Centre for Distance & Online Education (CDOE)

D.D.C.E.,

UTKAL UNIVERSITY

NAAC A+

BHUBANESWAR-751010

TENDER CALL NOTICE

Sealed Tenders are invited from reputed registered authorised suppliers / distributors with valid GSTIN for supply of next generation Firewall and Centralised End Point Antivirus. Interested Firms may submit their tender papers to the undersigned on or before 10.09.2024 by 5P.M. Tender documents will be submitted at office of the Director, DDCE, Utkal University. Visit Website : ddceutkal.ac.in for important date lines, terms and conditions and the tender forms. The authority reserves the rights to reject any or all tender papers without assigning any reason thereof.

DIRECTOR

DDCE ,UTKAL UNIVERSITY, VANI VIHAR,BHUBANESWAR
TENDER CALL NOTICE

Tender in plain paper in sealed covers invited by the undersigned from the intending reputed firm those who are registered under Goods and Services Tax (GST) Act and having valid Registration No. of PAN, TIN/SRIN AND GST clearance certificate to procure the following items, Firewall and End point security (Antivirus) of Desktop & server as mentioned below for DDCE ,Utkal University for the year 2024-25. The last date of submission of Tender along with the required documents & EMD (1% of the total quoted price or Rs.10,000/-) etc. is 10.09.2024 (up to 5:00 P.M).

The tender papers are to be downloaded from the website of the University (www.ddceutkal.ac.in) and need to deposit a crossed demand draft of Rs.500/- (Rupees Five Hundred) only (non-refundable) as tender paper cost drawn in favour of the Director, DDCE, Utkal University, payable at Canara Bank , DDCE Building Branch, Bhubaneswar.

LIST OF ITEMS FOR PROCUREMENT

A. Next Generation Firewall with 60 months Subscription ---- 01

B. Centralized End Point Security (Antivirus software) for server --- 02 & desktop – 60 with 60 months Subscription.

A. Technical Specification of Next Generation Firewall

Make : **Model :**

Sl. No.	Item Description	Technical Specification
1	Make	To be mentioned by the bidder/ Vendor
2	Model No.	To be mentioned by the bidder/ Vendor (***Existing model SOPHOS (XG310***) Proposed model should be higher model)
3	Hardware Architecture	• The proposed hardware-based firewall should not consume more than 1RU Rack mountable space • Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core CPU's based architecture to protect latest security threats. • Appliance must have one Console port, dedicated one management Port, two USB port and redundant power supply
4	General Firewall Features	• Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy -based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone traffic • Firewall should support clientless SSL VPN technology or an easy to manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.

Technical Specification of Next Generation Firewall

	NGFW Technical Specifications	Compliance (Y/N)
Sl.	**Hardware Architecture & Performance**	
1	The appliance based security platform should be capable of providing firewall, application visibility, Web Protection and IPS functionality in a single appliance	
2	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support minimum 8GB memory. Should have dedicated network preocessor with additional RAM for hardware accelaration .	
3	Should support minimum 120 GB SSD for logs & reports	
4	The appliance should support atleast 8 * 1G ports 2 * 1G SFP ports from day 1 . The appliance should have option to support additional 4 * 10G ports in future.	
5	Should support atleast 24 Gbps Firewall throughput & 5 Gbps of NGFW throughput	
6	Proposed appliance should support atleast 5 million concurrent sessions or more	
7	Firewall should support atleast 125K connections per second or more	
8	Solution should have 11 Gbps of IPSec VPN throughput	
9	Firewall Should support atleast 1Gbps of Threat Protection Throught (Measured with Firewall, IPS, Application Control, and Malware prevention enabled)	
10	Solution should have 1.1Gbps SSL/TLS inspection throughput & 1500 SSL VPN concurrent tunnel	
	General Management	
1	Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators	
2	Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN	
3	High Availability (HA) support clustering two devices in active-active or active-passive mode.	
4	Automated firmware update notification with easy automated update process and roll-back features	
5	Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers	
6	SNMPv3 and Netflow support , API for 3rd party integration	
7	Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly	
	Firewall, Networking & Routing	
1	Stateful deep packet inspection firewall	
2	Network Flow FastPath acceleration for trusted traffic	
3	User, group, time, or network based policies	
4	Access time polices per user/group	

5	Enforce policy across zones, networks, or by service type	
6	Zone isolation and zone-based policy support	
7	Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi	
8	Custom zones on LAN or DMZ	
9	Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule	
10	Flood protection: DoS and portscan blocking Country blocking by geo-IP	
11	WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules	
12	Full configuration of DNS, DHCP and NTP, 802.3ad interface link aggregation	
13	IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment through IPSec	
14	Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping optionsincluded with the Web Protection subscription)	
15	Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical	
	Next Gen VPN Support	
1	Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key	
2	L2TP and PPTP,Route-based VPN	
3	Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support,IKEv2 Support	
4	SSL client for Windows and configuration download via user portal	
5	Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC	
6	Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH	
7	Enables Synchronized Security and Security Heartbeat for remote connected users	
8	Unilimited IPSec & SSL client with unlimited 2factor mobile (android & IOS) authenticator license	
9	Single client support for IPSec & SSL remote VPN	
10	Mac and Windows Support	
	Wireless Protection	
1	Wireless controller with 50 access point management license from day1	
2	Multiple SSID support per radio including hidden SSIDs	
3	Bridge APs to LAN, VLAN, or a separate zone with client isolation options	
4	Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support	
5	Support for 802.11r (fast transition)	
6	Hotspot support for (custom) vouchers, password of the day, or T&C acceptance	
7	Wireless guest Internet access with walled garden options	
8	Time-based wireless network access	
9	Wireless repeating and bridging meshed network mode with supported Aps	

	Intrusion Prevention (IPS)	
1	High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	
2	Minimum 5000 of signatures,Support for custom IPS signatures	
3	Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	
4	Security Heartbeat instantly identifies compromised endpoints including the host,user,process, incident count, and time of compromise	
5	Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned	
6	Lateral Movement Protection further isolates compromised systems by having healthy -managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain	
	Web Protection and Control	
1	Fully transparent proxy for anti-malware and web-filtering	
2	Enhanced Advanced Threat Protection	
3	URL Filter database with millions of sites across 92 categories backed by OEMLabs	
4	Surfing quota time policies per user/group ,Access time polices per user/group	
5	Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email	
6	Advanced web malware protection with JavaScript emulation	
7	Live Protection real-time in-the-cloud lookups for the latest threat intelligence	
8	Second independent malware detection engine for dual-scanning	
9	HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions	
10	File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)	
11	YouTube for Schools enforcement per policy (user/group)	
12	SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)	
13	Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists	
14	Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users	
15	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated	
	Application Protection and Control	
	Zero Day Protection	

	60 months License Includes :	
1	Network Protection Subscriptions (IPS,HTML5, ATP, Anti-malware),	
2	Web Protection Subscriptions (URL, AppCtrl, Web/App Traffic Shaping),	
3	Zero Day Protection	
4	24 X 7 hardware & warranty support from OEM	

Next Generation Firewall Description of work

Sl.	Item	Description of Work
01.	Installation & Configuration of Firewall	1. Configuration of Network LAN, WAN & DMZ 2. Create the policy for inbound & outbound. 3. NAT Policy 4. Web filtering policy 5. User-based authentication 6. App-based policy 7. Location-based policy 8. Creation of different groups 9. Quality of service implementation 10.VPN Set-up 11.Set up for logging & reporting. 12.Load Balancing set-up 13.Configure Access Control Lists (ACLs) 14.Establish Firewall Zones and an IP Address Structure 15. **Buy back of existing Firewall (Model - XG310) Maker - SOPHOS**

B. **Centralized End Point Security (Antivirus software) for server --- 02 & desktop – 60 with 60 months Subscription.**

Specification for Centralized End Point Security (Antivirus)		
	MAKE : **Model :**	
S.No	**Description**	**Compliant (Yes / No)**
1	Proposed Solution should be in 'Leaders' quadrant of the gartners Magic Quadrant for Endpoint protection platform for past 5 years.	
2	The Endpoint security solution should provide enhanced antivirus protection for desktops & servers of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code.	
3	The The Endpoint security solution Should have a Centralized Management Console for both servers & desktop/laptop	
4	Solution should have application based console rather than web based console for secure access	
5	The OEM must have its own proprietary scan engine	
6	The antivirus solution Should Support Multi -Platform operating system(Windows , Mac, Linux) and the same should be managed from a single Centralised Management cosole	
7	Solution should have exploit prevention technology Solutions should have deep learning/machine learning features	

8	Solution must offer Forensic-level system cleanup	
9	The solution Should have single, Configurable Installation with centralized configuration & policy management.	
10	Solution should support integration with Active directory for directory structure of computers for better management	
11	Solution should provide the functionality of the Download Reputation that allows for a check to be performed against files as they are downloaded,in order to determine the reputation of the file	
12	Solution should have capability of Automatic update of Antivirus Server from Vendor Site & The client should get update from the local Server If updating from the Primary Server fails for any reason (such as the user being off the network) an attempt should be made to contact the Secondary Server (I.e Vendor site)	
13	Solution should provide the centralized scanning of all network Machines	
14	Centralized management should be aloways up and running, zero downtime	
15	Solution must mitigate exploits in vulnerable applications a) Protect web browsers b) Protect web browser plugins c) Protect Java applications d) Protect media applications e) Protect office applications	
16	Solution should offer Data Loss Prevention (DLP) to Restrict unauthorized data flow using prebuilt or custom rules	
17	Administrator should have flexibility to schedule Scan and update at the endpoints from central Server.	
18	Antivirus should be able to capture Viruses, Trojans, Worms,Spyware and Malware,adware and PUA from single agent.	
19	Solution should Protect processes by a)Preventing process hollowing attacks b) Preventing DLLs loading from untrusted folders	
20	Anti Virus Should have Host Intrusion Prevention System (HIPS) technology which works in 4 Layers to provide zero day protection without the need for updates (Unknown Virus Detection & Repair),	
21	Antivirus should have run time detection technology i.e behavioral & Heuristic scanning to protect from unknown viruses and buffer overflow protection integrated with AV scan engine for protection from threats/exploits that uses buffer overflow	
22	Anti-Virus Software must have the capability to clean, Qurantine or delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms	
23	Antivirus vendor should provide definitions with incremental updates. Should support daily update for definition files. Size of daily update should be extremely small in size	
24	Administrator Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.	
25	Solution should allow the below alerting Mechanisms a)Desktop Messaging b)Email Alerting c)SNMP Messaging	

	d) Event Log	
26	Solution client firewall should be running in stealth mode that denies the unauthrorised network access by hackers	
27	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure.	
28	Administrator should be able to lock down all anti-virus configurations at the desktop & User should be prevented from being able to uninstall the anti-virus software.	
29	Solution should have PUA scanning that will inform administrator which applications have been found. You can then configure your anti-virus policies to allow or remove applications on this list. This gives you full control over what is available to users, enabling you to retain or remove individual applications as required.	
30	Administrator must be able to distribute new and update anti-virus software, virus definitions and Policies automatically to clients and servers from a central location .	
31	Administrator Should be able to initiate virus sweeps remotely in case of an outbreak.	
32	Antivirus should provide centralized event logging to locate and cure virus problems.	
33	Should have cryptoguard & wipeguard zero day ransomware protection & file recovery without disrupting business user	
34	Antivirus solution Should have APPLICATION Control module with the ability to block or be alerted to the use of a long list of UnAuthorised applications (E.g. File Sharing , Games, etc.)	
35	Solution should provide the Application Control that enables network administrators to block certain legitimate applications from running on work computers.In accordance with your company policy on Application Control, it should give option to authorize required applications, and block those which are not required - all from the central console.	
36	Soluntion should have Data control that enables you to monitor and control the transfer of files from computers to storage devices and applications connected to the internet.	
37	Solution should support Data protection policy to Monitor data copied or shared through external Mediums and Internet Browsers.	
38	Antivirus solution should have integrated DEVICE control module with a features to set devices to " Read Only " , "Add Exceptions'" and " Block " Black listing and whitelisting of the devices.	
39	Solution must support malicious traffic detection to monitor non-browser based traffic for any Command & Control Servers connection	
40	Antivirus solution should have a Live web protection module Integrated into existing endpoint agent with no endpoint configuration required to Blocks URLs that are hosting malware and Should Support all major browsers.	
41	Vendor Should have Threat analysis centers to provide proactive rapid protection against known and unknown threats	
42	Vendor Should have 24*7 toll free Global Technical Support .	

43	Solution should have decision chaching technology , for scanning modes.	
44	Solution should have genotype technology that should be able to detect malicious behaviour even before specific signature-based detection has been issued. This technology shall be available at endpoint ,email & web security components of OEM	
45	Solution should have Have Web Filtering on category basis.	
46	Patch assesment for top Vendors and assistance to understand security risk on endpoints	
47	Device Blocking and Exeptions with Vendor and Model (Device ID)	
48	Solution should have the feature in which User activity is logged and viewable directly within management Console, allowing you to audit and identify undesirable behaviour	
49	Solution should Prevent users from compromising browsing policies	
50	Solution Web Filtering should allow to configure the policy to Allow,Warn,Block	
51	Solution should have the customization to allow or block certain websites as required by administrator.	
52	Solution should work together with gateway via security heartbeat to instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise	
53	Solution should work together with gateway via security heartbeat that can limit access to network resources or completely isolate compromised systems until they are cleaned up	
54	OEM should have recived highest rating for endpoint protection in NSS lab.	
55	OEM should be leader in Gartner magic quadrant for last 5 years.	

DETAILS TERMS AND CONDITIONS OF THE TENDER NOTICE

1. The bid proposals are to be sent in 03 (three) separate sealed covers i.e. mentioning

(i) **Technical Bid (Annexure-I)** (ii) **Financial Bid (Annexure-II)** (iii) **Tender fee & EMD**. These three envelopes should be kept in one sealed envelope dully super scribed with Tender Reference No. as appended hereunder:

From	To
M/S.	The Director
Contact No.	DDCE,Utkal University
E.Mail	Vinivihar, Bhubaneswar-7

2. The bids without tender fees or EMD will summarily be rejected and no further communications in this regard shall be entertained Those who are technically qualified, onlytheir price bid shall be opened.
3. The bidders shall deposit earnest money as mentioned in shape of Bank Draft/Pay Order infavor of DIRECTOR , DDCE Utkal University, payable at Canara Bank, DDCE Building Branch, Utkal University, Vani Vihar,Bhubaneswar.
4. The Tender Paper (Technical Bid) shall be opened on 12.09.2024 at 11:30 A.M. at Office of the Registrar, Utkal University in the presence of the bidders or their authorized representatives.
5. OEM Authorization to be submitted .
6. Both the product having single OEM
7. If, the firm becomes unwilling to honor after it is selected in due process, its EMD shall be forfeited. There shall be no over writing on the Tender paper submitted.
8. The rates quoted shall be inclusive of all Taxes /GST, transportation, delivery and installation charges.
09. The bid submitted once cannot be withdrawn.
10. The Authorities of the University reserve the right to reject any or all tender/tenders without assigning any reason thereof. The incomplete tender papers or received after the scheduled date and time shall be rejected.
11. The Authorities are not bound to accept the lowest financial bid and reserve the right to negotiate the rates and other terms and conditions with the lowest bidders.
12. All disputes arising out of the transaction shall be subject to the jurisdiction of the Hon'bleHigh Court, Odisha.

DIRECTOR,
DDCE,Utkal,University

Annexure-I

Technical Bid

Sl.#	Particular	Details
1	Name of the Firm	
2	Type of Firm (Proprietary/ Partnership/ Pvt. Ltd. / Public Ltd/ Sole Proprietorship)	
3	Date of Establishment and Experience in business	
4	Registered office Address & Complete postal address	
5	Local office in Odisha (along with address & contact details).	
6	Telephone & e-Mail id of authorized person	
7	G.S.T. Registration No. (Attach Photo copy)	
8	PAN No. (Attach Photo copy)	
9	EMD & TENDER FEE AMOUNT / DD No. / Date	
10	OEM Authorization copy	
11	Latest Income tax Clearance certificate. (Attach Photo copy)	
12	MSME / ISO 9001 : 2015 certificate. (Attach Photo Copy)	
13	Details of service provided to the Government. undertaking organization with proof.	Present:
		Past:

Certified that:-

1. I / we have read the terms and conditions governing this work of the University and hereby agree to abide by them.
2. The agency (or any of its members) has neither been blacklisted by any central or state government organization in the last five years or any litigation pending with any of these department or Course of Law.
3. The information provided as above regarding the details of firms is correct and if found to be incorrect at later stage; our bids may be summarily rejected.

Name and signature of the authorized Signatory with sea

Annexure-II

Financial Bid

Print in Letter Pad.

Sl. No	Item Description	Qty	Make & Model	Rate per unit (In Rs.)	Total Price (In Rs.)
1	Next Generation Firewall with 5 years warranty and Subscription	1 no.s			
2	End Point For Node(Desktop / laptop) For 5 years Subscription	60 no.s			
3	End Point For Server for 5 years Subscription	2 no.s			
Grand Total (Rs.)					
Grand Total (In words)					

Signature of the authorized
Signatory with seal