WEBSITE:www.keralapsc.gov.in
EMAIL:jsrna.@psc.kerala.gov.in
FAX : 0471 - 2553485
Telephone : 0471-2443068

KERALA PUBLIC SERVICE COMMISSION

No. R&A I (3) 50018/2018/KPSC (1)

Thiruvananthapuram,
Dated:17/01/2020

E-TENDER NOTICE

Invitation of E-Tender for the supply and installation of **2(Two) numbers of Next Generation Firewall device** at the offices of the Kerala Public Service Commission, pattom, Thiruvananthapuram.

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** 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.1,520/-	Rs.19,000/-

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.	: 6/2020/SN
Document download/sale start date	: 18/01/2020
Bid submission start date	: 18/01/2020
Document closing date	: 03/02/2020 – 5.00 pm
Date & Time of opening of tender	: 05/02/2020 - 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 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 Product should be supplied within 20 days from the date of Purchase Order, otherwise the tender will be cancelled without any prior intimation.**
6. The installation, commission and initial operation to the satisfaction of the KPSC will be the responsibility of the supplier.
7. 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.
8. 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 or external redundant Power Supply.
2	The proposed Firewall Vendor should be in the Leaders 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, leased 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 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 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	
1	The solution should support a minimum of at least 450 Mbps IPS throughput & minimum 350 Mbps NGFW throughput on real-world / enterprise mix traffic test condition.
2	The solution should support minimum 200 Mbps threat protection throughput on real-world / enterprise mix traffic test condition.
3	Should support 2 Gbps IPSec VPN throughput and 1500 Tunnels.
4	The Firewall must support at least 1,500,000 concurrent connections and 30,000 new sessions per second.
5	The platform must be having minimum of 12 interfaces with auto sensing 10/100/1000 capability and 2 Gigabit SFP ports.
Firewall Features	
1	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.
2	Firewall must support Zoning option along with User based authentication. It must have 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 emergency where management solution is not available and policy needs to be changed.
4	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 than 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 than 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 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.
5	SSL vpn must support high level algorithm along with TLS v1.2.
6	SSL VPN must not have any user license and should have option to integrate with local AD or RADIUS server.
7	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 capability shall minimally attain NSS Certification
2	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
3	The IPS system shall have at least 7,000 signatures
4	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.
5	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.
6	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.
7	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 an alert and logging the incident.

8	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	Update of 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	Firewall module should be ICSA Labs and EAL 4 certified

2	Network Intrusion Prevention System (NIPS) and should be ICSA Labs certified.
Warranty	
1	**Five years comprehensive Onsite OEM Warranty (should also specify in MAF) from the date of invoice, including subscription of App Ctrl, IPS, AV, Web Filtering, Anti-spam, FSA Cloud, Security Rating, SD-WAN Cloud Assisted Monitoring, SD-WAN Overlay Ctrl VPN, FMG/FAZ Cloud, Industrial Security.**
MAF	
1	Manufacturer Authorization Required.