INDIRA GANDHI INSTITUTEOFTECHNOLOGY
SARANG, DHENKANAL (ODISHA)-759 146
(An Autonomous Institute of Govt. of Odisha)

No.IGIT/CSE/ 632 **Date:-** 14/11/2023

NOTICEINVITINGTENDER

Subject: Tender for procurement and installation of Next-Generation Firewall, core switch and POE Switches ,IGIT, Sarang

Bid Opening Venue: Department of CSEA,IGIT Sarang

For and on behalf of IGIT Sarang, sealed Tenders are invited from eligible reputed OEM (Original Equipment Manufacturer)/ Authorized Distributor /Dealer having valid GST registration/PAN/TIN clearance for supply and **installation of Next-Generation Firewall, core switch and POE switches for** I.G.I.T. Sarang, Dhenkanal. The interested Authorized Distributor / Dealer / supplier / GEM registered vendors may collect details list of specifications and other related documents which are available in the office and our website www.igitsarang.ac.in.

N.B. If desired, party may also visit to enquire regarding the items in department office during working hours (old academic block first floor)

The detail tender completed in all aspect may be submitted in sealed envelope in the office of the **Director, (Special attention to Internet Administrator) I.G.I.T. Sarang, Dist. – Dhenkanal – 759146 (Odisha) by Speed Post / Registered Post only** under strong sealed cover marked as "**TENDER FOR THE SUPPLY AND INSTALLATION OF Next-Generation Firewall, core switch and POE switches for IGIT,Sarang**".

Important Dates & Time.

S.No.	Particulars	Important Dates	Time
1	Last date & time for submission of tender	15/12/2023	4.00PM.
2	Date & time of opening of Technical Bid and sample verification by committee members	19/12/2023	11.00A.M.
3	Date & time of opening of Financial Bid	20/12/2023	11.00 A.M.

Supply and installation for procurement of Next-Generation Firewall and POE switch. (Annexure – III)

Sl. No.	Items	Qty.	EMD(Rs)	Tender fee (Non refundable in Rs)
1	Item No 1 (refer **Annexure – III**)	For quantity , refer **Annexure III**	1,72,000	10000

14/11/2023
DIRECTOR

INDIRA GANDHI INSTITUTEOFTECHNOLOGY
SARANG,DHENKANAL(ODISHA)-759 146

(An Autonomous Institute of Govt. of Odisha)

(Refer to tender notice no IGIT/ /dt. _____ ,which was published in newspaper and institute website)

1. Scope of Work:

The scope of work under this tender is as follows.

i) **Tender for procurement and installation of Next-Generation Firewall, core swich and POE switches ,IGIT, Sarang**, (Old Academic Block)at designated place as specified in the list placed at **Annexure-III and Annexure - II**. IGIT can increase order the quantity of supply, subject to actual requirement. In the case of unavoidable circumstances, the Institute can also place a repeat order to the successful bidder, at its discretion within 180 days from the date of original Purchase Order.

ii) Supply of items: The supply of items shall be made to this Institute within 30-60days (depending on volume of order) from the issue of purchase order. Accordingly a supply agreement is to be made with the party.

iii)The quantity may vary according to the requirement.

iv) The tenderer should quote the rate including all taxes F.O.R. IGIT SARANG **Tender for procurement and installation of Next-Generation Firewall, core switch and POE switches, IGIT, Sarang**,(Old Academic Block Internet Administrator room).

v) The firm is supposed to confirm regarding supply of items after getting the PO / at the time of submission of tender.

vi) The said tender will be awarded on the basis of overall lowest rate, verification of sample as per our required specification of item.

2. Eligibility Criteria

The tenderers must fulfill the following eligibility criteria:-

i) The supplier MUST be an established and reputed Manufacturer or Authorized Distributor / System Integrator of the OEM of the offered product. The supplier must submit authorization specific to this particular tender in the tender document, which will be verified from the concerned Account Manager of the OEM during technical evaluation. Supply of items mentioned in annexure III. Copies of proof may be attached.

ii) The vendor MUST have good knowledge and experience of providing Items mention in Annexure III. Copy of work orders(similar work order)/client certificates required.(Performance Report of last three years i.e 2020-2021,2021-2022 and 2022-2023 is required).

iii) The bidder MUST have G S T Registration ,valid PAN, and valid TIN, with his clearance as applicable in their case and MUST submit with upto date returns a copy of each of these documents along with acknowledgement copies of the IT Returns for the last 3 year.

iv) The manufacturer /supplier or their product has not been blacklisted by the government / Government Agency / Defence / Financial Institutions in past both in India and abroad. There shouldn't be any past / ongoing legal trial in name of any of the directors / Partners / Proprietor. **A self-declaration letter on the company letter head to be furnished with the tender document for the above**.

v) The tenderers should have minimum three similar completed work orders during last three years in any of the Central and State Govt. Depts. / Public Sector undertaking only / Reputed Private Educational Institutions/university/Organizations. Proof to this effect to be attached with Technical Bid.

Similar work order means providing, installing and commissioning of items as mentioned in annexure III. **The bidders are required to quote rates in all items mentioned at page number 16 to 20. Separate item wise bid is not allowed.**

Work Order copies/client certificates required.

vi) No subletting of work will be allowed at any stage.

vii)The average annual turnover of the bidder should be 3cr for last 3 consecutive financial years.

3. Bidding Procedure(Two Bid System)

Bidding Application must be accompanied by the following:-

Technical Bid on the Tender document appearing at Annexure duly filled in & signed and stamped on every page along with following documents.

i) Tender Fee (non-refundable) and EMD (refundable)are payable only in the form of Bank Draft from any Nationalized bank, in favour of **Principal, IGIT, Sarang payable at SBI, IGIT Sarang. (IFSCCODE : SBIN0010246)**. Cheque/Bank Guarantee/Cash are not accepted, if so in the tenders will not be acceptable.

ii) Proof of Permanent address of the Firm/Agency/Person/Vendor etc.

iii) A complete list of clients including clients (along with quantity and year of sale) from Govt./ Semi Govt./ Autonomous Bodies/ PSUs/ Institutions/university served during last three years with Name, Telephone No, etc along with copies of supply order,

iv) Details of Bank Account of Bidder i.e. Account No .,IFSC Code ,MICR No., Bank Name and address,

v) Copies of Income Tax Return of last 3 year,

vi) Details of GST/PAN/TAN/TIN/Service Tax, Registration number, EPF & ESI Registration, Contract Labour Registration ,if any as applicable.

vii) An authorization letter from the firm in favour of the person signing the tender documents.

viii) A self-attested copy of the certificate of registration/ incorporation pertaining to the legal status of the Bidder/Firm/Agency, should be submitted in the tender document.

ix) Tender document with all the Annexures duly **signed and stamped** on each page as acceptance of the terms and conditional aid down by IGIT authority.

x) Copies of Balance Sheet & turn over Profit/Loss account for the last Three year,

xi) An undertaking to the effect that the Agency/Firm has not been black listed in India and Abroad. There shouldn't be any past / ongoing legal trial in name of any of the directors / Partners / Proprietor.

xii) a) The EMD of successful bidder will be retained until the submission of Performance Security as security deposit. Performance Security fee will be 2% of purchases order value.

b) The DD of EMD of unsuccessful/invalid bidder will be returned to the bidder or his representative on the same day.

xiii) The EMD of the unsuccessful bidder will be returned to them immediate after finalization of tender or latest on or before the 30 day after the award of the contract without interest.

xiv) Separate sealed envelopes, containing Technical Bid, Financial Bids, EMD and Tender Fee super-scribed accordingly and these sealed envelopes be put in a bigger sealed envelope and duly **super-scribed** in block letters as shown below. Technical and Financial Bids should be submitted separately. Technical Bids **For procurement and installation of Next-Generation Firewall, core swich and POE switches ,IGIT, Sarang** should be duly sealed and super scribed **"Technical bid for procurement and installation of Next-Generation Firewall, core switch and POE switches ,IGIT, Sarang".** Financial bid for **procurement and installation of Next-Generation Firewall, core switch and POE switches ,IGIT, Sarang** should be duly sealed and super-scribed **"Financial Bid for procurement and installation of Next-Generation Firewall, core switch and POE switches ,IGIT, Sarang"** and sealed in separate envelope and all the envelopes should be kept in a big envelope super scribing **"Tender for procurement and installation of Next-Generation Firewall, core switch and POE switches ,IGIT, Sarang ",** should be submitted. The tenderer is required to submit Five year on site Guaranty i.e. to replace the damaged equipments during the guarantee period or repair.

The tender not submitted in the prescribed formats or in complete in any respect is liable for rejection. IGIT is not responsible for non-receipt of tender within the specified date and time due to any reasons, including postal holidays or delays.

The tender addressed to the **"Director (Attention- Internet Administrator) I.G.I.T, SARANG-759146, DIST: DHENKANAL, ODISHA,** should reach on **or before dt.15-12-2023 (4.00 PM)**.The authority is not responsible for non-receipt of tender on or before the schedule date due to the postal delay or any other reason. Tenders should be submitted through **Registered/Speed post only**.

xv)EMD/Tender Fee exemptions and price preference are applicable as per the authentic certificate holders. If the firm claiming EMD/Tender Fee exemptions, the firm should have to submit the supporting documents like NSIC registration certificate, MSME registration certificate issued by competent Govt. bodies to become eligible for the above exemption .Also the certificate(NSIC)/MSME shall cover the items tendered to get EMD/Tender fee exemptions. NSIC certificate shall be valid as on due date / extended due date of the tender. This is not applicable to non NSIC/MSME unit.

4. Evaluation Procedure

The eligibility of bidders and their technical bid will be evaluated by the Committee on the basis of documents submitted by the bidders with the Technical Bid. The Financial Bids will only be considered of those bidders who are qualify at the technical bid of the eligibility criteria and other terms and conditions lay in the tender. The work will be awarded to the **lowest bidders on over all basis including sample verification**.

The lowest bidder with qualified sample is to be retained in the institution and other sample (though qualified in technical bid, but not in lowest price) to be taken back by the vender. In this regard the decision of authority shall be final for Annexures I ,II and III.

5. General Term & Conditions

i)In case, after Pre-bid meeting(wherever applicable)any modification(s)/ addition(s)/deletion(s)or any alteration in the requirement(s)/specification(s) etc. is required, the same will be placed on the IGIT website-www.igitsarang.ac.in therefore, all the bidders are advised to visit our website before filling/submitted their tenders. No separate advertisement/information will be published in this regard in the Newspapers.

ii) The offered rates will be valid initially for a period of one year. The Institute can place repeat order on same terms &conditions within this period.

iii) Acceptance of tender will be intimated to the successful tenderer through a Letter of Intent(LOI)duly signed by the authorized signatory of the institution.

iv)EMD/Performance Security of successful bidder may be forfeited, if the bidder withdraws or amends or derogates from the tender in any respect.

v)This tender is valid upto180 days from the issue of tender notification.

vi) The supplier will provide guarantee as per the product, and under guarantee period all the damages items shall be repaired/replaced by the supplier at their cost and risk.

vii)IGIT's official(s) can visit the work place of successful bidder and can review the progress of work and can instruct regarding quality aspect.

viii) The rates quoted by the bidder shall be complete for supply and installing of the finished items as per the specification(s) and shall be inclusive of all applicable tax, duty(ies),loading, unloading, packing, transportation to IGIT, Sarang installation (in Old academic block i.e. first floor Internet Administrator room)etc. and nothing extra/additional shall be payable on these rates.

ix) In any case, if tenders are not opened due to any reason, the Tender documents, processing Fee and EMD shall be returned to all bidders.

x)Conditional Tender will not be accepted.

xi) Successful bidder will be required to submit schedule of activities to complete the work order (day wise/Date wise)with technical bid document.

xii) The supplier has to ensure the rectification of defects within 7 days of the complaint during the period of guarantee.

xiii)AMC charges if any will be mentioned in the Tender.

xiv) The tenderer is required to submit Guaranty details to replace the damaged items during the guarantee period or repair.

xv) The authority reserves the right to accept or cancel any or all tenders without assigning any reason there-of.

xvi)All items should be ISI standard or equivalent.

6. Payment

i)The payment will be made on submission of bills after complete satisfactory supply ,installation, operation/functioning and dully verification of items as per OGFR/IGIT rule. No advance payment will be made against the supplies. Addition to this on complaint whenever reported it should be rectified within 7 days.

ii) Counter conditions by the Tenderers in matters concerning payment of bills shall not be acceptable.

7. Penalty Clause

The Time schedule should be strictly followed by the agency. An agreement will be made with the party/supplier to complete the work after getting purchase order within stipulated time. If work is not completed within stipulated schedule, penalty will be imposed as mentioned below.

i)The Agency will strict to the time schedule i.e 30-60 days for completing the supply order,

ii) In case of any abnormal irregularity noticed the penalty will be levied by IGIT. The decision of authority will be final and binding,

iii) In case the successful tenderer fails to complete the order in part or in whole, as the case may be, the penalty as deemed fit including for feiting the Performance Security/EMD by the Competent Authority shall be imposed on the tenderer.

Sd/-
Director, IGIT,Sarang

Annexure-I

Tender Form (Technical Bid) format

(To be submitted by the tenderer on their letter head.

To---------- Ref:-

---------- Dt-

Tender Notice No and Date Name of Work:"
The date and time of opening of tender:- at

Format for Qualifying Details of Technical Bid

A.General Details of the Bidder:			
Sl. No.	**Particulars**	**Remarks/Documents to** be **attached**	
01.	Name of the Organization:		
02.	Address of Head Office: Telephone No: E-mail: Fax number (if any) Name(s) of the contact person(s):		
03.	Company Status:- Proprietor/Partner/Pvt. Ltd. Company Enclose Details.-		
04.	Turnover of the Agency for The last three years: Annualized average financial turnover equivalent to Indian Rupees during last three financial years	YearINR (inLakh) 2020-21- 2021-22 - 2022-23	
05.	Indian Income Tax Return Acknowledgement	Financial Year-2020-21 Financial Year-2021-22 Financial Year-2022-23	
06.	Income Tax-PAN No.		
07.	VAT Tax Payer Identification Number(TIN)		
08.	Constitution of Firm (Proprietor/Partnership/ Company/Society)	Company Incorporation Certificate	
09	VAT Clearance Copy: -Service Tax Registration		
10	Similar work order of last 3 years to any govt. institution / university		

DECLARATION

I_____ hereby declare that the documents submitted/ enclosed are true and correct. In case any document at any stage found fake/ incorrect, action as deemed fit by the_____ can be taken against me. Also we here by accept all the Terms & Conditions of the Tender will abide by it.

A Processing Fee/EMD demand draft bearing No_____ dated drawn on is enclosed with Technical bid.

Signature.
Name
Address..
Mobile:....

Date:-

Signature and Seal of firm.

Annexure-II

ACCEPTANCE OF THE TENDERERS

All the clauses of tender document and Terms and Conditions as detailed in the Tender Document have been read/understood by me/ us are acceptable to me/ us. Me/ We confirm that we will abide by these terms & conditions.

Dated:- Signature

(Name in Block letters)_____Name of Tenderer_____

Address_____Address with stamp

Signature and seal of the firm

UNDERTAKING

To

The Director,
IGIT Sarang,
ODISHA

Sir,

1. I/we the undersigned, certify that I/we have gone through the terms and conditions mentioned in the tender documents and undertake to comply with them.

2. It is further certified that our firm has not been blacklisted by any agency in India or abroad.

Dated:

SIGNATURE OF THE TENDERER WITH SEAL

NAME OF THE TENDERER WITH ADDRESS

ANNEXURE-III

TECHNICAL BID

(Should be submitted in a sealed envelope separately)

Sl. No.	Item with specifications	Qty Required	Brand and Model no.	Manuals provided (YES / NO)
1.	**Next Gen Firewall NGFW** **3rd Party Test Certification:** Offered product should not have any observed evasions in 2019 SVM NGFW report of NSS and above 95% security effectiveness. The proposed OEM must be in the latest Leader's quadrant of the Enterprise Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof. **Equipment Test Certification:** Proposed solution should be ICSA, Common Criteria, NDPP/NDcPP certified. In case of newly released model, it must be under Common Criteria, NDPP/NDcPP evaluation and validation process. **Form factor:** Modular or Fixed **Architecture:** The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). 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. Should support redundant Power Supply Minimum 8 x 1G Cu Interface ports from day one. Minimum 6 x 1G SFP and 4 x 1G/10G SFP/SFP+ Interfaces from day one populated with 2 x 10G optical transceivers SR from same OEM from day one for each NGFW Unit. 2 x LC-LC Multi-Mode OFC patch cord supporting 10G connectivity to be included from day one. Dedicated HA ports, RJ-45 console port and management port in addition to requested data ports. Active/Active, Active/Passive for future enhancement **Performance Capacity:** NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware anti-spyware, Advance Threat, Zero day Protection, file blocking, and logging enabled, utilizing HTTP/IMIX/appmix transactions – Minimum 3.2 Gbps. Minimum IPSec VPN throughput – 4 Gbps Minimum client based remote access vpn – 500 from day one Proposed appliance should support New sessions per second – Minimum 100,000 utilizing 1 byte HTTP transactions. Proposed appliance should support Concurrent Connection	1	Fortinet/Cisco/PaloAlto/Check point or equivalent	

	per second with threat prevention features enabled – Minimum 940,000 or more. The device must support minimum concurrent access user 2000. Storage: Minimum internal storage 120 GB SSD **Memory (DRAM):16GB** **Prevention Features:** Next Generation Firewall, IDS and IPS, Application Control Anti-Malware, Anti-Virus, Anti-Spyware, Anti-Bot, Zero day protection, Same Hardware platform should be scalable to provide all above mentioned security protection features and should maintain same performance/throughputs mention in Performance Capacity Capabilities to evaluate proposed NGFW configuration by measuring the adoption of security capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks. The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic. The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP, Solution should support blocking of IPs/Domains/URLs either via External Dynamic List hosted on an external web server or via any other service with minimum 50,000 IPs, 1 Million domains and 100,000 URLs from day one. The proposed firewall shall be able to identify port-based rules/policies so admin / security team can convert them to application-based white list rules or add applications to existing rules without compromising application availability. Firewall must have inbuilt Automatic policy optimization to identify port-protocol based policies and convert the same into true application-based policies instead of combing through traffic logs and manually mapping applications to port-based rules. For example-Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/Rapidshare etc.) traffic going through the same policy, then the firewall should automatically identify those risky applications and help to add more application specific security policies which might be using the same ports (80/443). This will help us to tighten the application flow control and reduce the attack surface area. The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network. Proposed NGFW's Unknown malware analysis service must prevent unknown/zero-day threats inline and real-time using machine learning-based approach beyond traditional sandboxing. Solution should be able to capture snapshots of malicious activity in memory and conducts real-time analysis to identify malicious behavior, detecting highly evasive malware that would have otherwise gone undetected. Cloud / On-Prem Sandboxing service of proposed solution should support analysis of minimum 50000 or more files/day from day one. In case of cloud based solution, The Unknown malware analysis cloud must be in India. Unknown malware analysis service should be certified with SOC2 or any other			

	Data privacy compliance certification for customer data privacy protection, which is uploaded to unknown threat emulation and analysis. Same Hardware platform should be scalable to provide URL filtering and web protection and should maintain same performance/throughputs mention in primary scope. Solution should have the ability to detect and block new threats in real time, preventing patient zero. Solution should have capabilities of Fake captcha interaction analysis, deobfuscating java script engine , deep learning model , deep recursive analysis to provide comprehensive Phishing Detection and Protection. The proposed firewall shall have URL Filtering policies by AD user, group, machines and IP address/range. Should have full-path categorization of URLs only to block re categories the malicious malware path not the full domain or website. The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound and outbound connection The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections**.** SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well. Proposed NGFW should support TLS Version newer from day one. **Monitoring, Management and Reporting:** On device management with complete feature parity on firewall administration, logging, reporting and event correlation. Report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis. Export reports into other format such as PDF, HTML, CSV, XML etc. Built in report templates base on Applications, Users, Threats, Traffic and URLs. **Support & Warranty:** 5 Years Premium support bundle with 24x7x365 days, RMA, software updates and subscription update support. The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, AntiVirus, Anti Malware, Anti Spyware, Anti Botnet and Zero day protection.			
2	**Access Switch**, Switch should be 1U and rack mountable in standard 19" rack, have minimum 2 GB RAM and 2 GB Flash and have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 48 Gbps of stacking throughput with 8 switch in single stack. **Performance :** Switch shall have minimum 128 Gbps of switching fabric and 95.23 Mpps of forwarding rate, have minimum 16K MAC Addresses and active VLAN, support minimum 11K IPv4 routes or more, support 128 or more STP Instances and have 6MB or more packet buffer. **Functionality :** Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z. Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1. Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs. Switch shall have 802.1p class of service, Switch should support management features like SSHv2, SNMPv2c, SNMPv3,	5	Cisco, Dlink,HP or equivalent	

	NTP, RADIUS. Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports. Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type. During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified; it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic. **Interfaces:** Switch shall have 24 nos. 10/100/1000 Base-T ports and additional 4x 1/10G uplink ports, populated with 2 x 10G optical transceivers LR from same OEM and 2 x SC-LC Single-Mode OFC patch cord supporting 10G connectivity from day one for each Access Switchto be included. The SI must consider 9U rack (for each switch) having suitable depth to install the proposed switch if the old rack is not feasible. In case of new rack installation, the SI will be responsible for shifting other passive components from old rack. IGIT will not pay any separate charge for migration. All 24 port should support PoE (802.3af) and PoE+ (802.3at) with a PoE power budget of 370 W. **Certification:** Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements. Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification. OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from last 3 years before releasing this RFP. **Warranty support :** Minimum 5 years Term License.			
3	**Core Switch 24-Port** **General Features :** Switch shall have a minimum of 24 x 1Gig copper downlink port, Switch should Support Modularity on the Uplink Port for Future Scale. Switch Uplink should support 2x40Gig or 2x25Gig or 8x10Gig or 4x1Gig or 4x Multi gig SFP module, populated with 2 x 10G SR optical transceivers& 4 x 10G LR optical transceivers from same OEM from day one. 4 x SC-LC Single-Mode OFC patch cords supporting 10G connectivity also to be included from day one. **Performance Specifications :** Switch shall have 32000 total MAC addresses or more. 32000 of IPv4 routes (ARP plus learned routes), 16000 IPv6 routing entries or more. 8000 Multicast routing scale, capable of 5120 QoS scale entries, capable of 5120 ACL scale entries, capable of 64000 FNF entries, have minimum 8GB DRAM, have minimum 16GB FLASH, support jumbo Frames and capable of 4094 VLAN IDs. **Bandwidth Specifications :** Switch should have at least 256 Gbps or more of Switching capacity, 700 Gbps or more of	1	Cisco, Dlink,HP or equivalent	

	Switching capacity with Stacking, have 180 Mpps or more of forwarding rate, have 500 Mpps or more of forwarding rate with stacking and capable of Software define Access architecture. **Security Features :** Switch should support Encrypted Traffic Analytics day 1 for malware, support AES-256 MACsec encryption which is IEEE 802.1AE, support IPsec encryption and should provide support high-speed back-panel stacking bandwidth solution. The switch should be capable of P unicast routing protocols (including static, Routing Information Protocol Version 1 [RIPv1], RIPv2, RIPng, and Open Shortest Path First [OSPF], Routed Access). **High Availability Feature:** Ability to configure Link aggregation technology across different members of the stack for high resiliency. Switch shall deliver resilient architecture in stackable solution with sub-50-ms failover. The switch should support web GUI and CLI management tool. **Functionality :** Switch should support QoS through Differentiated Services Code Point (DSCP) mapping and filtering. Switch should support Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance. Switch should support management features like SNMPv3, NTP, RADIUS. Switch should support DHCP, Auto Negotiation, DTP, LACP, UDLD, MDIX, VTP, TFTP, NTP, Per-port broadcast, multicast, Static routing, Layer 2 trace route and unicast storm control. Should support management CLI and web UI over SNMP, RJ-45, Bluetooth or USB console access. Should have trunk failover capabilities to ensure server NIC adapters team up to provide redundancy in the network so that in case of the link is lost on the primary interface, network connectivity is transparently changed to the secondary interface. Security with 802.1X support for connected devices, Switched Port Analyzer (SPAN), and Bridge Protocol Data Unit (BPDU) Guard. ICES-003 Class A, EN 55032 Class A, CISPR 32 Class A, EN 55024, EN300386 **Operating temperature: -5°C to +45°** **Safety certifications:** UL 60950-1, EN 60950-1, IEC 60950-1, AS/NZS 60950.1, IEEE 802.3 Warranty support : Minimum 5 years Term License.			

NB* : For any clarification regarding above mentioned items the quotationer may visit CSEA department office during office hour before sending the tender.

Signature and Seal of the firm.

FINANCIAL BID

(Should be submitted in a sealed envelope separately)

LIST OF ITEMS

Sl. No.	Item with specifications	Qty Required	Total cost (Inclusive of all taxes F.O.R. to IGIT Sarang and installation etc.) (Rs.)	TAX(%)
1.	**Next Gen Firewall NGFW** **3rd Party Test Certification:** Offered product should not have any observed evasions in 2019 SVM NGFW report of NSS and above 95% security effectiveness. The proposed OEM must be in the latest Leader's quadrant of the Enterprise Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof. **Equipment Test Certification:** Proposed solution should be ICSA, Common Criteria, NDPP/NDcPP certified. In case of newly released model, it must be under Common Criteria, NDPP/NDcPP evaluation and validation process. **Form factor:** Modular or Fixed **Architecture: :** The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). 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. Should support redundant Power Supply Minimum 8 x 1G Cu Interface ports from day one. Minimum 6 x 1G SFP and 4 x 1G/10G SFP/SFP+ Interfaces from day one populated with 2 x 10G optical transceivers SR from same OEM from day one for each NGFW Unit. 2 x LC-LC Multi-Mode OFC patch cord supporting 10G connectivity to be included from day one. Dedicated HA ports, RJ-45 console port and management port in addition to requested data ports. Active/Active, Active/Passive for future enhancement **Performance Capacity:** NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware anti-spyware, Advance Threat, Zero day Protection, file blocking, and logging enabled, utilizing HTTP/IMIX/appmix transactions – Minimum 3.2 Gbps. Minimum IPSec VPN throughput – 4 Gbps	1		

	Minimum client based remote access vpn – 500 from day one Proposed appliance should support New sessions per second – Minimum 100,000 utilizing 1 byte HTTP transactions. Proposed appliance should support Concurrent Connection per second with threat prevention features enabled – Minimum 940,000 or more. The device must support minimum concurrent access user 2000. Storage: Minimum internal storage 120 GB SSD **Memory (DRAM):16GB** **Prevention Features:** Next Generation Firewall, IDS and IPS, Application Control Anti-Malware, Anti-Virus, Anti-Spyware, Anti-Bot, Zero day protection, Same Hardware platform should be scalable to provide all above mentioned security protection features and should maintain same performance/throughputs mention in Performance Capacity Capabilities to evaluate proposed NGFW configuration by measuring the adoption of security capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks. The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic. The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP, Solution should support blocking of IPs/Domains/URLs either via External Dynamic List hosted on an external web server or via any other service with minimum 50,000 IPs, 1 Million domains and 100,000 URLs from day one. The proposed firewall shall be able to identify port-based rules/policies so admin / security team can convert them to application-based white list rules or add applications to existing rules without compromising application availability. Firewall must have inbuilt Automatic policy optimization to identify port-protocol based policies and convert the same into true application-based policies instead of combing through traffic logs and manually mapping applications to port-based rules. For example- Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/Rapidshare etc.) traffic going through the same policy, then the firewall should automatically identify those risky applications and help to add more application specific security policies which might be using the same ports (80/443). This will help us to tighten the application flow control and reduce the attack surface area. The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network. Proposed NGFW's Unknown malware analysis service must prevent unknown/zero-day threats inline and real-time using machine learning-based approach beyond traditional sandboxing. Solution should be able to capture snapshots of malicious activity in memory and conducts real-time analysis to identify malicious behavior, detecting highly evasive malware that would have otherwise gone undetected. Cloud / On-Prem			

	Sandboxing service of proposed solution should support analysis of minimum 50000 or more files/day from day one. In case of cloud based solution, The Unknown malware analysis cloud must be in India. Unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection, which is uploaded to unknown threat emulation and analysis. Same Hardware platform should be scalable to provide URL filtering and web protection and should maintain same performance/throughputs mention in primary scope. Solution should have the ability to detect and block new threats in real time, preventing patient zero. Solution should have capabilities of Fake captcha interaction analysis, deobfuscating java script engine , deep learning model , deep recursive analysis to provide comprehensive Phishing Detection and Protection. The proposed firewall shall have URL Filtering policies by AD user, group, machines and IP address/range. Should have full-path categorization of URLs only to block re categories the malicious malware path not the full domain or website. The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound and outbound connection The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections**.** SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well. Proposed NGFW should support TLS Version newer from day one. **Monitoring, Management and Reporting:** On device management with complete feature parity on firewall administration, logging, reporting and event correlation. Report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis. Export reports into other format such as PDF, HTML, CSV, XML etc. Built in report templates base on Applications, Users, Threats, Traffic and URLs. **Support & Warranty:** 5 Years Premium support bundle with 24x7x365 days, RMA, software updates and subscription update support. The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, AntiVirus, Anti Malware, Anti Spyware, Anti Botnet and Zero day protection.Specification May Change.			
2	**Access Switch**, Switch should be 1U and rack mountable in standard 19" rack, have minimum 2 GB RAM and 2 GB Flash and have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 48 Gbps of stacking throughput with 8 switch in single stack. **Performance :** Switch shall have minimum 128 Gbps of switching fabric and 95.23 Mpps of forwarding rate, have minimum 16K MAC Addresses and active VLAN, support minimum 11K IPv4 routes or more, support 128 or more STP Instances and have 6MB or more packet buffer. **Functionality :** Switch should support IEEE Standards	5		

	of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z. Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1. Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs. Switch shall have 802.1p class of service, Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS. Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports. Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type. During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified; it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic. **Interfaces:** Switch shall have 24 nos. 10/100/1000 Base-T ports and additional 4x 1/10G uplink ports, populated with 2 x 10G optical transceivers LR from same OEM and 2 x SC-LC Single-Mode OFC patch cord supporting 10G connectivity from day one for each Access Switchto be included. The SI must consider 9U rack (for each switch) having suitable depth to install the proposed switch if the old rack is not feasible. In case of new rack installation, the SI will be responsible for shifting other passive components from old rack. IGIT will not pay any separate charge for migration. All 24 port should support PoE (802.3af) and PoE+ (802.3at) with a PoE power budget of 370 W. **Certification:** Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements. Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification. OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from last 3 years before releasing this RFP. **Warranty support :** Minimum 5 years Term License.			
3	**Core Switch 24-Port** **General Features :** Switch shall have a minimum of 24 x 1Gig copper downlink port, Switch should Support Modularity on the Uplink Port for Future Scale. Switch Uplink should support 2x40Gig or 2x25Gig or 8x10Gig or 4x1Gig or 4x Multi gig SFP module, populated with 2 x 10G SR optical transceivers & 4 x 10G LR optical transceivers from same OEM from day one. 4 x SC-LC Single-Mode OFC patch cords supporting 10G connectivity also to be included from day one. **Performance Specifications :** Switch shall have 32000 total MAC addresses or more. 32000 of IPv4 routes	1		

	(ARP plus learned routes), 16000 IPv6 routing entries or more. 8000 Multicast routing scale, capable of 5120 QoS scale entries, capable of 5120 ACL scale entries, capable of 64000 FNF entries, have minimum 8GB DRAM, have minimum 16GB FLASH, support jumbo Frames and capable of 4094 VLAN IDs. **Bandwidth Specifications :** Switch should have at least 256 Gbps or more of Switching capacity, 700 Gbps or more of Switching capacity with Stacking, have 180 Mpps or more of forwarding rate, have 500 Mpps or more of forwarding rate with stacking and capable of Software define Access architecture. **Security Features :** Switch should support Encrypted Traffic Analytics day 1 for malware, support AES-256 MACsec encryption which is IEEE 802.1AE, support IPsec encryption and should provide support high-speed back-panel stacking bandwidth solution. The switch should be capable of P unicast routing protocols (including static, Routing Information Protocol Version 1 [RIPv1], RIPv2, RIPng, and Open Shortest Path First [OSPF], Routed Access). **High Availability Feature:** Ability to configure Link aggregation technology across different members of the stack for high resiliency. Switch shall deliver resilient architecture in stackable solution with sub-50-ms failover. The switch should support web GUI and CLI management tool. **Functionality :** Switch should support QoS through Differentiated Services Code Point (DSCP) mapping and filtering. Switch should support Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance. Switch should support management features like SNMPv3, NTP, RADIUS. Switch should support DHCP, Auto Negotiation, DTP, LACP, UDLD, MDIX, VTP, TFTP, NTP, Per-port broadcast, multicast, Static routing, Layer 2 trace route and unicast storm control. Should support management CLI and web UI over SNMP, RJ-45, Bluetooth or USB console access. Should have trunk failover capabilities to ensure server NIC adapters team up to provide redundancy in the network so that in case of the link is lost on the primary interface, network connectivity is transparently changed to the secondary interface. Security with 802.1X support for connected devices, Switched Port Analyzer (SPAN), and Bridge Protocol Data Unit (BPDU) Guard. ICES-003 Class A, EN 55032 Class A, CISPR 32 Class A, EN 55024, EN300386 **Operating temperature: -5°C to +45°** **Safety certifications:** UL 60950-1, EN 60950-1, IEC 60950-1, AS/NZS 60950.1, IEEE 802.3 Warranty support : Minimum 5 years Term License.			

Signature and Seal of the firm.

CHECK LIST

TENDER NO :

1. Tender Fee Demand Draft : _____
2. EMD Demand Draft :_____
3. Registration certificate of the firm :_____
4. OEM / AUTHORIZED DEALER / DISTRIBUTOR / DEALER / RETAILER CERIFICATE_____
5. PAN NO._____
6. Service Tax_____
7. GST NO. _____
8. Experience certificate (Last 03 years)_____
9. Turnover Certificate issued by CA (Last3years)_____
10. IncomeTaxReturns(Last3years)_____
11. Annexure_____
12. Undertaking_____