MAHARASHTRA STATE WAREHOUSING CORPORATION

(A Government Under taking)
583/B, Market Yard, Gultekadi, PUNE-411 037
Tel. 020-24206800
Website: www.mswarehousing.com, Email: - info@mswc.in
GST No. 27AABCM3988M1ZT

NO. MSWC/Computer/Pur_Firewall/36A Date:- 20.02.2025

To:

Subject: Quotation for purchase of Firewall at MSWC Head office, Pune.

Sir,

The Maharashtra State Warehouse Corporation is inviting sealed quotation for purchase of server at Firewall at MSWC Head office, Pune in below configuration.

Sr. No.	Particular	Qty	Basic Rate in Rs	GST %	GST Amt in Rs	Total
1	2	3	4	5	6 = 4 x 5%	7 = 4 + 6
1	Hardware Firewall as per attached minimum specifications	1				
2	Network Protection, Web Protection, Enhanced Support, Zero-Day Protection, Central Orchestration for 36 months validity	1				
	Grand Total					

Terms and Conditions-

1. The vendor should have Maharashtra based office (enclose the proof of the same along with quotation i.e. GST Cert.
2. Supplier should enclose following documents along with quotation letter. without these documents quotation will not be treated as valid.
    1. Company PAN Card & GST Certificate
    2. Authorised Service partner/dealer/ Manufacturer certificate.
    3. Bank details along with IFSC code on company letter head
    4. Details of product specification, model number, brochure as per OEM and deviation statement if any with minimum specification attached with this quotation.
3. Price: The rate should be inclusive of taxes, installation and support for warranty period. The percentage of tax should be indicated separately in the invoice along with HSN/SAC Code.

4. Delivery and installation: Delivery and installation of firewall along with network configuration should be done within one month from the date of this purchase order.

5. Warranty – Three years onsite comprehensive warranty with 4 Hrs SLA from the date of installation.

6. Security Deposit: The successful party will have to pay Security Deposit @ 5% of total cost of purchase order in MSWC by online transfer, which will be refunded after warranty period. The MSWC Bank details for the same will be communicate to the successful party separately.

7. Payment: 80 % payment will made after delivery and submit delivery challan after sign of appropriate person of MSWC, submission of security deposit and signing of Agreement with MSWC. Balance 20% payment will be made after installation and configuration of firewall at MSWC and submitting the installation report along with serial number and proof of warranty registration on OEM website.

8. Successful party to entre in an agreement with MSWC for this work on required stamp paper within 15 days from the date of work order.

9. Support- The successful party should give onsite for firewall for configuration for the period of 3 years.

10. MSWC reserves the right to accept or reject any offer without assigning reason thereof.

The sealed quotation should be addressed to the Programmer within following dates and should be superscripted with “QUOTATION FOR FIREWALL”

Thanking You,

Quotation Date

Quotation submission date – From 20.02.2025 to 03.03.2025 up to 2.00 pm

Last date of quotation – 03.03.2025 up to 2.00 pm.

Quotation opening date – 03.03.2025 up to 5.00 pm.

Encl – Firewall minimum Specifications

Firewall minimum Specifications

S.No	Firewall minimum specifications	Specification of supplied product
1	Solution should be 1U rack mountable appliance with meeting 35 Gbps or above firewall throughput, 7 Gbps or above IPS throughput, 6 Gbps or above NGFW throughput, 5 Gbps threat protection throughput, 6 million or above concurrent session, 145k or above new connections per second, IPsec VPN throughput of 20 Gbps or above.	
2	Hardware should have at least 8 Ports RJ45, 2 x SFP fiber* interfaces and additional 1 Flexi Port slot, 1 RJ45 management port, 1 Micro-USB management port, inbuilt 120 GB or above SSD storage and 12 GB or above RAM.	
3	Hardware should have Multiple processors to offload resources to coprocessor for better performance.	
4	Solution should have GUI/CLI based management console, Role-based administration, user threat level mapping, cloud application usage visibility.	
5	Solution should have SDWAN routing based on jitter/latency/packet loss, reporting analyzer function, ability to identify risky users based on browsing behaviour, integration provision with managed services, IPv6 certified, malicious file reports with screenshot and dashboard file release capability.	
6	Solution should provide TLS inspection offers high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade policies.	
7	Solution should support SD-WAN providing performance-based link selection based on SLA profile with Jitter / Latency / Packet Loss with zero-impact re-routing, SD-WAN monitoring, multi-site SD-WAN orchestration tools, and FastPath acceleration of IPsec VPN tunnel traffic. And same should be demonstrated by OEM/Vendor in post bid POC if required.	
8	Solution should support Static Routing, BGP, BGPv6 and OSPFv3 routing.	
9	Solution should have the provision to configure TLS-encrypted syslog.	
10	Solution should have Self-service user portal, API for 3rd party integration	
11	Solution should have two-factor authentication (One-time-password) support for administrator access, user portal, IPsec and SSL VPN. 200	
12	Solution should support the High Availability (HA) of two devices in active-passive and active- active mode from day 1.	
13	Solution should have on-appliance or external reporting storage to store logs and historical reports.	
14	Solution should provide 1000+ types of reports including bandwidth usage, application usage, web usage, firewall, ATP, geo-activity, IPS, Zero Day Threat Protection and compliance reports.	
15	Solution should have a centralized management to manage multiple firewall appliances from day 1.	
16	Solution should have SNMP v3 and Netflow support.	
17	Solution should have the configuration option to block sign-in for all types of authentications, such as the web admin console, CLI, or VPN. Administrator should be provided with an option to enter the maximum number of failed sign-in attempts and the duration (in seconds) within which the attempts can be made from a single IP address. Therefore, when the failed attempts exceed the number, the administrator is locked for the configured minutes. Administrator must be provided with the configuration option to specify the number of minutes for which the administrator will not be allowed to sign-in.	

18	Solution should provide administrator with option to use name lookup to query the domain name service for information about domain names and IP addresses. The option shoukd be able to send a domain name query packet to a configured domain name system (DNS) server.	
19	Solution should provide administrator with an option to use packet capture showing the details of the packets that pass through an interface.	
20	Solution should help administrator in tracing the path taken by a packet from the source system to the destination system. The output shows all the routers through which data packets pass from the source system to the destination system, maximum hops, and total time taken by the packet to return (measured in milliseconds).	
21	Solution should provide administrator with the ability to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.	
22	Solution should have the ability to sends the Netflow records of source,destination, and traffic volume to the Netflow server. The records help administrator to identify the protocols, policies, interfaces, and users consuming high bandwidth. Administrator thus can use data analysis tools, such as Open Source Data Analyzer and PRTG to generate reports from the Netflow records.	
23	Solution should have the ability to configure a mail server and email settings to send and receive alert emails.	
24	Admin user interface should provide the ability to synchronize the clock on the firewall with predefined or custom Network Time Protocol (NTP) servers.	
25	Appliance should support syslog protocol and ust have the capability for collecting and forwarding messages from firewall module to a server running a syslog daemon.	
26	Solution should provide administrator with an option to add certificates and generate a locally-signed certificate or certificate signing request (CSR). Administrator can also add certificate authorities (CA) and certificate revocation lists (CRL).	
27	Solution should have ability to define policies to block traffic to high-risk applications. New applications should be automatically added to application filters and firewall rules when the application signature database is updated.	
28	Appliance syslog protocol should be compliant to RFC5424.	
29	Solution should have the ability to specify protection on a zone-specific basis and limit traffic to trusted MAC addresses or IP–MAC pairs.	
30	Solution should support VoIP using both Session Initiation Protocol (SIP) and H.323 standards.	
31	Solution should support QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared.	
32	Solution should have fully transparent proxy for anti-malware and we filtering and X- Forwarded-For Header support for up-stream load balancers and proxies.	
33	Solution should have group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group.	
34	Solution should be stateful deep packet inspection firewall.	
35	Solution should have the provision to enforce policy across zones, networks, or by service type.	
36	Solution should have ability for detecting and blocking network traffic attempting to contact command and control servers.	

37	Solution should inspect executables and documents containing executable content (including.exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of thefile types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)	
38	Solution should have Machine Learning technology with Deep Learning scans all dropped executable files. And In-depth malicious file reports and dashboard file release capability.	
39	Solution should have the ability to create user, group, time, or network-based policies.	
40	Solution should have the ability to create access time polices per user/group.	
41	Solution should support Site-to-site VPN: SSL, IPsec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key. Solution should support RB-VPN.	
42	Solution should support 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.	
43	Appliance should have jumbo frame support.	
44	Appliance should support 802.3ad interface link aggregation.	
45	Solution should have the ability to set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical.	
46	Solution should have Flexible network or user-based traffic shaping (QoS) with control based on Surfing Quota, Network Traffic Quota and Time-based Access. And should support DSCP marking.	
47	Solution should have zero-impact re-routing maintains application sessions when link performance falls below thresholds and a transition is made to a better performing WAN link.	
48	Solution should have SD-WAN load balancing across multiple SD-WAN links with round-robin weighting or session persistence strategies.	
49	Cloud Orchestration should have wizards for easy and quick creating of VPN Tunnels.	
50	Solution should have a centralized management platform (On-prim/Cloud) to manage 50 or more Firewall appliances.	
51	Centralized management and reporting solution should be in India in case of cloud management platform.	
52	Solution should support 3rd party threat feeds integration to automatically block traffic based on the IPv4 addresses, domains, and URLs listed from third-party threat feeds.	
53	Solution should include **3 years subscription** of NGFW-IPS-Gateway Anti Virus-Zero Day Protection- Sandbox-ATP, VPN and two-factor authentication provision for 200 users including appropriate licenses if applicable.	
54	OEM/Equipment should have Common Criteria EAL4+ Certification, IPv6 Ready Logo Program Approved List, ISO 27001:2022 or above certificate, TEC MTCTE Certification. Failure to submit certifications will deem bid disqualified.	
55	Bidder must submit publicly available reference documents for proposed solution like appliance datasheet, features list and device specifications. Any reference documents that are not available publicly won't be accepted.	
56	Bidder must submit publicly available cross reference link for each technical specifications mentioned in compliance document	
57	Firewall should have **3 years** licenses, advanced replacement warranty & 24/7 OEM online support.	
58	OEM Support Escalation Matrix to be attached in bid.	