

WEBSITE:[www.keralapsc.gov.in](http://www.keralapsc.gov.in)  
EMAIL:[jsrna.psc@kerala.gov.in](mailto:jsrna.psc@kerala.gov.in)



FAX : 0471 - 2553485  
Telephone : 0471-2546202  
0471-2546396

## KERALA PUBLIC SERVICE COMMISSION

No. RA I-(3) 50018 /2018-KPSC-Part(2)

Thiruvananthapuram,  
Dated: 29/07/2022

### E-TENDER NOTICE

Invitation of E-Tender for the supply and installation of **2(Two) numbers of Next Generation Firewall device and 6 (Six) numbers of 48 Port Access Switch** at the Online Examination Center, Kasaragod of the Kerala Public Service Commission.

E-Tender in one cover system is invited from competent dealers and manufacturers for the supply and installation of **2(Two) numbers of Next Generation Firewall device and 6 (Six) numbers of 48 Port Access Switch** in accordance with respective specifications as shown in Annexure I of the Tender document.

Sl No.	Item Details	Quantity (Nos)	Cost of Tender Forms	EMD
1	Next Generation Firewall Device	2	Rs.2,500/-	Rs.35,000/-
2	48 Port Access Switch	6	Rs. 720/-	Rs. 9,000/-

Tenders shall be submitted as e-tender through <https://etenders.kerala.gov.in>. Bidders who have enrolled in the above portal with their own digital signature certificate (DSC) can participate in the tender. For obtaining digital signature certificate (DSC) and necessary portal enrollment bidders can visit the above website. E-Tender document and other details can be obtained from the above e-portal.

Tender no. : 12/2022/SN  
Document download/sale start date : 03/08/2022  
Bid submission start date : 03/08/2022  
Document closing date : 17/08/2022 – 5.00 pm  
Date & Time of opening of tender : 19/08/2022 - 2.30 pm

Cost of e-Tender & EMD (Online payment):-

Payment as shown in the above table including EMD should be made as a single payment through online.

Dates upto which rates are to remain-firm for acceptance : 90 days

Performance security	:	5% of the contract value
Period of supply	:	within 20 days of supply order

The bidder desiring to take part in the bid shall log in to <https://etenders.kerala.gov.in/> and then select tender and initiate payment. Bidders will be directed to the online payment gateway page and they shall make payment as directed therein.

**The e-tenders submitted by the competent dealer should definitely contain a scanned and signed copy of the declaration of product offered to supply and dealership certificate from the manufacturer.**

Tenders will be opened in the online presence of each bidders or their authorized representatives who have logged in at the prescribed time of opening. If the date fixed for opening happens to be holiday or due to net failure the tenders will be opened in the next working day at the same time.

The price of the e-tender form will be received only through online payment methods stipulated in the website.

**Scanned copy of the agreement (Annexure II) in the prescribed format in Kerala Stamp paper worth Rs.200/- shall be submitted online and original shall be given to the Secretary, Kerala Public Service Commission before opening of e-tender.**

The rates should be quoted in Indian Currency only.

Details with respect to the e-tender and the details of specifications (Annexure I) of the item to be supplied can be obtained from the e-tender website <https://etenders.kerala.gov.in>.

The Secretary, Kerala Public Service Commission, Pattom will scrutinise the tenders received and will take necessary action for the award of contract.

The right of acceptance or rejection of any e-tender in full or in part without assigning any reasons thereof is reserved with the Secretary.

The rules and regulations prescribed for e-tenders by the Government of Kerala, shall be applicable to this e-tender also.

### **Terms and Conditions:**

1. The make, model, year of manufacture etc of the Firewall Device and network switch shall be clearly mentioned.
2. **Five years Comprehensive Onsite OEM warranty should be assured. Dealership/Authorization and Warranty Certificates from OEM shall be submitted with the tender. Dealership warranty will not be accepted.**
3. All charges, taxes, duties and levies should be clearly indicated.
4. The items should be supplied to the office of the Kerala public Service Commission,

- Pattom, Thiruvananthapuram-4 at the expense of the Tenderer.
5. The installation, commission and initial operation to the satisfaction of the KPSC will be the responsibility of the supplier.
  6. The payment will be made after completion of supply, installation and commission subject to the certification by our Technical Experts as to the quality and efficiency of the item supplied.
  7. In case of under performance during the warranty period, the item should be replaced and period of warranty will recommence from the date of replacement. Any legal disputes that may arise in relation to the e-tender formalities will be restricted to jurisdiction of Thiruvananthapuram District.

The communications should be addressed to :

The Secretary,  
Kerala Public Service Commission  
Pattom, Thiruvananthapuram  
Kerala-695004

SAJU GEORGE  
SECRETARY,

KERALA PUBLIC SERVICE COMMISSION

Note:- More details can be had from the office of **Additional Secretary, R&A wing, Kerala Public Service Commission, Pattom, Thiruvananthapuram-4**

#### ANNEXURE-1

#### Specification for Next Generation Firewall (NGFW)

Sl. No.	Description
General Requirements	
1	The Firewall must be appliance based, rack mountable and it should support 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 build in GUI and CLI to make on the go changes to Firewall Policies without any dependency to management and troubleshoot any issue related to network outage.
4	NGFW must support secure SD-WAN feature along with advance routing protocols such as BGP.
5	SD-WAN must be able to link and failover between various connections such as internet, MPLS, <b>leash</b> 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 combination of all 3 option 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 clear dashboard showing which links are down and which are up. This help 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 ISPlload-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 option to configure it separately if required.
13	Build-in GUI on the NGFW should have option to display logical topology of the network the NGFW is protecting. The display should also be able to give security recommendation for the NGFW.
14	Device should support Static routing, RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3 and BGP4+

### **Performance Parameters**

15	The solution should support a minimum of at least 2.5 Gbps IPS throughput & Minimum 1.5 Gbps NGFW throughput on real-world / enterprise mix traffic test condition.
16	The solution should support minimum 900 Mbps threat protection throughput on real-world / enterprise mix traffic test condition.
17	Should support 8 Gbps IPsec VPN throughput and 1500 Tunnels.
18	The Firewall must support at least 15,00,000 concurrent connections and 50,000 new sessions per second.
19	The platform must be having minimum of 12 interfaces with auto sensing 10/100/1000capability, 2 Gigabit SFP Ports and 2 10-Gb E SFP+Interfaces from day one.

### **Firewall Features**

20	Firewall policy should be single policy where all the feature get applied such as IPS, application control, URL, filtering, antivirus, SSL Inspection, logging and even NAT.
21	Firewall must support Zoning option along with User based authentication. It must have automatic option to group all the same zone policy.
22	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 emergency where management solution is no available and policy needs to be changed.
23	Firewall must support NAT46, NAT66, and NAT64 along with policy for such NAT along with option to configure DNS64.
24	Firewall must support NAT policy for multicast traffic for both IPv4 and IPv6.
25	Firewall must support option to configure FQDN server rather <b>then</b> IP address in case server have dynamic IP address or site have multiple IP addresses for single

	domain.
26	There must be option to even configure wildcard FQDN.
27	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.
28	Firewall must support Geo-based IP address blocking option.
29	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 than their public IP address.
30	Build – in GUI / CLI must support option to configure firewall policy which allow packet capture for troubleshooting purposes.
31	The security appliance should be having configurable option to quarantine attack generating source address
	<b>Virtualization</b>
32	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided.
33	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.
34	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.
35	Global option of virtualized NGFW shouldn't take much of CPU and memory
36	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.
37	Each virtualized NGFW system must have option to configure various parameter to limit the resources utilization such as number of session , etc.
	<b><u>VPN Features</u></b>
38	NGFW must have build in support IPSec VPN and SSL VPN. There shouldn't be any user license restriction
39	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
40	Route based IPSec VPN must be supported along with SD-WAN in case of two or more ISP's.
41	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
42	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.
43	SSL vpn must support high level algorithm along with TLS v1.2

44	SSL VPN must not have any user license and should have option to integrate with local AD or RADIUS server
45	Both VPN must support 2-factor authentication with option to have locally imported tokens on the NFGW appliance itself , if required.
	<b><u>Intrusion Prevention System</u></b>
46	The IPS capability shall minimally attain NSS LAB Certification
47	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
48	The IPS system shall have at least 7,000 signatures
49	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
50	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
51	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.
52	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
53	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)
	<b><u>Antivirus</u></b>
54	Firewall should have integrated Antivirus solution
55	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
56	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.

	<b><u>Web Content Filtering</u></b>
57	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
58	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.
59	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
60	The proposed system shall be able to queries a real time database of over millions+ rated websites categorized into 75+ unique content categories.
61	Update of local Database based on malicious category discovered by local Sandboxing solution from same vendor
	<b><u>Application Control</u></b>
62	The proposed system shall have the ability to detect, log and take action against network traffic based on over 4000 application signatures .
63	The application signatures shall be manual or automatically updated .
64	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions
65	Application control and URL filtering must work independent of each other.
	<b><u>High Availability</u></b>
66	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component .
67	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.
68	High Availability Configurations should support Active/Active or Active/Passive
	<b><u>OEM should be having the following certifications/Ratings</u></b>
69	Firewall module should be ICSA Labs certified
70	Gateway Antivirus should be ICSA Labs certified.
	<b><u>Warranty</u></b>
71	5 year OEM warranty/subscription for Hardware, Application Control, IPS Services, Malware Protection, Antivirus, Botnet, CDR and Virius Outbreak Protection

	<b><u>MAF</u></b>
72	Manufacturer Authorization Required

### **48 port Network switch - 6 No.s**

Sl. No.	Specification
	<b><u>General Requirements</u></b>
1	Managable switch should have minimum 48x GE RJ45 ports and 4x 10 GE SFP + ports
2	Proposed switch should have a RJ-45 Serial console port
3	The form factor of the proposed switch should be 1 RU Rack-Mount Appliance
4	Switching capacity of the proposed switch should be minimum 170 Gbps
5	Packet per second capacity of the switch should be minimum 250 Mpps
6	Proposed Switch should support minimum 30 K MAC address storage
7	Proposed switch should support 1000 VLANs
8	Should support min DRAM-512 MB DDR3, maximum to be specified
	<b><u>Layer 2 Requirements</u></b>
9	Should support Jumbo frames and link auto-negotiation
10	Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root & BPDU Guard
11	Should support Edge Port / Port Fast
12	IEEE 802.1AX Link Aggregation
13	IEEE 802.1q VLAN tagging, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, DHCP-Snooping
14	should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
15	Should support IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z , 1000Base-SX/LX, IEEE 802.3ab 1000Base-T
	<b><u>Authentication Requirements</u></b>
16	Admin Authentication Via RFC 2865 RADIUS
17	Should support 802.1x port-based authentication
18	Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB)
19	Should support IEEE 802.1x Guest and Fallback VLAN
20	Should support IEEE 802.1x Dynamic VLAN Assignment
21	Switch should support local user database and can integrate with LDAP,



	RADIUS, TACACS+ servers
	<b><u>Management</u></b>
22	Should support Telnet,SSH, HTTP,HTTPS with IPv4 and IPv6 Management
23	Switch should support SNMP v1, v2c and v3
24	Software download/upload: TFTP/FTP/GUI
25	Proposed switch should be managed via both, GUI and CLI
	<b><u>Central Management</u></b>
26	Should be ready to integrated with switch controller which offers visibility, user access control, and threat mitigation to quarantine automatically on the compromised host at the switch port level. If bidder not supported they should include switch controller with required hardware and license in the quotation.
27	Should support centralized security management, configuration and reporting through a single console from switch controller or from external NMS
28	Should have option to create switch profiles to allow specific settings to be applied to all authorized Switches.
29	Proposed switch should be managed by switch controller for performing the following configurations. VLAN, POE Control, RSTP/MSTP, 802.1x Authentication, Syslog Collection , Device Detection, Host Quarantine on Switch Port, QoS, Radius accounting(COA) and Centralized Firmware Management through this single pane of glass.
30	Centralized management should show the network topology of all managed switches through a single console
	<b><u>Environment</u></b>
31	Power Required :100–240V AC, 50–60 Hz
32	Operating Temperature : 32–104°F (0–40°C)
33	Humidity : 10–90% non-condensing
	<b><u>Certifications</u></b>
34	FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2
	<b><u>Warranty</u></b>
35	5 year comprehensive OEM warranty required
	<b><u>MAF</u></b>
36	Manufacturer Authorization Required