431005
Tender Fee	₹. 17,000 /- (Non-Refundable)
EMD	₹. 5,25,000/-
Website	www.mahatenders.gov.in

All the bidders may note the revised technical specifications are as follows:-

A) PROJECT SCOPE

Sr. No.	ITEM DESCRIPTION		Qty	Amount
1]	Layer3 Core Switch - 24 1/10G Copper + 24 1/10G SFP+ Ports, 960Gbps Throughput, Stackable Managed Layer3 Switch *(Preferred Make : Cisco /Juniper / Netgear)* **Technical Specifications**		01	
	1.1) Physical Interfaces	24 # 1/10G Base-T Copper Ports (Dedicated)		
		24 # 1/10G Base-X Fiber SFP Ports (Dedicated)		
		Ethernet: Out-of-band 1G port (Front)		
		Console: RJ45 RS232 (Front)		
		Console: Mini-USB (Front)		
		Storage: USB (Front)		
		Full-width 1-unit 1U rack mount		
		2 PSUs in RPS mode		
	1.2)CPU/ Memory	CPU: 800 MHz		
		RAM: 1 GB		
		Packet buffer memory: 56 MB		
		Flash: 256 MB		

1.3)Performance	Stack height: 8 switches	
	Mixed Stacking on 10G & 1G models	
	Non-Stop Forwarding Failover	
	Switching fabric: 960 Gbps Line-Rate (non blocking fabric)	
	Throughput: 714 Mpps	
	Forwarding mode: Store-and-forward	
	Address database size: 128K MAC addresses (48-bit MAC address)	
	Number of VLANs: 4,093 (IEEE 802.1Q) simultaneously	
	Number of multicast groups= 2K IPv4	
	Number of multicast groups= 2K IPv6	
	ARP/NDP= 8K	
	Number of LAGs (802.3ad): 128 LAGs with up to 8 ports per group	
	Number of hardware queues for QoS: 8 (Standalone)	
	Number of routes: 12K IPv4 Unicast routes	
	Number of routes: 4K IPv6 Unicast routes	
	Jumbo frame support: up to 9KB packet size	
	Mean time between failures (MTBF): 133,000 hours or more	
	sFlow=416 samplers, 416 pollers, 8 receivers	
1.4) L2 Services	Protocol based VLAN	
	IP Subnet	
	IPX	
	ARP	
	Subnet based VLAN	
	MAC based VLAN	
	Voice VLAN	
	Private Edge VLAN	
	Private VLAN	
	Guest VLAN	
	Double VLAN Tagging (QoQ)	
	GARP with GVRP/GMRP	
	MVR (Multicast VLAN Registration)	
	Multiple Registration Protocol (MRP)	
	Multicast VLAN Registration Protocol (MVRP)	
	LAG Hashing	
	LAG Member Port Flaps Tracking	
	UDLD support	
	Distributed Link Aggregation	
	Storm Control	
	Link Dependency	
	Spanning Tree Protocol	
	Per VLAN STP (PVSTP) with Fast Uplink and Fast Backbone	
	Per VLAN Rapid STP (PVRSTP)	

		STP Loop Guard		
		STP Root Guard		
		BPDU Guard		
		STP BPDU Filtering		
		STP BPDU Flooding		
		IGMP v2/v3 Snooping support		
		MLD v1/v2 Snooping support		
		Expedited Leave Function		
		Static L2 Multicast Filtering		
		MLDv1/2 Snooping Support		
		IGMPv2/3 Snooping Support		
	1.5) L3 Services	IGMP Proxy		
		Policy based routing		
		MLD Proxy		
		Any Source Multicast (ASM)		
		Source Specific Multicast (SSM)		
		Multicast streams routing between subnets, VLANs		
		Multicast Static Routes (IPv4, IPv6)		
		DVMRP		
		Neighbor discovery (IPv4, IPv6)		
		PIM-DM (IPv4, IPv6)		
		PIM-SM (IPv4, IPv6)		
		PIM multi-hop RP support		
		IPMC replication (hardware support)		
		DHCP Client (IPv4, IPv6)		
		DHCP Server (IPv4, IPv6)		
		DHCP Snooping (IPv4, IPv6)		
		DHCP/ BootP Relay (IPv4, IPv6)		
		DHCP options 66, 67, 150, and 55, 125		
		Static Routing (IPv4, IPv6)		
		Port based Routing		
		ECMP Static Routing		
		Port Based Routing		
		VLAN Routing		
		RIP v1 and v2		
		OSPF v2 and v3		
		OSPF Flood Blocking		
		Route Redistribution		
		VRRP		
		VRRP Route/Interface Tracking		
		Loopback Interfaces		
		Tunnel interfaces		
		Router Discovery		
		IP Helper		
		IP Source Guard		
		IP Event Dampening		
		ECMP		
		Proxy ARP		
		Multinet ting		
		ICMP v4 and v6		
		IPv4/IPv6		
		DNS v4 and v6		
		IPv6 Routing		

	Configured v6-over-v4 tunnels	
	Automatic (6to4) tunnels	
1.6) QoS	IEEE 802.1p CoS	
	DiffServQoS	
	WRED (Weighted Deficit Round Robin)	
	Single Rate Policing	
	Strict Priority queue technology	
	Auto-VoIP	
	iSCSI Flow Acceleration	
	IP DSCP	
	IP Precedence	
	IP TOS	
	L3 IPv6 Flow Label	
	Interface Traffic Shaping	
	PHB Support	
	Minimum Bandwidth per-interface	
1.7) Security	Broadcast, Multicast and Unicast Network Storm Protection	
	CPU Protection	
	DoS attack protection	
	ICMP throttling	
	Management ACL	
	Radius accounting	
	TACACS+	
	L2/L3/L4 Access Control List (ACL)	
	MAC, IPv4, IPv6, TCP, UDP ACL	
	Protocol based ACL	
	ACL over VLAN	
	Dynamic ACL	
	IEEE 802.1x Radius Port Access Authentication	
	802.1x MAC Address Authentication Bypass (MAB)	
	Port Security	
	Dynamic ARP Inspection	
	MAC Filtering	
	Port MAC Locking	
1.8) IEEE Network Protocols	IEEE 802.3 10Base-T	
	IEEE 802.3 Ethernet	
	IEEE 802.3i 10BASE-T	
	IEEE 802.3u 100BASE-T	
	IEEE 802.3ab 1000BASE-T	
	IEEE 802.3z Gigabit Ethernet 1000BASE-SX/LX	
	IEEE 802.3ae 10-Gigabit Ethernet	
	IEEE 802.3ad Trunking (LACP)	
	IEEE 802.1AB LLDP with ANSI/TIA-1057 (LLDP-MED)	
	IEEE 802.1D Spanning Tree (STP)	
	IEEE 802.1s Multiple Spanning Tree (MSTP)	
	IEEE 802.1w Rapid Spanning Tree	

		(RSTP)		
		IEEE 802.1p Quality of Service		
		IEEE 802.1Q VLAN tagging		
		IEEE 802.1v protocol-based VLAN		
		IEEE 802.1X Radius Network Access Control		
		IEEE 802.3x flow control		
		GMRP — Dynamic L2 multicast registration		
		GVRP — Dynamic VLAN registration		
		GARP -Generic Attribute Registration Protocol		
	1.9) Management	ISDP (Industry Standard Discovery Protocol)		
		Out of band Management		
		802.1ab LLDP and LLDP-MED		
		SNMP v1, v2 and v3		
		RMON 1, 2, 3, 9		
		sFlow		
		Command Line Interface (CLI)		
		Web-based graphical user interface (GUI)		
		Admin access control via Radius and TACACS+		
		Telnet		
		Dual Software (Firmware) images		
		Dual Configurations file (Text-based)		
		Radius accounting		
		Malicious Code Detection		
		SNTP		
		XMODEM		
		Port Mirroring		
		Cable Test Utility		
		SSH v1/v2		
		SSL/HTTPS and TLS v1.0 for web-based access		
		File Transfer (uploads, downloads) through TFTP/HTTP		
		SCP/ SFTP/ HTTPS		
		Syslog		
		Non disruptive Config Management		
		Remote Port Mirroring (RSPAN)		
		Persistent log supported		
	1.10)Network Traffic	Access Control Lists (ACLs) L2 / L3 / L4		
		Time-based ACLs		
		ACL over VLANs		
		IPv6 RA Guard Stateless Mode		
		Network Authentication Successive Tiering		
		802.1x MAC Address Authentication Bypass (MAB)		
	1.11) LED	Per port: Speed, link, activity		

	Power, Fan, Stack Master, Stack ID	
	Cooling front to back	
1.12) **Environmental**	Operating Temperature: 32° to 122°F (0° to 50°C)	
	Operating Humidity: 90% maximum relative humidity, non-condensing	
	Storage Temperature: – 4° to 158°F (– 20° to 70°C)	
	Storage Humidity: 95% maximum relative humidity, non-condensing	
1.13)Certifications	CE mark, commercial	
	FCC Part 15 Class A, VCCI Class A	
	Class A EN 55022 (CISPR 22) Class A	
	Class A C-Tick	
	EN 50082-1	
	EN 55024	
	CSA certified (CSA 22.2 #950)	
	UL listed (UL 1950)/cUL IEC 950/EN 60950	
1.14)Warranty	True Lifetime Hardware replacement warranty	
	Lifetime free latest firmware support	
	Replacement with New Product Only No refurbished Products.	

2]	**L3- Network Switch** 24-Port 1/10G SFP+ **Managed Switch** **with480Gbps Throughput**(Preferred Make : Cisco /Juniper /Netgear)	**3**
	Technical Specifications : 24-Port 1/10G SFP+ Managed Switch with480Gbps Throughput	

3]	**L2- NETWORK Switch** (Preferred Make : Cisco/ Juniper /Netgear)	**52**

Technical Specifications :(24-port 10/100/1000 Base-T Gigabit PoE+ Managed Switch)	
3.1) Physical Specifications	24 # 10/100/1000 Base-T auto-sensing PoE+ ports
	2 dedicated 100/1000 Base-X Fiber SFP ports
3.2) Performance Specification	CPU: 800MHz single core, 512MB DDR RAM, 2MB SPI NOR, 128MB FLASH
	Bandwidth: 52 Gbps non-blocking
	Mean Time Between Failures (MTBF): 1,328,429 hrs (152 yrs)
	Heat Dissipation (worst case, all ports used, full PoE, line-rate traffic) (BTU/hr):- Max: 784.88 BTU/hr
	Forwarding modes: Store-and-forward
	4 Priority queues
	Weighted Round Robin (WRR) and Strict Priority
	MAC Address database size: 16,000 media access control (MAC) addresses

		VLAN: 64		
		512 Multicast groups		
		Number of DHCP snooping bindings: 8K		
		Access Control Lists (ACLs): 100 shared for MAC (ingress)		
		Packet forwarding rate (64 byte packet size) (Mpps) : 38.6		
		Jumbo frame support: Up to 9K packet size		
		Packet buffer memory (Dynamically shared across only used ports): 0.5 MB		
		1G Copper Latency (64-byte packets): 3.734µs		
		1G Fiber Latency (64-byte packets): 2.896µs		
		Max power (worst case, all ports used, full PoE, line-rate traffic) (Watts): 229.9W		
		PoE budget: 190W		
3.3) IEEE Network Protocols		IEEE 802.3 Ethernet		
		IEEE 802.3u 100BASE-T		
		IEEE 802.1Q VLAN Tagging		
		IEEE 802.3ab 1000BASE-T		
		IEEE 802.3af PoE		
		IEEE 802.3at PoE+		
		IEEE 802.3az Energy Efficient Ethernet (EEE)		
		IEEE 802.3ad Trunking (LACP)		
		IEEE 802.3z Gigabit Ethernet 1000BASE-SX/LX		
		IEEE 802.3x Full-Duplex Flow Control		
		IEEE 802.1AB LLDP with ANSI/TIA-1057 (LLDP-MED)		
		IEEE 802.1p Class of Service		
		IEEE 802.1D Spanning Tree (STP)		
		IEEE 802.1s Multiple Spanning Tree (MSTP)		
		IEEE 802.1w Rapid Spanning Tree (RSTP)		
		IEEE 802.1X Radius network access control		
3.4) Network Security and Traffic		IEEE 802.1x		
		Guest VLAN		
		RADIUS-based VLAN assignment via .1x		
		RADIUS accounting		
		Network Storm Protection		
		DoS attacks prevention		
		Broadcast, Unicast, Multicast Protection		
		Access Control Lists (ACLs) L2 / L3 / L4		
		IP-based ACLs (IPv4)		
		MAC-based ACL		
		TCP/UDP-based ACL		
		MAC lockdown		
		MAC lockdown by the number of MACs		
		IEEE 802.1x Radius Port Access Authentication		
		Control MAC # Static entries: 48		
		IEEE 802.1Q VLAN Tagging		
3.5) L2 Services		Video VLAN		
		Voice VLAN		
		IEEE 802.3ad - LAGs - LACP (8 LAGS with max. of 8 members in each LAG)		
		Broadcast Storm Control		
		IGMP Snooping (v1, v2 and v3)		
		IGMP Snooping queriers		
3.6) Network		802.1ab LLDP		
		SNMP V1, V2, V3		

Monitoring and Discovery Services	RMON 1,2,3,9	
3.7) Quality of Service (QoS)	Port-based rate limiting: Egress	
	Port-based QoS	
	DiffServQoS	
	IEEE 802.1p COS	
	IPv4 DSCP	
	IPv4 ToS	
3.8)Management	Password management	
	Configurable Management VLAN	
	Admin access control via Radius and TACACS+	
	Web-based graphical user interface (GUI)	
	Dual Software (firmware) image	
	SNTP client over UDP port 123	
	SNMP v1/v2	
	SNMP v3 with multiple IP addresses	
	RMON 1,2,3,9	
	Port Mirroring	
	Many to One Port Mirroring	
	Cable Test utility	
	SSL/HTTPS and TLS v1.2 for web-based access	
	TFTP/HTTP File transfers (uploads, downloads)	
	HTTP Download (firmware)	
	Syslog (RFC 3164)	
3.9) LEDs	Per port: Speed, Link, Activity	
	Per device: Power, Fan, PoE Max	
3.10) Environmental Conditions	Operating Temperature: 0° to 45° C (32° to 113° F)	
	Operating Humidity: 95% maximum relative humidity, non-condensing	
	Storage Temperature: – 4° to 158°F (–20° to 70°C)	
	Storage Humidity: 95% maximum relative humidity, non-condensing	
	Operating Altitude : 10,000ft (3,000m) maximum	
3.11) Certifications	CE mark, commercial	
	FCC Part 15 Class A, VCCI Class A	
	Class A EN 55022 (CISPR 22) Class A	
	Class A C-Tick	
	EN 50082-1	
	47 CFR FCC Part 15, SubpartB, Class A	
	CCC	
3.12) Safety	UL listed (UL 1950)/cUL IEC 950/EN 60950	
	CB report / certificate IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013	
	CE LVD: EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013	
	BSMI: CNS 14336-1	
3.13) Warranty and Support	5 Years hardware replacement warranty	
	Replacement with New Product Only No refurbished Products.	

4)	**Single Mode 1G SFP MODULE**		110	
	Technical Specifications			
	4.1) SFP Module	1000Base-LX Fiber SFP		
		LC duplex connector		
		1310 nm, for distances up to 10 km		
		Single Mode Fiber		
		ROHS Compliant		
		Compliant with SFP Transceiver MSA specification		
		Compliant with Specifications for IEEE 802.3z/Gigabit Ethernet		
		Compliant with Industry Standard RFT Electrical Connector and Cage		
		Single + 3.3V Power Supply and TTL Logic Interface		
		EEPROM with Serial ID Functionality		
		Laser Class 1 Product which comply with the		
		requirements of IEC 60825-1 and IEC 60825-2		
	4.2) Warranty and Support	5 Years Hardware Replacement Warranty		
		Replacement with New Product Only No refurbished Products.		

5)	**Single Mode 10G SFP+ Module**		08	
	Technical Specifications			
	5.1) SFP+ Module	10GBase-LR Fiber SFP+		
		LC duplex connector		
		1310nm Wavelength		
		2m - 10km for 9/125 um SMF		
		Single Mode Fiber		
		ROHS Compliant		
		Compliant with SFP+ Transceiver MSA specification		
		Compliant with Specifications for IEEE 802.3ae 10-Gigabit Ethernet Over Fiber		
		Compliant with Industry Standard RFT Electrical Connector and Cage		
		Operating Temperature 32 -158° F (0 - 70°C)		
		MTBF 4,986,536 hr (569 years)		
		Power Consumption <1.5w		
		UL 1950 CSA 22.2 No. 950		
	5.2) Warranty and Support	5 Years Hardware replacement warranty		
		Replacement with New Product Only. No refurbished Products.		

6)	**Dual Band WiFi Access Point** (Preferred Make : Cisco/ Juniper /Netgear)		**183**	
	Technical Specifications (2 x 2 Dual Band Wireless-AX Wave2 Access Point)			
	6.1) Physical Interfaces	One 100/1000/2.5GBASE-T Gigabit Ethernet (RJ-45) ports with Auto Uplink (Auto MDI-X) supporting IEEE 802.3af or 802.3at Power over Ethernet (PoE)		
		Two (2) Internal 2.9/2.8dBi (2.4GHz/5GHz) antenna		
		Four (4) LED: Power and Cloud connection; LAN speed; 2.4GHz status; 5.0GHz status		
		Power adapter (not included): 12V DC, 2.5A		
	6.2) Standards	5.0GHz: 802.11a/n/ac/ax; 2.4GHz: 802.11b/g/n/ax		
		IEEE 802.11ax WIFI 6 standard		
		WMM - Wireless Multimedia Prioritization		
		WDS- Wireless Distribution System		
		Power over Ethernet (PoE) IEEE 802.3af/802.3at		
	6.3) Security	Wi-Fi Protected Access (WPA, WPA2, WPA3), 802.11i		
		WPA2 Enterprise		
		Wireless access control to identify authorized wireless network devices		
		MAC address filtering with access control		
		802.1x RADIUS support with EAP TLS, TTLS, PEAP		
		Neighbor AP detection		
		VLAN Support		
		Secure Socket Layer (SSL)		
		Guest Network/Captive Portal		
		Bandwidth management		
		Link Layer Discovery Protocol		
	6.4) Network Management	Cloud based App Management for setup, monitoring and management from anywhere anytime (Remote configuration and management)		
		Easy-to-use Web browser-based management GUI		
	6.5) Manageability	As standalone		
		Centralized Management through Mobile Application		
	6.6) Advanced Wireless Features	Wireless Distribution System (WDS)		
		Bridge mode: Point-to-point wireless WDS mode		
		Bridge mode: Point-to-multipoint wireless WDS mode		
		Repeater mode		
		Adjustable Transmit Power Control (TPC)		
		Wireless backhaul to form Mesh Network		
		Device detection		
		Identify type of wireless clients in the network		

6.7) Other Specifications	PoE power consumption: 21.2W			
	Business class WiFi based on next generation 802.11ax WiFi 6 technology on both 5.0GHz and 2.4GHz bands. Backward compatible to 802.11b/g/n/a/ac			
	Dual band 2x2 (2.4GHz and 5.0GHz) 4 streams of data for an aggregate throughput of up to 3Gbps			
	Theoretical Throughput per Band: 5.0GHz: 2400Mbps, 2.4GHz: 600Mbps			
	Orthogonal Frequency Division Multiple Access (OFDMA)			
	Multi-Gigabit Support			
	Target Wake Time (TWT)			
	Basic Service Set Coloring (BSS Coloring)			
	Bandsteering			
	Block SSID Broadcast			
	Ceiling mounting / Wall mounting			
	Bidir and MU-MIMO support			
6.8) Warranty and Support	5 Years Hardware Replacement Warranty	**183**		
	5 Years Centralized Management license must be included			
	5 Years free latest firmware support			
	Replacement with New Product Only. NoRefurbished Products.			

7] **Firewall (**Preferred make: Checkpoint / Fortinet / Cisco/Sophos). **01**

Feature set		
7.1)	**General Requirement**	
7.1.1)	Must have a 64-bit hardware platform & based on Multi-Core Architecture with Optimization for excellent throughput for all your key processes	
7.1.2)	The Proposed solution should have option for visibility into encrypted traffic flows, support for TLS 1.3 without downgrading the performance.	
7.1.3)	The device should be having security functions like Firewall, VPN (IPsec Site to Site &SSL Client VPN), Gateway level antivirus, Category based web and application filtering, Intrusion prevention system, Traffic shaping, DoS/DDoS, WAF, Anti-Spam.	
7.1.4)	Solution should offer with Central management solution with option to manage multiple firewalls from day one.	
7.1.5)	Solution should support Multiple WAN link balancing multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules, should support more than two ISP	
7.2)	**Hardware & Performance Requirement**	
7.2.1)	The appliance should support 8 x GbE copper ports, 2 X SFP fiber ports from day one and should support 4 x 10GE SFP+ fiber ports for future extension.	
7.2.2)	Appliance should have external redundant PSU option	
7.2.3)	Should support SSD storage of min 1 x 120 Gb SATA-III	

7.2.4)	Firewall must support at least 6.5 million concurrent connections	
7.2.5)	Firewall must support at least 1,48,000 new sessions per second processing.	
7.2.6)	Firewall should support up to 20 Gbps of Firewall IMIX throughput.	
7.2.7)	Firewall should support integrated IPS throughputs of minimum 7 Gbps.	
7.2.8)	Firewall should have a minimum Firewall throughput of 35 Gbps.	
7.2.9)	Firewall should have a minimum Threat Protection throughput 1.4 Gbps.	
7.2.10)	Firewall should have a minimum NGFW throughput of 6.3 Gbps.	
7.3)	**General Features**	
7.3.1)	Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type	
7.3.2)	Firewall should be able to filter traffic even if the packets are fragmented.	
7.3.3)	All known internet-based applications should be supported for filtering; like Telnet, FTP, SMTP, HTTP, DNS, ICMP, DHCP, ARP, etc.	
7.3.4)	Firewall should support SSL inspection over HTTPS	
7.3.5)	Firewall should support CLI and GUI based access to the firewall modules.	
7.3.6)	Firewall should have application-based and user-based logs.	
7.3.7)	Should support Local authentication and integration with third party authentication solutions like, Active Directory, LDAP Server, RADIUS, TACACS+, eDirectory and Kerberos	
7.4)	**Security**	
7.4.1)	Protects HTTP, HTTPS, FTP, POP3, POP3S, IMAP, IMAPS, SMTPS and SMTP.	
7.4.2)	Pattern-based spyware blocking at the gateway.	
7.4.3)	Centralized, daily updates, automatic and manual updates or offline update.	
7.4.4)	Advance Threat Protection should have Inst ant identification and immediate	
7.4.5)	response to today's most sophisticated attacks. Multi - layered protection identifies threats instantly	
7.4.6)	Should support Sandboxing Inspects executables and documents containing executable content like - Windows executables (including .exe, .com, and .dll) - Word documents (including .doc, .docx, docm and .rtf) - PDF documents - Archives containing any of the file types listed above (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)	
7.4.7)	The proposed solution should have an option to enable features like Web Application Firewall and Email Protection if needed in future	
7.5)	**Web Filtering**	
7.5.1	Firewall should support minimum of at least 70+ predefined categories.	
7.5.2	Should have flexibility to create network, user, Web and app-based traffic shaping (QoS) policy.	
7.5.3	Blacklist and White listing based on IPs and URLs.	
7.5.4	Exceptions based on network objects defined.	
7.5.5	Notification of custom messages or URL redirection.	

7.6)	**Intrusion Prevention System**			
7.6.1)	IPS should protect for 5000+ Signatures database.			
7.6.2)	Firewall should block attacks such as DoS- SYN, IP/ICMP/TCP/UDP related attacks.			
7.6.3)	Solution should have IPS deep packet inspection engine with an option to select			
7.6.4)	IPS patterns which can ne applied firewall rule for better protection and should have option to create custom signature			
7.6.5)	Firewall should block attacks such as DNS cache poisoning, FTP bounce, improper commands.			
7.7)	**Application Control**			
7.7.1)	Firewall should have feature to identify, allow, block or limit usage of applications beyond ports and protocols.			
7.7.2)	Firewall should provide protection against Block potentially unwanted Applications			
7.7.3)	Application signature database of 25000+ Applications for Application Control			
7.8)	**API Support**			
7.8.1)	The solution Should support API for 3rd party integration			
7.8.2)	The API has option to add, update, or delete configurations.			
7.8.3)	The API should have option to add or update policies for IPS, Web filter, Application filter			
7.8.4)	The solution API should have option to Manage physical interfaces and view Port wise Network and Zone details			
7.8.5)	The Solution API should have option to update Gateway details. routes traffic between networks.			
7.8.6)	The Solution API should have option to add or delete route			
7.9)	**Logging & Reporting**			
7.9.1)	Firewall logs must contain information about the firewall policy rule that triggered the log			
7.9.2)	Firewall must provide at a minimum basic statistic about the health of the firewall and the amount of traffic traversing the firewall.			
7.9.3)	Firewall should have support to log (in detail) all connections which are blocked or pass through the firewall.			
7.9.4)	Firewall should have support to generate performance statistics on real-time basis.			
7.9.5)	Firewall should have the capability to produce report s which measure usage.			
7.9.6)	Should Support 1000+ drilled down reports on the appliance			
7.9.7)	The solution should support User Threat Quotient to identify risky users based on recent browsing behaviour and ATP triggers			
7.10)	**OEM Criteria**			
7.10.1)	Proposed solution should have presence in Gartner's Magic Quadrant for Network Firewalls in latest reports			
7.10.2)	Should have ISO 9001:2015 or above certificate			
7.10.3)	Firewall operating system family should be EAL4+ certified from Common Criteria or under Indian Common Criteria Certification Scheme			
7.10.4)	Should have IPv6 Ready Logo/certified (Please submit proof in BID)			

	7.11)	**3 Year Lic.**	**01**
	7.11.1	Three Year Subscription license for Firewall, Advanced Threat Protection (ATP), Intrusion Prevention System (IPS), Zero-Day Protection, Anti-malware, Web and App visibility control, and protection, 24x7 support, security and software updates. License period will be counted after activation.	
8]	**Passive Components**		
	8.1) Technical Specifications:	Single Mode OFC LC-SC Patch cords 3 Mtr	**220**
	8.2)	Firewall, Layer3 & Layer2 PoE Switches and Access Points installation and Configurations charges	**01**

Note:-

1) It will be supplier's responsibility to integrate with our existing network. The management of all Access Points & Switches (existing & new) should be from single console.

2) MNLUA reserved all right to select / reject the product / equipment.

3) University shall seek an assistance of an IT Expert to scrutinize the bidders.

4) Mere L1 is not sufficient to claim the tender. The IT Expert report on overall parameters especially systems integration over the existing network of the University should be taken into consideration while finalizing.

Registrar
Maharashtra National Law University
Aurangabad - 431 005