Rajiv Gandhi Center for IT Development and e-Governance (Construction, Maintenance & Operation)

Annexure- B

Clarifications for

Specifications

After Pre-Bid meeting dated 15-MAY-2023

Department of Information Technology & Communication
Government of Rajasthan
IT Building, Yojana Bhawan, Tilak Marg, C-Scheme Jaipur, Rajasthan
302005

Contents

1. Specification of Electrical Panel Multi-Function Meter

1.1.1. Multi-Function Meter

Providing & Fixing of IS: 13875 & IEC :61326 confirming LED Digital type Multi Function Meter of class 1 accuracy as per IS : 1248 including making connection by PVC insulated copper conductor with PVC sleeves / channel etc. as required. All as per pre approved by Engineer in charge. For additional technical parameters of products/ work, refer Annexure "A" attached with Rajasthan PWD BSR 2022.

1.1.1.1. Multi-Function Meter: Type - M1

The multi-function meter should be able to measure the following electrical parameters:

Three phase with universal Auxiliary supply + AMP + HZ + PF + KW + KVA + KVAR + KVARH + KWH + DUAL ENERGY+ ENERGY+THD-I, THD-V & RUN HRS + MD with RS485

1.1.1.2. Multi-Function Meter: Type – M2

The multi-function meter should be able to measure the following electrical parameters:

Three phase AMP + HZ + PF + KW + KVA + KVAR + KVARH+KWH+ ENERGY+THD-I, THD-V & RUN HRS with RS485.

1.1.1.3. Multi-Function Meter: Type – M3

The multi-function meter should be able to measure the following electrical parameters:

Three phase AMP+HZ+PF+KW+KVA+KVAR+T.ENERGY+THD-I, THD-V & RUN HRS

Ankita Srivastava
Assistant Engineer, Civil
RISL

2. Specification of Firewall Type-2

Sr. No.	Features	Specifications	Compliance (Yes/No)
1	**3rd Party Test Certification**	The proposed vendor must have "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall comparative Test Report.	
2	**Equipment Test Certification**	ICSA, FCC Class B, CE Class B, VCCI Class B and CB Certified	
3	**Architecture**	The proposed NGFW solution 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, CC#), 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).	
		The proposed firewall must have min 4 physical cores with x86 processor and not an ASIC based solution	
		The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities	
4	**Storage**	The NGFW appliance should have minimum on-board 128 GB capacity	
5	**Interface Requirement**	Min 8 x 1 Gig Copper interfaces of which 4 ports will be POE and 2*1G SFP/RJ45 Combo Ports from day 1 with relevant SR transceivers	
6	**Performance Capacity**	A Minimum NG Firewall application control throughput in real world/production environment/Application Mix – minimum 2.5 Gbps with Application-ID/Application Control and Logging enabled utilizing 64 KB HTTP transactions. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.	

Sr. No.	Features	Specifications	Compliance (Yes/No)
		Minimum NG Threat prevention throughput in real world/production environment (by enabling and measured with Application-ID/AVC, User-ID/Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti Malware,DNS Security, File Blocking, sandboxing and logging security threat prevention features enabled – minimum 1 Gbps utilizing 64 KB HTTP Transactions. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.	
		IPsec VPN throughput – 1.5 Gbps or more	
		New Layer 7 sessions per second – Min 35K	
		Concurrent Layer 7 sessions – Min 200K	
7	**High Availability**	Active/Active and Active/Passive	
8	**Interface Operation Mode**	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in:	
		- Tap Mode	
		- Transparent mode (IPS Mode)	
		- Layer 2	
		- Layer 3	
9	**Next Generation Firewall Features**	The proposed firewall shall have native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.	
		The proposed firewall shall be able to handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP	
		The proposed firewall should have the ability to create custom application signatures and categories directly on frewall without the need of any third-party tool or technical support. Also the device should have capability to provide detailed information about dependent applications to securely enable an application	
		The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration	
		The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment	
		The proposed firewall shall delineate different parts of the application such as allowing Facebook	

Amrit Srivastava
Assistant Engineer, Civil
RISL

Sr. No.	Features	Specifications	Compliance (Yes/No)
		chat but blocking its file-transfer capability inside the chat application base on the content.	
		The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.	
		Solution should be have machine learning capabilities on the dataplane to analyze web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.	
10	**Threat Protection**	Should have protocol decoder-based analysis which can statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits	
		Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.	
		Should block known network and application-layer vulnerability exploits	
		The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures	
		The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour	
		All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS or AV engines.	
		Should be able to perform Anti-virus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, reset, alert etc	
		Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs	
		Shoud suppot inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT) values and drop the packet based on Zone Protection profile	

Sr. No.	Features	Specifications	Compliance (Yes/No)
		The device shojld support zero day prevention by submitting the executable files and getting the verdict back in five minutes post detection.	
		The device should have protection for at least 20000 IPS signatures	
		Should have. threat prevention capabilities to easily import IPS signatures from the most common definition languages Snort and Suricata	
		The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned	
		Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data	
		Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service	
		The NGFW should have native protection against credential theft attacks(without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the folowing :	
		· Automatically identify and block phishing sites	
		· Prevent users from submitting credentials to phising sites	
		· Prevent the use of stolen credential	
11	**Advanced Persistent Threat (APT) Protection**	There should be provision to enable the APT solution if required with following features. This should be provision for both on-premise and cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than 5 minutes.	
		Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment	
		Cloud base 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	
		The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required using hybrid setup.	

Sr. No.	Features	Specifications	Compliance (Yes/No)
		The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.	
12	**Network Address Translation**	The proposed firewall must be able to operate in routing/NAT mode	
		The proposed firewall must be able to support Network Address Translation (NAT)	
		The proposed firewall must be able to support Port Address Translation (PAT)	
		The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6 or equivalent)	
		Should support Dynamic IP reservation, tunable dynamic IP and port oversubscription	
13	**Routing and Multicast support**	The proposed firewall must support the following routing protocols:	
		- Static	
		- RIP v2	
		- OSPFv2/v3 with graceful restart	
		- BGP v4 with graceful restart	
		The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address	
		The firewall must support VXLAN Tunnel content inspection	
		The firewall must support DDN sprovides such as DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org, and No-IP.	
		The proposed firewall must have support for mobile protocols like GTP, SCTP and support for termination of GRE Tunnels	
		The device should support load balancing of traffic on mnultiple WAN links based on application, latency, cost and type.	
		The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	

Srivastava
Engineer. Civil

Sr. No.	Features	Specifications	Compliance (Yes/No)
		The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services	
		PIM-SM, PIM-SSM, IGMP v1, v2, and v3	
		Bidirectional Forwarding Detection (BFD)	
14	**DNS Security**	The Solution should support DNS security in line mode and not proxy mode.	
		Solution should have database maintenance containing a list of known botnet command and control (C&C) addresses which should be updated dynamically.	
		DNS Security should provide predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control	
		DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future considerations	
		It should have prevention against new malicious domains and enforce consistent protections for millions of emerging domains.	
		The solution should support integration and correlation to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Integrate.with URL Filtering to continuously crawl newfound or uncategorised sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots. Should take inputs from at least 25 third-party sources of threat intelligence.	
		Should support simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.	
		Solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection	

Amita Srivastava
Assistant Engineer, Civil
RISL

Sr. No.	Features	Specifications	Compliance (Yes/No)
		The solution should have capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain.	
		The solution should have support for dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink-holing malicious domains to cut off Command and control and quickly identify infected users.	
15	**URL Filtering Capabilities**	NGFW should protect against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding based attacks.	
		NGFW should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use	
		NGFW should support policy creation around end user attempts to view the cached results of web searches and internet archives.	
		NGFW should have a vast categorisation database where websites are classified based on site content, features, and safety in more than 60 benign and malicious content categories.	
16	**SDWAN Features**	Link metric collection, jitter, drop, delay Intelligent path selection based on metric; dynamic application steering Application and network condition aware sub-second steering Session-based link aggregation Predefined application thresholds for common application categories	
17	**SDWAN Management**	Monitoring and Visualization Dashboard view of SD-WAN impacted applications and links with drill down SD-WAN link down alerts to detect black out situation SD-WAN reporting Link jitter, delay, and drop trend charts	
18	**Authentication**	Solution should support the following authentication protocols:	
		- LDAP	
		- Radius (vendor specific attributes)	
		- Token-based solutions (i.e. Secure-ID)	
		- Kerberos	
		The proposed firewall's SSL VPN shall support the following authentication protocols	
		- LDAP	

Sr. No.	Features	Specifications	Compliance (Yes/No)
		- Radius	
		- Token-based solutions (i.e. Secure-ID)	
		- Kerberos	
		- SAML	
		- Any combination of the above	
19	**Authorization**	Original Manufacturer Authorization Certificate to be submitted along with the bid. We reserves the right to reject in case deviation on the basis of technical compliance as submitted in the tender document.	
20	**Support & Warranty**	OEM should proposed with 5 Years OEM support bundle with 24x7x365 days TAC support, RMA(There should be at least 4 RMA dept and one TAC for support in India), software updates and subscription update support. The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, Anti Virus , Anti Spyware, Advanced APT protection, URL filtering, DNS Security and SDWAN features as mentioned above bundled .	

Amita Srivastava
Assistant Engineer, Civil
RISL

3. Other revisions

S.No.	RFP Volume Name and Number	RFP Page No.	RFP Rule No.	Earlier Rule Detail	Revised Rule
1	Volume II	RFP Vol-II Page No. 395	14. Technical Specifications of Uninterrupted Power Supply (UPS) System > 14.3. Scope > 2. Specification / features of the Each UPS system are as follows:	**Features of the Each UPS system are as follows -> xv)** Inbuild Isolation Transformer	**Features of the Each UPS system are as follows -> xv)** Inbuild or external Isolation Transformer also accepted
2	Volume II	RFP Vol-II Page No. 395	18. IOS Summary	**Soft Integration (SI) for access control and automation light -> 0 Nos.** , SI Points ->1116 nos and Total IO points -> 1896 Nos.	**Soft Integration (SI) for access control and automation light ->** 500 Nos. , SI Points ->1616 nos and Total IO points -> 2396 Nos.