Centre for Development Studies

TENDER DOCUMENT

For

Supply and installation of Next Generation Firewall

TENDER NO. CDS/CC/ 2023-24/T1

Last date for Submission: 07-07-2023 , 5 PM

Centre for Development Studies (CDS)

Prasanth Nagar, Ulloor , Medical college PO, Thiruvananthapuram 695011

No. CDS/CC/2023-24/T1 22-06-2023

NOTICE INVITING TENDER

Sealed tenders are invited for the **Supply and installation of Next Generation Firewall at the Centre for development studies with 3 year subscription.**

Last date of submission of the bids : --- : 07-07-2023 , 5 PM

Tender Document Fee
The cost of the tender document is Rs:- 590/- (Rupees five hundred and ninety only) including taxes, and it should be submitted in the form of a Demand Draft drawn in favour of " Registrar, Centre for Development
Studies" payable at Thiruvananthapuram

Earnest Money Deposit (EMD)
EMD of Rs.10000/- (Rupees Ten Thousand Only), including taxes should be submitted as a Demand Draft drawn in favour of "Registrar, Centre for Development Studies" payable at Thiruvananthapuram.

1. **Technical Specification**
   Detailed Specification is given in Annexure 3

2. **The Terms and Conditions**

   1. The bidder must be responsible for supply, deploy and support the infrastructure during three years of service.
   2. 100% payment will be released only on satisfactory installation/services as per the scope of work as certified by the officer in charge of the Institute and after producing the GST invoice
   3. The existing Firewall installed at CDS is Fortinet 300D. The new device will be configured as per the current configuration and necessary modifications if required.
   4. The new product shall be installed and configured on or before the last week of September 2023.

3. Bidder requirements and documents to be submitted.

1. The bidder should be a registered company or firm in India.
2. The bidder should have an office in kerala. (Enclose relevant document).
3. The bidder must be an authorized reseller of the proposed product. The bidder need to submit Manufacturer authorization letter from OEM
4. The bidder should have previous experience of supply and installation of at least one firewall product in the last three years. Enclose proof of the same.
5. The Bidder company/firm must have PAN Number and GST registration. (Enclose copy of the relevant document).
6. The company/firm shall not enter into a franchisee contract with another vendor.
7. The bidder shall enclose a complete bill of material with OEM part code. Documentary evidence such as OEM datasheet/spec sheets etc. must be enclosed. All supporting documents such as datasheet, spec sheet, admin guide etc. must be enclosed. All documents should be readily available online. The bidder must share the online links for all the supporting documents.
8. The EMD and tender document fee is exempted for MSMEs registered suppliers.

4. The Bid process – Two bid processes (Technical and Financial)

The two bid system will be followed for this tender. The bidder is advised to carefully read this tender document before submitting his bid.

Interested Companies/ firms may submit their documents satisfying the technical bid requirements in a sealed cover super scribed with " **Tender for Supply and Installation of Next Generation Firewall for technical bidding**". The technical bids should contain Annexure- 1, Annexure- 2 , Annexure-3, Annexure 4, all the relevant documents mentioned in the tender, EMD and tender fee.

The other sealed envelope containing the quoted rates and documents relating to acceptance of all the terms and conditions, etc as mentioned in Annexure- 5 may be submitted super scribed with "**Tender for Supply and Installation of Next Generation for Financial bidding**". Thereafter, both the envelope may be placed in a third sealed cover super scribed with "**Supply and installation of Next Generation Firewall for technical and financial bidding**" addressed to **Registrar, Centre for Development Studies, Prasanth Nagar, Ulloor, Medical college PO, Thiruvananthapuram 695011**.

The technical bids will be opened at Registrar's office. The financial bid of only those parties shall be opened whose technical bids are found eligible. After verification of technical bids, CDS will shortlist eligible companies and inform them the date of opening of sealed "Financial bid" through email.

1. Late submission of tenders will not be accepted.
2. Tenders by Fax/e-mail will not be accepted. Tenders may be submitted by Registered Post, by Hand in Person or by Courier. However, any delay on this account shall not be accepted as a reason for the exception.
3. Bids received after the due date, those received without separate sealed cover and rates not quoted in specified Performa will not be accepted.
4. The rates quoted should be net, and no discount or free services/offers quoted will be considered.
5. The bid shall remain valid for 90 days from the date of opening of the financial bid.
6. The technically qualified bidder who quoted the lowest amount in the financial bid will be considered as the successful bidder.
7. CDS reserves the right to accept or reject any or all tenders without assigning any reasons.
8. If any dispute(s) arises between the CDS and the firm with reference to any provision of the contract, the decision of the CDS shall be final and binding on both parties.

ANNEXURE- 1 Bidder Profile

(To be filled on company/firm letterhead)

SINO	**Item**	**Description**
1	Name of the company/firm	
2	Address (with Tel. No., fax no. & e-mail address)	
3	Registration Number	
4	PAN Number	
5	GST Registration Number	
6	MSME Status (YES/NO)	
7	Details of the EMD and tender fee details (DD details)	
8	Details of the Contact person	

Confirm the following enclosure along with this format:

a. Technical literature about the company

b. Filled checklist and documents supporting items mentioned in the checklist and any other relevant documents supporting the tender document.

Declaration

I hereby certify that the information furnished above is full and correct to the best of our knowledge. We understand that in case found any deviation in the above statement occurs at any stage, the company will be black-listed and will not have any deal with the Trust in future.

(Seal and Sign of Authorized Signatory)

Name :

Annexure -2 Checklist

SINO	Description	Compliance (Yes/No)	Documents attached if any
1	The bidder company/firm registration		Please indicate bid page no. where the document is attached
2	The bidder company/firm should have implemented a similar solution in at least one location.		- do-
4	The Bidder company/firm must have an office in Kerala		- do-
5	The bidder must have a PAN Number and GST Registration.		-do-

Annexure – 3

Specifications

	NGFW Specifications	**Complaince (YES/NO)**
Sl.no	**General Requirements**	
1	The Firewall must be appliance based, rack mountable, and it should have an internal redundant Power Supply from day one	
2	The Proposed Firewall Vendor should be in the Leaders/ Challenger in Quadrant of Gartner Magic Quadrant for Enterprise Network Firewall.	
3	The proposed NGFW must have built-in GUI and CLI to make on the go changes to Firewall policies without any dependency to manage and troubleshoot any issue related to network outages.	
4	NGFW must support the Secure SD-WAN feature along with advanced routing protocols such as BGP	
5	SD-WAN must be able to link and failover between various connections such as the Internet, MPLS, leash line, and even Routed based VPN interfaces.	
6	Build-in SDWAN must be able to do load balancing of various links based on source address, User group , protocol and/or applications	
7	SLA for SDWAN must be defined based on packet loss or latency or jitter. Even a combination of all 3 options must be possible.	
8	Central management solution for the next generation Firewall must be able to Manage all the SDWAN link centrally and should give a clear dashboard showing which links are down and which are up. This helps the NOC to take action accordingly.	
9	NGFW must support multicast routing as well as firewalling	
10	The proposed solution should also support policy routing. Policy routing should work along with SD-WAN and ISP load-balancing.	
11	The proposed solution must also support identity based routing option allowing traffic to be forced out of specific Internet/MPLS gateway based on authentication rather than IP address	
12	The proposed system should have integrated Traffic Shaping functionality. This feature should have option to be configured on same firewall policy along with the option to configure it separately if required.	
13	Build-in GUI on the NGFW should have the option to display the logical topology of the network the NGFW is protecting. The display should also be able to give security recommendations for the NGFW.	
14	The device should support Static routing, RIP, OSPF,BGP and OSPFv3	

15	Device must be able to connect with LDAP, Winodws Active directory and , Radius.	
16	The service and support should be available for a period of 3 Years	
	Performance Parameters	
1	The solution should support a minimum of at least 4 Gbps IPS throughput & Minimum 3 Gbps NGFW throughput on real-world / enterprise mix traffic test condition	
2	The solution should support minimum 2.5 Gbps threat protection throughput on real-world / enterprise mix traffic test condition	
3	Should support 6 Gbps IPSec VPN throughput and 1000 Tunnels	
4	The Firewall must support at least 2,000,000 concurrent connections and 200,000 new sessions per second.	
5	1. The platform must be having a minimum of 8 GE RJ45 interfaces from day 1 with auto sensing 10/100/1000 capability 2. 4 Gigabit SFP ports and 4 * 10-GbE SFP+ Interfaces from day one or 4 * 1G/10G SFP+ Interfaces from day one	
	Firewall Features	
1	A firewall policy should be a single policy where all the features get applied such as IPS, application control, URL filtering , antivirus , SSL inspection, logging and even NAT	
2	The firewall must support Zoning option along with User based authentication. It must have an automatic option to group all the same zone policy	
3	There must be option to configure the said Firewall policy from GUI of the NGFW appliance without requiring any Management solution. This is in the case of an emergency where a management solution is no available and policy needs to be changed.	
4	The firewall must support NAT46, NAT66 and NAT64 along with policy for such NAT along with option to configure DNS64.	
5	Firewall must support NAT policy for multicast traffic for both IPv4 and IPv6	
6	Firewall must support option to configure FQDN server rather then IP address in case server have dynamic IP address or site have multiple IP addresses for single domain.	
7	There must be option to even configure wildcard FQDN	

8	Firewall should allow policy based on port or service to protect attack at L3 not just application based policy which might be vulnerable to L3 attacks.	
9	Firewall must support Geo-based IP address blocking option.	
10	DNS translation option must be available in Firewall to change only the specific DNS reply from public to private IP. This is required for allowing user to access local resources using Private IP rather then there public IP address	
11	Build-in GUI/CLI must support option to configure firewall policy which allow packet capture for troubleshooting purposes	
12	The security appliance should be having configurable option to quarantine attack generating source address	
	Virtualization	
1	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided.	
2	Virtualization must be for every feature which are IPS , Application control, Antivirus/Anti-malware , URL filtering , SSL inspection , SSL VPN , IPSec VPN,, Traffic shaping and user authentication.	
3	Enabling Virtualization shouldn't require any kind of downtime or reboot. It must be done seamless even if the NGFW is live in the network.	
4	Global option of virtualized NGFW shouldn't take much of CPU and memory	
5	When creating virtualized NGFW it should give mode option to configure each virtualized system such as first system can work in NAT/route mode and second system can work in transparent mode.	
6	Each virtualized NGFW system must have option to configure various parameter to limit the resources utilization such as number of session , etc.	
	VPN Features	
1	NGFW must have build in support IPSec VPN and SSL VPN. There shouldn't be any user license restriction	
2	IPSec VPN must include gateway to gateway and gateway to client vpn. In case of gateway to client the administrator must have option to assign private IP address to remote user without requiring any additional license	
3	Route based IPSec VPN must be supported along with SD-WAN in case of two or more ISP's.	

4	IPSec VPN must include gateway to gateway and gateway to client vpn. In case of gateway to client the administrator must have option to assign private IP address to remote user without requiring any additional license	
5	IPSec VPN must support SHA-1 and SHA-2 (SHA 256, 386 and 512) along with DH group 2,5,14,15,16,17,18,19,20,21,27,28,29,30 and 31.	
6	SSL vpn must support high level algorithm along with TLS v1.2	
7	SSL/IPSec VPN must not have any user license and should have option to integrate with local AD and RADIUS server	
8	Both VPN must support 2-factor authentication with option to have locally imported tokens on the NFGW appliance itself , if required.	
	Intrusion Prevention System	
1	The IPS detection methodologies shall consist of:	
	a) Signature based detection using real time updated database	
	b) Anomaly based detection that is based on thresholds	
2	The IPS system shall have at least 7,000 signatures	
3	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available	
4	In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved	
5	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure IPv4 and IPv6 Rate based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/ port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding. Threshold settings must be customizable for different sources, destinations & services	
6	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident	
7	Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)	
	Antivirus	
1	Firewall should have integrated Antivirus solution	

2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on Firewall authenticated user groups with configurable selection of the following services:	
	a) HTTP, HTTPS	
	b) SMTP, SMTPS	
	c) POP3, POP3S	
	d) IMAP, IMAPS	
	e) FTP, FTPS	
3	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	
	Web Content Filtering	
1	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.	
2	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.	
3	The proposed system shall provide web content filtering features:	
	a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.	
	b) Shall include Web URL block	
	c) Shall include score based web keyword block	
	d) Shall include Web Exempt List	
4	The proposed system shall be able to queries a real time database of over millions+ rated websites categorized into 75+ unique content categories.	
5	Option to update local Database based on malicious category discovered by local Sandboxing solution from same vendor	
	Application Control	
1	The proposed system shall have the ability to detect, log and take action against network traffic based on over 4000 application signatures	
2	The application signatures shall be manual or automatically updated	
3	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions	
4	Application control and URL filtering must work independent of each other.	
	High Availability	

1	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component	
2	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.	
3	High Availability Configurations should support Active/Active or Active/ Passive	
	OEM should be having the following certifications/Ratings	
1	NGFW OEM should be EAL 4 certified	
	Cloud based Logging & Reporting Solution	
1	The solution should deliver complete security oversight with granular graphical reporting	
2	The solution should provide centralized security event analysis, forensic research, reporting, content archiving, data mining and malicious file quarantining.	
3	The solution should provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.	
4	The solution should analyze user traffic behaviour and identify compromised users/computers	
5	The solution should provide network event correlation to allow administrators to quickly identify and react to network security threats across the network.	
6	The solution should provide streamlined graphical network-wide reporting of events, activities and trends occurring on UTM / NGFW	
7	The solution should provide centralized logging of multiple record types including traffic activity, system events, viruses, attacks, Web filtering events, and messaging activity/data	
8	The solution be able to provide real-time and historical logs with filtering and search capabilities	
9	The solution should be able to displays a map of the world that shows the top traffic destination country by colour	
10	The solution should provide predefined templates for building / generating reports	
12	The solution should be able to support threshold values to generate alerts.	
13	The solution should be able to send alert emails	
14	The solution should be able to manually generate the report or schedule the same	
15	The solution should be able to generate report based on user names	

16	The solution should be able to store log for the minimum period of 1 Year	
17	The cloud solution should be able to store 800Mb logs per day	

Annexure 4

Proposed solution

Quoted make/model **Details of hardwar, and software, cloud specifications etc.**	**Website Link of the proposed item where the specification and datasheets are available**

Annexure – 5 FINANCIAL OFFER

(To be filled on company/firm letterhead)

1.Name of the Company/firm :

2. Address

3. Tel. No., FAX No. and E-mail address.

4. Contact Person

5. Rates as per the following Performa:

1. Rate of NGFW

SINO	Item	Unit Price	GST (%)	GST Amount	Total Price with GST
1	NGFW appliance (As per the specification)				
2	Cloud log storage and reporting				

Rates also include transportation charges, other incidental charges etc.

I hereby certify that the information furnished above is complete and correct to the best of our knowledge. We understand that in case found any deviation in the above statement occurs at any stage, the company will be black-listed and will not have any deal with CDS in future.

I certify that I have read the entire tender document and shall abide by the terms/conditions/clauses therein.

(Seal and Sign of Authorized Signatory)

Name: