# HIGH COURT OF MADHYA PRADESH: JABALPUR

## // CLARIFICATION //

**No. Reg(IT)(SA)/2024/1455 Jabalpur, Dated: 03.10.2024**

**Sub:- Clarifications /reply of pre-bid meeting dated: 12th September, 2024 regarding the "Supply, Installation, Commissioning, Maintenance of Firewall, WAF with Server Load Balancer and Network Monitoring System for the High Court of Madhya Pradesh" with reference to tender no. Reg(IT)(SA)/2024/1263, dated: 22.08.2024.**

**Ref:- Pre-Bid Meeting dated: 12th September, 2024.**

## Reply / clarification to the pre-bid queries

On the basis of queries submitted by the bidders, the detailed reply /clarifications are prepared and the same is enumerated as per details given below for all prospective bidders:-

| Query No. | RFP Reference (Section No. /Page No.) | Content of RFP Requiring Clarifications | Query of the bidders / Remarks of the bidders | Reply / clarifications to the query /Remarks by the High Court. |
|---|---|---|---|---|
| | | | **1. M/s Atishay** | |
| 1 | Section No. 2.15.2 (ii) Page No. 10 | Experience in Supply, Installation, commissioning, Maintenance of firewall, WAF, NMS tool and similar IT equipments during last 05 year sending last day of month previous to the month of publication of | Bidder /OEM Experience in Supply, Installation, commissioning, Maintenance of firewall, WAF, NMS tool and similar IT equipments during last 05 years ending last day of month previous to the month of publication of this tender, should be either of the following :-<br>(a) Three similar completed work costing not less than the amount equal to 40% of the estimated cost.<br>**OR**<br>(b) Two similar completed work costing not less than the amount equal to 50% of the estimated cost. | No change. |

| | | | | |
|---|---|---|---|---|
| | | this<br>tender, should be either of the following :-<br>(a) Three similar completed work costing not less than the amount equal to 40% of the estimated cost.<br>OR<br>(b) Two similar completed work costing not less than the amount equal to 50% of the estimated cost.<br>OR<br>(c) One similar completed work costing not less than the amount equal to 80% of the estimated cost.<br>Similar works means: Supply, installation and System Integration of firewall, WAF, NMS tool and similar IT equipments. . | **OR**<br>(c) One similar completed work costing not less than the amount equal to 80% of the estimated cost.<br>Similar works means: Supply, installation and System Integration of firewall, WAF, NMS tool and similar IT equipments.<br>Justification: The revised clause broadens the scope to include all relevant suppliers and integrators who have demonstrated expertise in the supply and installation of key IT systems such as servers, computers, printers, and UPS systems, thereby promoting a fairer and more competitive tendering process. | |
| **2. M/s Check Point Software Technologies(I) Pvt. Ltd.** | | | | |
| 1 | Section – VII/Specifications – A/3-Interface and Connectivity Requirement /Page-32 | 6 X 10G Copper/RJ45 Day 1 | **Please change to:** "8 X 1G Copper/RJ45 Day 1". **Justification:** We support 1G Copper/RJ45 ports as is the industry norm. 10G RJ45 ports are rarely used & in this context point to a specific OEM. | Please refer the revised specifications given below. |
| 2 | Section – VII/Specifications – | 8 X 1/10G SFP/SFP+ Day 1 with LR/SM | **Please change to:** "4 X 1/10G SFP/SFP+ Day 1 with 10G LR/SM transceivers and 8x3m patch cords." | Please refer the revised specifications |

| | | | | |
|---|---|---|---|---|
| | A/3-Interface and Connectivity Requirement/Page-32 | transceivers and 8x3m patch cords. | **Justification:** Our appliance supports 4 Fiber ports which should be sufficient for the customer needs for present & future & hence should be allowed for wider participation | given below. |
| 3 | Section – VII/Specifications – A/3-Interface and Connectivity Requirement/Page-32 | 4X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one | **Please change to:** "2X 40/100G QSFP28 Ports with 2 nos. of LR transceivers and 4x3m patch cords from Day one**"** **Justification:** As discussed in pre bid meeting its better to invest in 40G/100G ports from a future scalability perspective rather than 25G. As 10G porsa are already provide above, need to change this clause into 40G/100G port. | Please refer the revised specifications given below. |
| 4 | Section – VII/Specifications – A/3-Interface and Connectivity Requirement/Page-32 | Minimum 2 x 10G HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management Port | **Please change to:** "Minimum 1 x 1G RJ45 HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management Port" **Justification:** 1 HA port is required for this purpose-2nd port is redundant. Hence please allow the change required for wider Participation. | Please refer the revised specifications given below. |
| 5 | Section – VII/Specifications – A/3-Interface and Connectivity Requirement/Page-32 | Should have support 2x40/100G for future use. | **Justification:** Please remove this clause as 40G/100G ports can be provided against 10/25G ports as mentioned above. While our appliance supports 2x40/100G, one set of 10/25 card needs to be replaced. This future requirement blocks our participation & hence request to allow changes. | Yes removed. |
| 6 | Section – VII/Specifications – A/4-Hardware Architecture /Page-32 | The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution | **Please change to** "The firewall should have integrated redundant fan and dual redundant power supply to remove any single point of failure in the solution".<br>**Justification:** Hot swap feature not available on this category of Firewalls in our portfolio. Please remove for participation | Please refer the revised specifications given below. |
| 7 | Section – VII/Specifications – A/5- | The NGFW throughput of the firewall should be a minimum | **Please change to** "The NGFW throughput of the firewall should be a minimum **30** Gbps with application identification and firewalling enabled | No change. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Performance& Scalability /Page-32 | 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be **11** Gbps."<br>**Justification:** Higher no of NGFW throughout is must to ensure higher IPS performance whereas minor change is needed in Threat Prevention throughput for wider participation. |  |
| 8 | Section –VII /Specifications – A /5-Performance& Scalability /Page-32 | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions | **Please change to:** "NGFW Firewall should support at least 1,400,000 Layer 7 Concurrent sessions /connections"<br>**Justification:** Checkpoint Firewalls are tested for performance in terms of the number of concurrent connections which are accessing instead of the sessions. Request to include both sessions/connections to allow participation. | No change. |
| 9 | Section –VII/Specifications –A/6-Next Gen Firewall Features/Page-33 | Firewall should support creating security policies with source /destination zones, network subnets/ranges, and relocation objects, ports /protocols, applications, user /group attributes, URL /URL categories and actions on traffic. The actions on the traffic should be to allow, alert, block, block and continue, reset. | **Please change to:** "Firewall should support creating security policies with source/destination zones, network subnets/ranges, geo location objects, ports/protocols, applications, user /group attributes, URL/URL categories and actions on traffic. The actions on the traffic should be to accept, drop, ask, inform, reject, user auth, client auth. The firewall should provide time based polices with options for recurring schedule or one time schedule."<br>**Justification:** What are relocation objects? It seems to be an OEM specific term- Can we change it to geo location objects? Also, for actions, we support accept, drop, ask, inform, reject, user auth and client auth options which provide the same functionality but have different | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | The firewall should provide time based polices with options for recurring schedule or one time schedule. | terminology. Please allow both set of terms for wider participation | |
| 10 | Section – VII /Specifications – A /6-Next Gen Firewall Features /Page-33 | The firewall should supports NAT's like source NAT, destination NAT, U-Turn NAT. Firewall should support Nat66, Nat 64 or Nat46 functionality | **Please change to:** "The firewall should supports NAT's like source NAT, destination NAT , U-Turn /Hairpin/Loopback NAT. Firewall should support Nat66, Nat 64 or Nat46 functionality".<br>**Justification:** Please note that U-Turn NAT is an OEM specific terminology, which is also known as Hairpin NAT and Loopback NAT used by other OEMs, providing same functionality. Request to change to U-Turn/Hairpin/Loopback to allow participation. | Please refer the revised specifications given below. |
| 11 | Section –VII /Specifications – A /6-Next Gen Firewall Features /Page-33 | Should support capability to create multiple virtual context /instances with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context /instance | **Please change to:** "Should support capability to create multiple virtual context/instances"<br>**Justification:** In providing strict hardware resource reservations, it is not a recommended architecture. Instead, system architecture should be flexible enough to manage any increase or decrease in load and efficiently utilize hardware resources. Hence request to change the specs as suggested. | Please refer the revised specifications given below. |
| 12 | Section –VII /Specifications – A /6-Next Gen Firewall Features/Page-33 | The solution should be able to provide contextual information about the hosts and the network subnets present such that the admins are able to capture all the required information and build the security profiles based | **Please change to:** "The solution should be able to provide contextual information about the hosts and the network subnets present such that the admins are able to capture all the required information and build the security profiles based on the details shown on the solution. The details captured should consist of the following: IOC's, IP address, Applications, Ports & protocols, vulnerabilities etc."<br>**Justification:** While the solution provides detailed information about the hosts and network subnets, | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | on the details shown on the solution. The details captured should consist of the following: IOC’s, MAC addresses, IP address, Applications, Ports & protocols, vulnerabilities etc. | capturing IOC's, IP address, applications, ports and protocols, vulnerabilities, it is not recommended to capture MAC addresses as it is a legacy way of managing security. Request to remove the same. | |
| 13 | Section – VII/Specifications – A/6-Next Gen Firewall Features/Page-33 | Should support more than 19,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's. | **Please change to:** "Should support more than 15,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's.<br>**Justification:** Checkpoint supports more than 15000 IPS signatures which is more than enough to combat known threats. | Please refer the revised specifications given below. |
| 14 | Section – VII/Specifications – A/6-Next Gen Firewall Features/Page-34 | The solution should provide traffic hit count, Rule Conflict Detection (Redundant & Shadowed) and policy warning for streamlining firewall policies. | **Please change to**: "The solution should provide traffic hit count, and policy warning for streamlining firewall policies."<br>**Justification:** Rule Conflict Detection (Redundant & Shadowed) can currently be achieved through an external dedicated solution like alogsec. For Check Point this feature is in roadmap and expected as part of R82 release. | Optional. |
| 15 | Section – VII/Specifications – | Should support the capability of providing | **Please change to** "Should support the capability of providing network-based detection of malware by | Please refer the revised specifications |

| | | | | |
|---|---|---|---|---|
| | A/8-Anti-APT / Malware Features/Page-35 | network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis. | checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis."<br>**Justification:** While we support this feature, putting a no on the timelines may not always hold true as it may vary on the file size, bandwidth etc., hence request to retain the feature without time constraint | given below. |
| 16 | Section – VII/Specifications – A/11-DNS Security/Page-36 | The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1. | **Please change to**: "The Solution should support DNS security. Necessary licenses to be included from day 1.<br>**Justification:** DNS security inline mode is specific to a particular OEM. Request to remove to allow participation. | Please refer the revised specifications given below. |
| 17 | Section – VII/Specifications – A/11-DNS Security/Page-37 | The solution should have capabilities to neutralize DNS tunneling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers. | **Please change to** "The solution should have capabilities to neutralize DNS tunneling".<br>**Justification:** What is the meaning of blocking the parent domain for all customers? The second part is not technically clear. Hence either elaborate the use case or remove the second part for participation | Yes changed. |
| 18 | Section – VII/Specifications – A/12-SD_WAN/Page-37 | Integrated Traffic Shaping functionality for both inbound and outbound traffic. | **Please change to** "Integrated Traffic Shaping functionality for outbound traffic"<br>**Justification:** We do outbound, not inbound currently-hence needed for participation | Please refer the revised specifications given below. |
| **3. M/s DRS IT Consultancy Private Limited** | | | | |
| 1 | Web Application | Traffic Ports support: 4x10 | Traffic Ports support: As per the present data centre/It infra | Please refer the revised |

| | | | | |
|---|---|---|---|---|
| | Firewall with Server Load Balancer/Point 2/Page no.39 | GE Fiber, 4x1G GE Fiber and 4x1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 7 requests per second: 1300,000 Layer 4 connection per second: 500,000 Concurrent Connection: 38 Million RSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for ADC/WAF/SLB deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amending this clause.<br>Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. Please amend this clause.<br>Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. Please amend this clause.<br>It is suggested to amend the clause as :<br>Traffic Ports support: 8 x 10 GE SFP+ from day-1 Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps<br>Layer 7 requests per second: 5 million<br>Layer 4 connections per second: 3 Million SA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU or equivalent or better Concurrent Connections: 40 Million Processor - Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | specifications given below. |
| 2 | Web Application Firewall with Server Load Balancer/Po | The proposed appliance should support the below metrics:<br>— Minimum | Different OEM has different terminology and technique to achieve similar function. We would like to request the honorable tendering committee to use vendor agnostic terminology for wider participation. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | int 6/Page no.40 | Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | — Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash/Equivalent<br>— Weighted Hash/Equivalent<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | |
| 3 | Web Application Firewall with Server Load Balancer/Point 7/Page no.40 | Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | Virtual Matrix Architecture feature is specific to one ADC OEM. Kindly remove this clause for wider participation and for other points please allow similar or equivalent feature metrics for broader participation.<br>Following Load Balancing Topologies should be supported:<br>• Client Network Address Translation (Proxy IP) /Equivalent<br>• Mapping Ports /Equivalent<br>• Direct Server Return /Equivalent<br>• One Arm Topology Application /Equivalent<br>• Direct Access Mode /Equivalent<br>• Assigning Multiple IP Addresses /Equivalent<br>• Immediate and Delayed Binding /Equivalent | Please refer the revised specifications given below. |
| 4 | Web Application Firewall with Server Load Balancer/Point 31/Page no.43 | The proposed appliance/software should be EAL2 certified. | For wider participation, We would like to request the honorable tendering committee to amend the clause as requested.<br>"The proposed appliance/software should be EAL2 certified/Make in India" | Please refer the revised specifications given below. |
| 5 | Web | Capable of | In order to switch over the | Please refer the |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Application Firewall with Server Load Balancer/Point 34/Page no.43 | handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | applications traffic like web app, email app etc. the GSLB solution must understand all types of DNS records and not just A or AAAA. Kindly add following functionality for complete Solution. It is suggested to amend this clause as :-<br>The Proposed Solution must have Global Server Load Balancing and should be able to host SRV Records, AAAA Records, A , PTR , MX ,TXT ,SOA, NS, Dname, Dmarc Records and should also support DNSSEC. | revised specifications given below. |
| 6 | Web Application Firewall with Server Load Balancer/Point 44 a/Page no.44 | Application load balance with functionality of Application delivery features ,<br>Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense,<br>Zero day prevention , DLP , Analytics, Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support. | IPS is completely different technology even deployment is different. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P" | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8 months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | | |
| **4. M/s Everest IMS Technologies Private Limited** | | | | |
| 1 | Section –VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-44 | The solution should automatically group servers that work closely together based on analysis of communication between them | Request you to modify the OEM specific clause as:<br>The solution should automatically /Manually group servers that work closely together based on analysis of communication between them | Please refer the revised specifications given below. |
| 2 | Section –VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.- | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 44 | host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. |  |  |
| 3 | Section –VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-44 | The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. | Request you to modify the specific clause as:<br>The solution should be able to automatically /manually detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery.<br>As multiple software does not provide the required data on any standard protocol so please modify the clause as suggested | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| 4 | Section –VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-45 | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | Request you to provide more details on the software/application from which EMS application need to integrate | Please refer the revised specifications given below. |
| 5 | Section –VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-45 | The solution should be able to track connectivity between network endpoints and display the delay between nodes | As per our understanding here need to monitor the latency of all the nodes from application server, please clarify | Please refer the revised specifications given below. |
| 6 | Section –VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.- | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated | The required features is not the standard ask of NMS solution and can be achieved via ITSM solution, so please confirm here whether new ITSM need to propose here or NMS will be integrated with existing running ITSM solution.<br>If Existing please provide OEM and version details of the ITSM solution. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | 48 | assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | | |
| 7 | Section –VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-44 | It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any node of the application. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate. | Please refer the revised specifications given below. |
| 8 | | Additional | Request you to please provide the required details of the IT Infrastructure which will be monitored in NMS solution<br>1) No. of servers:<br>i) Physical Server ii) VMs<br>iii) Physical server on which virtualization platform running.<br>2) No. & Make Of Network devices<br>i) Router/Switches /Firewall<br>ii) Wireless Controller /Wi-Fi AP<br>iii) Storage<br>3) No. & Name Of Applications | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | | 4) No. Of containers.<br>Or any other IP devices | |
| **5. M/s F5 Networks** | | | | |
| 1 | "Specifications – B" Web Application Firewall with Server Load Balancer Page no.39 | 2. Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. | Server load Balancer and WAF will deploy for Application Security. Application resides on Servers which are connected on 10gig fiber ports with Server Farm switch. Asking 1gig ports in Server load balancer is creating a bottleneck in high speed server farm connectivity. In today's deployments no data center is using and connecting on 1gig copper or fiber connectivity. Kindly consider 10gig or 25gig connectivity for using proposed solution for next 5-7 years. Kindly modify clause as" Traffic Ports support: 4 x 10 GE/25Gig Fiber and 4 x 1G/10gig Copper Port from day-1. All transceivers (multimode) from day1. 10gig interface should upgrade to 25Gig speed by changing transceivers only in future." | |
| 2 | "Specifications – B" Web Application Firewall with Server Load Balancer Page no.39 | 6. The proposed appliance should support the below metrics:<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least Connections,<br>— Least Connections Per Service, — Round-Robin,<br>— Response Time, — Bandwidth, etc | Kindly allow Equivalent feature for other reputed OEM's to participate.<br>Kindly modify clause as" 6. The proposed appliance should support the below metrics:<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash or Equivalent,<br>— Tunable Hash or Equivalent,<br>— Weighted Hash or Equivalent,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc" | Please refer the revised specifications given below. |
| 3 | "Specifications – B" Web Application Firewall with Server | 7. Following Load Balancing Topologies should be supported:<br>• Virtual Matrix | Kindly allow Equivalent feature for other reputed OEM's to participate. Kindly modify clause as" 7. Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture or | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Load Balancer Page no.39 | Architecture<br>• Client Network Address Translation (Proxy IP) • Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | Equivalent<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports or Equivalent<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding" | |
| 4 | “Specifications – B” Web Application Firewall with Server Load Balancer Page no.40 | 8. The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source /3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during | Appliance asked with 64GB RAMS. If we create 4 x virtualized environment with minimum 16GB RAM only 4 virtual tenants can be created.<br>Kindly modify the clause, so reputed OEM's can participate" 8. The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature or Multi-Tenancy that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. 2 virtual instances from Day 1 and scalable upto 4 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality. Each Virtual Instance contains a complete and separated environment of the Following: | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality. Each Virtual Instance contains a complete and separated environment of the Following:<br>a) Resources, b) Configurations, c) Management, d) Operating System | a) Resources, b) Configurations, c) Management, d) Operating System" | |
| 5 | “Specifications –B” Web Application Firewall with Server Load Balancer Page no.41 | 18. The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be | "As far as we know, ICSA Labs is out of business. Few OEM's might have older reports, but they likely won’t be able to renew it. Also Wikipedia mentions it: https://en.wikipedia.org/wiki/International_Computer_Security_Association “ICSA Labs ceased operation in 2022, following closure by its parent company Verizon”. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | Also their website is down: https://www.icsalabs.com/"" ""Kindly remove the ICSA certified as it no longer applies on new products." Kindly modify clause as "18. The proposed Solution should be mentioned in Secure IQ /Koppengiercole report for WAF Solution and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks with OWASP Dashboard and WASC Web Security Attack Classification." | |
| 6 | "Specifications –B" Web Application Firewall with Server Load Balancer Page no.41 | 25. Auto Policy Optimization<br>• Known Types of Attack Protection - Rapid Mode<br>• Zero Day Attack Blocking - Extended Mode<br>• Working in Learn Mode<br>• Auto Discovery | Kindly allow Equivalent feature for other reputed OEM's to participate. Kindly modify clause as" 25. Auto Policy Optimization<br>• Known Types of Attack Protection - Rapid Mode or Equivalent<br>• Zero Day Attack Blocking - Extended Mode or Equivalent<br>• Working in Learn Mode<br>• Auto Discovery" | Please refer the revised specifications given below. |
| 7 | "Specifications –B" Web Application Firewall with Server Load Balancer Page no.42 | 31 The proposed appliance/software should be EAL2 certified. | "EAL2 is now known as network device collaborative protection profile. A collaborative Protection Profile (cPP), developed and maintained in accordance with CCRA Annex K, with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and ALC_FLR, developed through an International Technical Community endorsed by the Management Committee; https://commoncriteriaportal.org/products/index.cfm<br>Kindly modify clause as"" 31. The proposed appliance/software should be EAL2/NDPP certified." | Please refer the revised specifications given below. |
| 8 | "Specifications –B" Web Application Firewall with Server Load Balancer Page no.42 | 33 Global loads balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT/ full DNS server with | Kindly modify clause to include DNS /GSLB license from day one as" 33 Global load balancing should support advance functions Authoritative name sever, DNS proxy, DNS NAT, full DNS server with DNS Sec, DNS DDOS, application load balancing from day one with relevant Licenses. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | DNSSec /DNS DDOS/application load balancing from day one with relevant Licenses. | | |
| 9 | “Specifications –B” Web Application Firewall with Server Load Balancer Page no.42 | 34 Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | Kindly include major DNS record types for full function of DNS and GSLB feature.<br>Kindly modify clause as" 34 Capable of handling complete Full DNS bind records including A, AAAA, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV, TXR etc. etc. for IPv4/IPv6 | Please refer the revised specifications given below. |
| 10 | “Specifications – B” Web Application Firewall with Server Load Balancer Page no.42 | 35 Should have a Web Vulnerability Scanner feature to detect existing vulnerabilities like SQL Injection, Cross Site Scripting, Source code disclosure, OS Commanding in the web applications. | Kindly allow Equivalent feature for other reputed OEM's to participate.<br>Kindly modify clause as" 35 Should have a integration with third party Web Vulnerability Scanner to detect existing vulnerabilities like SQL Injection, Cross Site Scripting, Source code disclosure, OS Commanding in the web applications." | Please refer the revised specifications given below. |
| 11 | “Specifications – B” Web Application Firewall with Server Load Balancer Page no.43 | 44 Support a Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 | WAF and SLB solution will provide certain features but not IPS, DLP and antivirus.<br>Kindly modify clause as" 44 Support a Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics, Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support.<br>Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. " | |
| 12 | "Specifications – B" Web Application Firewall with Server Load Balancer | Add Clause as Key Web Application Firewall L7 DDOS features are missing. Kindly incorporate. | The proposed solution should have server stress based L7 Behavioral DOS detection and mitigation including the ability to create real time L7 DOS signatures. | Yes accepted. Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Page no.43 |  |  |  |
| 13 | "Specifications – B" Web Application Firewall with Server Load Balancer Page no.43 | Add Clause as Key Web Application Firewall L7 DDOS features are missing. Kindly incorporate. | The proposed solution should provide behavioral DoS (BADoS) which provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. | Please refer the revised specifications given below. |
| 14 | "Specifications – B" Web Application Firewall with Server Load Balancer Page no.43 | Add Clause as Key Web Application Firewall L7 DDOS features are missing. Kindly incorporate. | The proposed solution must support Single Sign-On functionality on the same appliance running on the same OS version from the same OEM in the future. The solution must protect against FTP, SMTP, HTTP, HTTPS, and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks. | The vendor can quote higher side /proposed better solution. |
| 15 | "Specifications – B" Web Application Firewall with Server Load Balancer Page no.43 | Add Clause as Key Web Application Firewall features are missing. Kindly incorporate. | The proposed solution should have the capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating JavaScript and CAPTCHA challenges. | The vendor can quote higher side /proposed better solution. |
| 16 | "Specifications – B" Web Application Firewall with Server Load Balancer Page no.43 | Add Clause as Key Web Application Firewall features are missing. Kindly incorporate. | The proposed WAF should support of prevention of theft as well as the mitigation of attacks that uses previously stolen credentials. | The vendor can quote higher side /proposed better solution. |
| **6. M/s iValue InfoSolutions Pvt. Ltd.** |  |  |  |  |
| 1 | Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps |  | Due to license capping the OEMs have the advantage to quote higher for the incremental license which is not cost effective to customer. Hence request you to amend the point as "The ADC+WAF should be fully populated with the license throughput of 40 Gbps from Day-1." | Please refer the revised specifications given below. |
| 2 | Processor: Intel 12-core CPU, 64GB RAM, minimum |  | To derive the performance number from the specific compute numbers does not decide performance of the device at all due to Different architecture, ASICS, FTGA cards | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | 480GB SSD Disk and dual power supply. | | etchave different hardware requirement which cannot be generalized for performance. Request you to change the required Processor to Intel Xeon 8-core or higher. | |
| **7. M/s SonicWall** | | | | |
| 1 | Hardware Architecture | The proposed vendor must be in the Leader's or challenger quadrant of the Network Firewalls Gartner Magic Quadrant for latest year report. | The proposed vendor must be present in the Network Firewalls Gartner Magic Quadrant for latest year report. Required changes for Participate. | Please refer the revised specifications given below. |
| 2 | Performance & Scalability | High Availability: Active/Active and Active/Passive and should support session state synchronization among firewalls from day 1 | High Availability: Active/Active, Active/Passive and should support session state synchronization among firewalls from day. Required changes for Participate. | Please refer the revised specifications given below. |
| 3 | Performance & Scalability | Should support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance | Should support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context / instance. Make this point Optional - Required to participate | Please refer the revised specifications given below. |
| 4 | Next Gen Firewall Features | Should support more than 4000+ (excluding custom application signatures) distinct application | Should support more than 2000+ (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency. Required changes for Participate. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency | | |
| 5 | Next Gen Firewall Features | Should support more than 19,000 (excluding custom signatures) IPS signatures or more. | Should support more than 10,000 IPS signatures or more. Request to Start with Minimum. | 15000 |
| 6 | DNS Security | Should take inputs from at least 25 third-party sources of threat intelligence. | Should take inputs from at least 25 third-party sources of threat intelligence.<br>Make this point Optional – Required to Participate | The vendor can quote equivalent or better solution. |
| 7 | Interface and Connectivity Requirement | 6 X 10G Copper/RJ45 Day 1<br>8 X 1/10G SFP/SFP+ Day 1 with LR/SM transceivers and 8x3m patch cords.<br>4 X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one.<br>Minimum 2 x 10G HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management | Minimum 4 X 10G Copper/RJ45 Day 1 or more. 6 X 1/10G SFP/SFP+ Day 1 with LR/SM transceivers and 8x3m patch cords. 4 X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one. Minimum 2 x 1G/10G HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management Port. Required changes for Participate. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Port. | | |
| 8 | Next Gen Firewall Features | The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. | The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. Make this point Optional. | Optional. |
| 9 | Next Gen Firewall Features | The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor. Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist. The solution should have the capability to detect MD5, SHA256 and SHA512 traffic hashes to detect any malicious traffic pattern | The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor. The solution should have the capability to detect MD5, SHA256 and SHA512 traffic hashes to detect any malicious traffic pattern. We do have our own Capture threat labs – intel from here is used as of now to trap zero day & ransomware. | No Change. |
| 10 | Next Gen | The solution | It should also provide configuration | Please refer the |

| | | | | |
|---|---|---|---|---|
| | Firewall Features | should provide Configuration Deployment History, Pending Changes and Policy Compare capability before the security policies are deployed on the firewall. It should also provide configuration rollback capacity to the last good configuration running on the firewall. | rollback capacity to the last good configuration running on the firewall. Audit logs show the changes history with success/failed details. Requested to edit this clause as Pending changes is feasible via centralized management solution NSM. | revised specifications given below. |
| 11 | URL Filtering Features | Should must support URL threat intelligence feeds to protect against threats | Should support URL threat intelligence feeds to protect against threats.<br>Make this point optional | No change. |
| 12 | Logs & Reporting | Solution should offer Centralized NOC/SOC Visibility for the Attack Surface | Solution should offer Centralized NOC/SOC Visibility for the Attack Surface.<br>Remove this point or make it optional as it seems to be OEM specific. | No Change. |
| | | **8. XtraNet Technologies Private Limited** | | |
| 1 | Page no.22 4.8 TIME SCHEDULE TO COMPLETE THE CONTRACT:-<br>Point no. 4.8.1 | The successful bidder shall complete the assignment within 60 days from the date of issue of Letter of Acceptance / Letter of Intent. | We request the Department to amend the clause as below:<br>The successful bidder shall complete the assignment within 120 days from the date of issue of Letter of Acceptance / Letter of Intent. | No change. |
| 2 | Page no. 30 WARRANTY SERVICE LEVEL REQUIREMENTS – SLA 6.7.4 The | **Details :**<br>(i) Within 48 working Hours from the call logging time – for all High Severity events<br>(ii) Within 72 | We request the Department to amend the clause as below:<br>**Details :**<br>(i) Within 48 working Hours from the call logging time – for all High Severity events<br>(ii) Within 72 working hours from the time of attending the problem for all | No change. |

| | | | | |
|---|---|---|---|---|
| | various Service Level Requirements and related penalties for default | working hours from the time of attending the problem for all Low severity events<br>**Penalties per day of delay / per fault / per occasion**<br>(i) For High Severity events, Rs.1000/-.<br>(ii) For Low Severity events, Rs.500/-<br>Delay will be counted in steps of one hour. | Low severity events.<br>**Penalties per day of delay / per fault / per occasion**<br>(i) For High Severity events, Rs.1000/-.<br>(ii) For Low Severity events, Rs.500/-<br>Delay will be counted in steps of 1 day. | |
| 3 | Page No. 8 2.5 EARNEST MONEY DEPOSIT (EMD): | The proposal should be submitted along with only online application fee of Rs.5,000/- (Rs. Five Thousand only) and Earnest Money Deposit(EMD) of Rs.03 Lakh (Rupees Three Lakh only) in the form of online mode through e-procurement | We request the department to allow the EMD in the form Bank Guarantee. | No change. |
| 4 | Page no. 1 Hardcopy Submission of tender | The sealed tender complete in all respect addressed to “Registrar General, High Court of Madhya Pradesh, Jabalpur” must be submitted before 05:00 P.M. on 15th October, 2024 (mandatory). | We request the department Remove hard copy submission of tender. | No change. |
| 5 | Technical Query | | We request to consider our recommendation for dedicated | Quote as per tender. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | purpose built NIPS appliance. Reason "Whenever throughput increases, by default the box capacity will decrease as it is working with all the modules of FW, NIPS & Anti-APT or in worst case NGFW will bypass the NIPS & Anti-APT & will offer basic Firewall functionality only" |  |
| 6 | Firewall - Technical Specifications | The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1. | We request the department to generalize these points for wider and more competitive participation as it seems OEM Specific. | Quote as per tender and clarifications published. |
| **9. AKS Information Technology Services Pvt. Ltd** |  |  |  |  |
| **PQC Queries** |  |  |  |  |
| 1 | 2.5.1 or 3.13 page no. 08 | EMD worth 3 lakh INR OR The firms registered under NSIC and MSME (The vendor to be registered with both NSIC and MSME for claiming exemption of tender fees) are exempted for submission of tender fees only. But they have to submit valid EMD as per the tender requirement. | Kindly provide exemption to MSME /NSIC Bidders. | No change. |
| 2 | 2.15.2 page no. 12 | Three similar completed work costing not less than the amount equal to 40% of the estimated cost.<br>OR<br>Two similar completed work costing not less | Relaxation in the % | No change. |

| | | | | |
|---|---|---|---|---|
| | | than the amount equal to 50% of the estimated cost.<br>OR<br>One similar completed work costing not less than the amount equal to 80% of the estimated cost. | | |
| 3 | Phase 3 page no. 13 | The Commercial Proposal Evaluation will be based on the “individual cost”, which would be the total payouts including all taxes, duties and levies for the supply, installation, commissioning, system integration of equipments and Maintenance cost. | Evaluation Type | Evaluation will be done on line item basis. |
| 4 | 2.20.3 page no.14 | Successful bidder must ensure his establishment in India and in the State of Madhya Pradesh for post-installation services and support of the supplied equipments. | Exemption for MP | No change. |
| 5 | 2.22 page no. 15 | The Government of India had amended the General Financial Rules 2017 to enable the imposition of restrictions under Rule | Exemption in Firewall Category | Quote as per tender document. |

| | | | | |
|---|---|---|---|---|
| | | 144(xi) on bidders from countries which share a land border with India on grounds of defense of India, or matters directly or indirectly related thereto including national security. The bidder has to submit proper documents in this regards as per the policy. As per the Public Procurement (Preference to Make in India), Order 2017, the Class-I local suppliers shall get preference in procurement of goods, services or works. In furtherance of the Revised PPP-MII Order dated 04.06.2020, the Ministry of Electronics & Information Technology (MEIT) has notified the mechanism for calculation of local content for the 13 electronic products vide Notification no. 43/4/2019IPHW-MeitY dated 07.09.2020. | | |
| **NMS Queries** | | | | |
| 6 | Specificatio | The solution | Requesting authority to amend the | Please refer the |

|  |  |  |  |  |
|---|---|---|---|---|
|  | ns – C, Network Monitoring System, Page No. 44 | should automatically group servers that work closely together based on analysis of communication between them. | clause as follows: The solution should automatically group servers that work closely together based on an analysis of communication analysis or grouping criteria such as tags and types between them. | revised specifications given below. |
| 7 | Specifications – C, Network Monitoring System, Page No. 44 | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. **It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them.** | Requesting authority to kindly revise the clause as this is OEM Specific and restrictive for other OEM to participate in this tender, suggested revised clause: "The solution should automatically build visualizations that shows dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities" | Please refer the revised specifications given below. |
| 8 | Specifications – C, Network Monitoring System, Page No. 45-46 | The solution should support extensive monitoring capabilities from an OS (Linux, Windows)/ platform standpoint and should provide capabilities for customer to develop, deploy customized | Kindly amend the clause as follows: The solution should support extensive monitoring capabilities from an OS (Linux, Windows) and platform standpoint, and should provide options to deploy customized monitoring requirements. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | monitoring requirements | | |
| 9 | Specifications – C, Network Monitoring System, Page No. 48 | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | This clause is restrictive to our participation. We kindly request authority to remove it. | Yes Removed. |
| 10 | Specifications – C, Network Monitoring System, Page No. 49 | Consider options for transferring licenses between devices or reallocating licenses as needs change. | We understand that the license used for a network device should also be applicable to a server device when needed, provided the network device is removed from monitoring and provisioning on the server. This would allow the same license to be used for monitoring the server device. Could you please confirm if our understanding is correct? | Yes. |
| 11 | Specifications – C, Network Monitoring System, Page No. 49 | Suggestion to additional clause | The proposed NMS solution should be aligned with ITIL framework principles, certified with ITIL4 for Monitoring & Event Management and Capacity & Performance Management processes, and must include comprehensive documentation demonstrating | No. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | compliance with these standards to ensure best practices in service management and operational excellence |  |
| 12 | Specifications – C, Network Monitoring System, Page No. 49 | Suggestion to additional clause | The proposed NMS solution must comply with recognized security standards, including ISO 27001:2013/ ISO 27034, and CIS (Center for Internet Security) certifications, to ensure robust security management, secure software development, and adherence to best practices in information security. | Yes changed in the specifications s given below. |
| **WAF Queries** |  |  |  |  |
| 13 | Section – VII Page 41, Point-18 | The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | As Haltdos is a Made in India firm, it does not qualify for ICSA accreditation. Instead, it will provide an STQC certification. **Justification:** Since Haltdos is a well-known Made in India (MII) company, we are not applicable for certifications like Gartner and ICSA. Instead, Haltdos will provide certifications like EAL2+ and STQC. | Please refer the revised specifications given below. |
| **10. M/s Palo Alto Networks** |  |  |  |  |
| 1 | “Specifications – A” Firewall Technical Specifications s 15. Device Storage Page 38 | Minimum 800GB SSD | Since these are hardware appliances, it comes with a fixed storage size, different vendor models would have different size of storage based on the models. Also since the RFP is also asking for Management server which would have more storage space to store the logs and configs a regular storage size SSD is adequate on the firewall, it is recommended to change the clause as below:<br>Minimum 400 GB SSD. | Please refer the revised specifications given below. |
| 2 | “Specifications – A” Firewall Technical Specifications s 14. Automation & Incident | The Proposed system shall support automation response based on following events:<br>Compromised Hosts detected | These are the features generally part of the Security Automation tool such as SOAR and the Firewall management could provide an insight for the below events and alert the analysts. Please remove the section or modify as below:<br>Monitor and send email alerts for below events: | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Response Page 37 | Configuration Change<br>Event Log<br>High CPU<br>License Expiry<br>Email Alert<br>IP Ban | System<br>Threats<br>Zero day / unknown malware<br>traffic logs |  |
| 3 | “Specifications – A” Firewall Technical Specifications s 5. Performance & Scalability Page 32 | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | Considering the current requirement and future scalability for MP High Court, it is recommended to increase the throughput of NGFW ad Threat Prevention. It would also take care of the periodical spike in the traffic and higher throughput requirement for the contract period as well. Request MP High Court to modify / amend the clause as below:<br>The NGFW throughput of the firewall should be a minimum 28 Gbps with 64 KB including application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, antispyware, sandboxing, user identification, file blocking, DNS security and logging enabled should be 15 Gbps considering 64 KB HTTP transaction size. | No change. |
| 4 | “Specifications – A” Firewall Technical Specifications s 5. Performance & Scalability Page 32 | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions | For better throughput and performance and to be in line with the throughput, please amend the clause as below:<br>NGFW Firewall should support at least 2.5 Million Layer 7 Concurrent sessions measured utilizing HTTP transactions or 20 Million Layer 3 / 4 concurrent sessions. | No change. |
| 5 | “Specifications – A” Firewall Technical Specifications s 5. Performance & Scalability | NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 connections per second – Min 90,000 | For better throughput and performance and to be in line with the throughput, we recommend amending the clause as below: NGFW Firewall should support at least 2 Million connections per second L3/L4 or New Layer 7 connections per second – Min 225K measured with application override, utilizing 1 byte HTTP transactions. | No change. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Page 32 |  |  |  |
| 6 | “Specifications – A” Firewall Technical Specifications s 10.Support Page 36 | OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The NGFW should be proposed with 5 years onsite support and subscription license for NGFW, NGIPS, Anti Virus, Anti Spyware, URL Filtering, DNS, VPN and Antibotnet | For a better visibility of the various licenses to be proposed / quoted, please amend the clause as below:<br>OEM should be present in India from at least 5 years and should be 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, Threat Protection, APT Protection (Zero Day Protection with integrated Sandboxing), URL Filtering and DNS Security from day 1. The solution shall support bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns for future use. | No Change. |
| **11. M/s Newgen It Technologies Limited** |  |  |  |  |
| 1 | Page no:10 & point no: 2.15.2 | Experience in Supply, Installation, commissioning, Maintenance of firewall, WAF, NMS tool and similar IT equipment’s during last 05 years | We kindly request the inclusion of experience in IT equipment, Data Centers, and related infrastructure. | Quote as per tender document. |
| 2 | Page No:15 & Point no: 2.20.3 | Successful bidder must ensure his establishment in India and in the State of Madhya Pradesh for post-installation services and support of the supplied equipment’s | We propose allowing bidders to establish their office after the award of the tender. To demonstrate commitment, bidders can submit a letter of undertaking to open an office in Madhya Pradesh post award. This flexibility will enable a wider range of qualified bidders to participate without compromising on service quality. | Yes changed. |

| | | | | |
|---|---|---|---|---|
| 3 | Page No: 33 | Technical Specifications | Tender specifications currently support a single OEM. We request a relaxation of this restriction to accommodate multiple brands. This change will enhance competition, potentially reduce costs, and provide more options for high-quality equipment and services. | Please refer the revised specifications given below. |
| | | **12. M/s Sophos** | | |
| 1 | 3rd party Test Certification Page No. 32 | The proposed firewall vendor must have over 97% of Exploit Block rate in latest NGFW NSS Lab Test report. | Please remove.<br>NSS Labs already closed and already irrelevant since we are unable to get succeeding certification from them. | Please refer the revised specifications given below. |
| 2 | 3rd party Test Certification Page No. 32 | The proposed vendor must be in the Leader's or challenger quadrant of the Network Firewalls Gartner Magic Quadrant for latest year report. | The proposed vendor must be in the Gartner's Magic quadrant for the network firewalls as per the latest report .<br>OR<br>The proposed vendor should be qualified as a class 1 Make In India vendor as per DPIT guideline. As per DPIT notification DPIIT Notification File No- P-45021/2/2017-PP(BE-II) dated 16-09-2020 from the Ministry of India , Make In India product should be given privilege and Gartner/ or any other 3rd party international certificate are not considered. | Please refer the revised specifications given below. |
| 3 | Interface and Connectivity Requirement Page No. 32 | 6 X 10G Copper/RJ45 Day 1 | 6 X 10G Copper/ 10 G fiber with RJ45 Transreciever from Day 1. Every OEM has it's standard architecture, kindly make it more generic feature to participate more number of OEM in this bid. | Please refer the revised specifications given below. |
| 4 | Interface and Connectivity Requirement Page No. 32 | 4X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one | 4X 10/25/40 Gig SFP28/QSFP Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one. Sir, your backend network ports are standard on 10G/ 40G/ 100G QSFP. Whereas, you have asked for 10G/25G which does not make sense because your entire network is on 10G and after link aggregation on your SD-WAN your capacity will increase from 10G. Hence, You should ask for "Minimum 40G of | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | | SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one."<br>Today this will not increase your price rather will make it standard for everyone and you will get the best product otherwise everybody will quote 10G product only. | |
| 5 | Next Gen Firewall Features Page No. 33 | Should support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance | Should support capability to create multiple virtual context/instance /virtual zones with physical interfaces, ensure traffic isolation between virtual context/instance /Virtual Zones. Every OEM has it's standard architecture, and parlance we request you to make it generic by putting "Should support capability to create multiple virtual context/instance /virtual zones with physical interfaces, ensure traffic isolation between virtual context/instance/Virtual Zones". Keep it more generic because the definition becomes very OEM specific. | Please refer the revised specifications given below. |
| 6 | Next Gen Firewall Features Page No. 34 | The solution should provide Configuration Deployment History, Pending Changes and Policy Compare capability before the security policies are deployed on the firewall. It should also provide configuration rollback capacity to the last good configuration running on the firewall. | The solution should provide Configuration Deployment History and Web Policy Compare/test capability before the policies are deployed on the firewall. It should also provide configuration rollback capacity to the last good configuration running on the firewall. Every OEM has its standard architecture, Sir; It is difficult to show what comparison means between different policies it is always better to have web policy comparison /Testing capability. Kindly make it more generic feature to participate more number of OEM in this bid. | Please refer the revised specifications given below. |
| 7 | Manageme nt Page No. 35 | The management platform must be capable of integrating third party vulnerability information into threat policy | The management platform must be capable of integrating third party security information into data lake & correlate them to provide contextual information & accelerated threat discovery and response. Every OEM has it's standard architecture and feature set. In today's highly evolved threat | No change. |

| | | | | |
|---|---|---|---|---|
| | | adjustment routines and automated tuning workflows | environment, security management console should have 3rd party security product & logs integration facility. In collaboration with 3rd party security logs, threat can be discovered quickly and response can be more faster across all estates. | |
| 8 | Logs & Reporting Page No. 38 | Bidder has to propose on premise dedicated logging, analytics & reporting solution from same OEM (Virtual /Physical Appliance) from day1, the logging solution to be deployed at Data Center only.<br>In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. Required Features:<br>Should Deliver single-pane visibility, also | Bidder has to propose on premise dedicated logging, analytics & reporting solution from (Virtual /Physical Appliance/India Cloud) from day1, the logging solution to be deployed at Data Center only. In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. Required Features: Should Deliver single-pane visibility, also have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance reports in different formats. The solution should have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics /event correlation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained models and traffic classifiers. The same should be available on public website to validate the capabilities. Every OEM has its standard architecture, kindly make it more generic feature to participate more number of OEM in this bid. As per latest guideline by Cert-IN data | No change. Quote as per tender document. |

| | | | | |
|---|---|---|---|---|
| | | have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance reports in different formats. The solution should have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics /event corelation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained | should be reside within geographical border of India. Hence requesting , reports can be stored in India DC which is SOC2 certified and empanelled with MeitY for better and efficient management, feature rich SIEM like details reporting, flexibility in storage increment at any point of time and saving more energy to encourage Go-Green policy. | |

| | | | | |
|---|---|---|---|---|
| | | models and traffic classifiers. The same should be available on public website to validate the capabilities. | | |
| **13. M/s Microworld Infosol Pvt. Ltd., M/s Computer Bazar & M/s Veltronics India Pvt. Ltd.** | | | | |
| **FirewallTechnicalSpecifications** | | | | |
| 1 | 4-Hardware Architecture | The appliance hardware should be multi core CPU architecture and should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one.<br>The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any | Security appliance should be evaluated based on their security effectiveness, features, and functionality, rather than their architecture. The current clause seems to favor PC-based architecture, potentially excluding ASIC OEMs from the tender. We would like to emphasize that ASIC technology is no longer proprietary, as many leading OEMs are adopting it for its superior performance. Please refer to the URL below, which highlights that ASIC is not exclusive to Fortieth. Therefore, we request the removal of this clause and suggest that MP High court to consider architectures based on their performance and security effectiveness.<br>https://community.cisco.com/t5/networking-blogs/the-new-era-of-wan-an-asic-innovation- story/ba-p/4175243<br>https://www.paloaltonetworks.com/network- security/hardware-firewall-innovations<br>https://blog.checkpoint.com/security/check- point-software-introduces-the-worlds-fastest-firewall-delivering-20-times-better-price-performance-to-the-worlds-most-demanding-datacenters/<br>The appliance hardware should be multi core CPU architecture or should be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | single point of failure in the solution | The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution. | |
| 2 | 4-Hardware Architecture | OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one. | OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one or should be proprietary ASIC based in nature to make sure all the security capabilities are provided without degradation from day one. | Please refer the revised specifications given below. |
| 3 | 5 Performance & Scalability | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real World /enterprise /production traffic with logging enabled. The Threat Prevention /NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled shouldbe 12Gbps. | Reason for change Every OEM has different ways to measure the throughput values. We request to changes so all major OEM matches this and can participate.<br>The NGFW throughput of the firewall should be a minimum 15 (enterprise mix /Real world with logging enabled) OR Application throughput measured with 64K http minimum 20Gbps. Threat prevention throughput minimum 10Gbps (Enterprise Mix / Real World with logging enabled) | Please refer the revised specifications given below. |
| 4 | | It is highly recommended to ask SSL inspection throughput. This is important parameters to size the right box. Because lower SSL inspection | Minimum 10Gbps of SSL inspection throughput and 500K SSL inspection concurrent session support | No change. |

| | | | | |
|---|---|---|---|---|
| | | throughput can degrade the performance while Complete inspection of the packet is enabled. | | |
| 5 | | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions | Most of the OEM is publish the connection per second and concurrent session in TCP. It's highly recommended on the basis of the ports count that the connections requirement must be higher so device not becomes bottle neck. Asking the lower connections is favoring specific OEM model. | Please refer the revised specifications given below. |
| 6 | 6-Next Gen Firewall Features | NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 connections per second –<br>Min 90000 | Min 500K Connection per Second and 5M concurrent connections. | No change. |
| 7 | 6-Next Gen Firewall Features | Should support more than 19,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's | Favoring to specific OEM signature count.<br>Request to make changes and allow min 10000 Signatures. | Yes changed TO 15000. |
| 8 | | Should support | Every OEM has different counts and | Yes changed. |

| | | | | |
|---|---|---|---|---|
| | | Reputation- and category- based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 75+ categories from day1. | categories. This is favoring to specific OEM nos.<br>Request to remove this clause | |
| 9 | 11-DNS Security | The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1. | Favoring to Specific OEM.<br>The Solution should support DNS security in line mode/proxy mode. Necessary licenses to be included from day 1. | Please refer the revised specifications given below. |
| 10 | | DNS security 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. | Every OEM has different counts in threat intelligence asking specific favoring to specific OEM.<br>Request to remove 10M malicious domain. | Please refer the revised specifications given below. |
| 11 | | The solution should integrate and correlate to provide effective prevention against. New C2 domains, file download source domains, and domains in malicious email | Favoring to Specific OEM: Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence.<br>Request to remove this clause. | The vendor can quote equivalent or better solution. |

| | | | | |
|---|---|---|---|---|
| | | links.<br>Integrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators.<br>Should have OEM human-driven adversary tracking and malware reverse Engineering, including insight from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence. | | |
| **Load Balancer + WAF** | | | | |
| 12 | Clause No. 2 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 7 requests per second: 1300,000 Layer 4 connection per second: 500,000 Concurrent Connection: 38 | Every OEM has its own architecture. Scalability ask within same appliance is favoring specific OEM architecture. We request MP high court specific the required throughput values including scalability requirement and it is highly recommended to Layer 7 throughput of the appliance now a day's most off the applications are HTTP and HTTPS. Ask parameters are favoring specific OEM model and designed such a way to make competition model higher. For fair participation we request relaxation in parameters. ASIC technology does not required higher memory and throughput to match the desired performance. So Request the processor and memory clause. Also request to relax ports here. Ask ports counts are favoring specific OEM model.<br>Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G From day 1 Device L7 Throughput: Minimum 20 Gbps Layer 7 CPS : Minimum: 200K Concurrent | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | Million RSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | Connection : Minimum 25 Million SSL CPS : minimum 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support OR SSL Bulk encryption throughput min 10Gbps. |  |
| 13 | Clause No. 7 | Following Load Balancing Topologies should be supported:<br>•Virtual Matrix Architecture<br>•Mapping Ports<br>•Direct Server Return<br>•One Arm Topology Application<br>•Direct Access Mode<br>•Assigning Multiple IP Addresses<br>•Immediate and Delayed Binding | Some of the topologies favoring to specific OEM architecture Suggest relaxing this clause.<br>Following Load Balancing Topologies should be supported: Router Mode, One-Arm Mode, and Direct Server Return Mode deployments, Direct access Mode, Mapping Ports, Client Network Address Translation (Proxy IP), Assigning Multiple IP Addresses. | Please refer the revised specifications given below. |
| 14 | Clause No. 8 | The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) that virtualizes the Device | Hardware appliance also supports virtual context / domains. Request to allow the same.<br>The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) OR inbuilt support of virtual domain that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality. | use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality.<br><br>Each Virtual Instance contains a complete and separated environment of the Following:<br>a) Resources, b) Configurations, c) Management, d) Operating System. | |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | Each Virtual Instance contains a complete and separated environment of the Following:<br>a)Resources,<br>b)Configurations<br>c)Management,<br>d)Operating System |  |  |
| 15 | Clause No.19 | WAF should have the flexibility to be deployed in the following modes:<br>Reverse proxy<br>Out of Path (OOP) | Favoring to specific OEM<br>Request to remove - Out of Path (OOP) | Yes changed / removed. |
| 16 | 2.15 Eligibility /Pre-Qualification Criteria: | Bidders meeting ALL of the following pre-qualification criteria are eligible to apply: (i) Experience: Experience in the supply, installation, commissioning, and maintenance of firewall, WAF, NMS tools, and similar IT equipment during the last 5 years, ending on the last day of the month preceding the publication of this tender, should meet either of the following: [Details as per your document. | Our Request: As the Original Equipment Manufacturer (OEM) is responsible for the maintenance and installation of the firewall, and we coordinate directly with the OEM, we kindly request that you consider our experience in supplying IT equipment as sufficient qualification. | No change. |
| **14. M/s VSN International Pvt. Ltd.** |  |  |  |  |
| **1** | Section – IV | 4.2.1 The | As the warranty asked in the bid is for | Yes changed. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 4 GENERAL CONDITIONS OF THE CONTRACT (GCC):- 4.2 PERFORMANCE GUARANTEE:- | Successful Bidder will be required to furnish performance guarantee in the form of unconditional Bank Guarantee issued by a Nationalized / Scheduled Bank in India equivalent to 05% of the Contract Value initially valid for a period of 36 months within 30 days from the date of issue of Letter of Award / acceptance. For remaining 24 months Bidder will submit fresh BG before expiry of the initial BG. | 5 years onsite, We would request to ask for Performance bank Guarantee for 5 years only at the time of release of purchase order this will bind bidder for warranty obligation and service support till the end of warranty period. | The Successful Bidder will required to furnish performance guarantee in the form of unconditional Bank Guarantee issued by a Nationalized / Scheduled Bank valid for a period of 60 months within 30 days from the date of issue of Letter of Award / acceptance. |
| **2** | Section – I NOTICE INVITING TENDER | Estimated project cost (In Lakh Rs.): 1.50 Crore | As per the clause the Budget Projection mentioned in the NIT is very low as per the solution required in the RFP. As per the requirement we assume that the budget for the RFP should be at least **6-7 Cr.** to execute the Order properly. We kindly request you to kindly revise the budget projection as requested to meet the tender requirement. | The budget is revised to approximately Rs. 05 Crore. |
| **3** | "Specifications – A" Firewall Technical Specifications s, Page No.32, S.No.04- Hardware Architecture | The appliance hardware should be a multicore CPU architecture and should not be proprietary ASIC based in nature & should be open architecture based on multi- | **<u>Justification:-</u>**Security appliance should be evaluated based on their security effectiveness, features, and functionality, rather than their architecture. The current clause seems to favor PC-based architecture, potentially excluding ASIC OEMs from the tender. We would like to emphasize that ASIC technology is no longer proprietary, as many leading OEMs are adopting it for its superior performance. Please refer to the URL below, which | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one. | highlights that ASIC is not exclusive to Fortinet. Therefore, we request the removal of this clause and suggest that MP High court to consider architectures based on their performance and security effectiveness.<br>https://community.cisco.com/t5/networking-blogs/the-new-era-of-wan-an-asic-innovation-story/ba-p/4175243<br>https://www.paloaltonetworks.com/network-security/hardware-firewall-innovations<br>https://blog.checkpoint.com/security/check-point-software-introduces-the-worlds-fastest-firewall-delivering-20-times-better-price-performance-to-the-worlds-most-demanding-datacenters/<br>Request for change:- The appliance hardware should be a multicore CPU architecture or can be ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM. | |
| **4** | “Specifications – A”Firewall Technical Specifications s, Page No.32, S.No.04- Hardware Architecture | The appliance hardware should be a multicore CPU architectureand should not be proprietary ASIC based in nature & should beopen architecture based on multi-core cpu's to protect & scaleagainst dynamic latest security threats. The appliance hardwareshould have a hardened operating system from the OEM andshould support | Justification:- ASCI solution do not require higher memory and CPU to deliver the desire functionality. Only PC based architecture require high memory. We suggest removing this clause as it is favoring single OEM devices. We emphasize MP High court team to evaluate the Firewall solution based on the performance parameters Not memory and CPU We would request to amend the clause to "OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one or or should be proprietary ASIC based in nature to make sure all the security capabilities are provided without degradation from day one." | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | minimum of 64GB of RAM to make sure all thesecurity capabilities are provided without degradation from dayone | | |
| **5** | “Specifications – A” Firewall Technical Specifications s, Page No.32, S.No.05-Performance & Scalability | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | Justification:- Every OEM have different ways to measured the throughput values. We request for changes so all major OEM match this and can participate in the bid. We would request to amend the clause to" The NGFW throughput of the firewall should be a minimum 15 (enterprise mix /Real world with logging enabled) OR Application throughput measured with 64K http minimum 20Gbps. Threat prevention throughput minimum 10Gbps (Enterprise Mix / Real World with logging enabled)". | Please refer the revised specifications given below. |
| **6** | “Specifications – A” Firewall Technical Specifications s, Page No.32, S.No.05-Performance & Scalability | Additional Point | It is highly recommended to ask SSL inspection throughput. This is important parameters to size the right box. Because lower SSL inspection throughput can degrade the performance while complete inspection of the packet is enabled. We would request to add new clause as "Minimum 10Gbps of SSL inspection throughput and 500K SSL inspection concurrent session support." | No change. |
| **7** | “Specifications – A” Firewall Technical Specifications s, Page | NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 | Most of the OEM is publish the connection per second and concurrent session in TCP. It's highly recommended on the basis of the ports count that the connections requirement must be higher so device | No change. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | No.32, S.No.05-Performance & Scalability | connections per second – Min 90,000 | not becomes bottle neck. Asking the lower connections is favoring specific OEM model.<br>We would request to amend the clause to "NGFW Firewall should support at least Min 500K Connection per Second and 5M concurrent connections." |  |
| **8** | "Specifications – A" Firewall Technical Specifications s, Page No.32, S.No.06-Next Gen Firewall Features | Should support more than 19,000 (excluding custom signatures)<br>IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's | This clause is favoring to specific OEM signature count so, we would request to make changes and allow min 10000 Signatures. | Please refer the revised specifications given below. |
| **9** | "Specifications – A"Firewall Technical Specifications s, Page No.32, S.No.07-URLFiltering Features | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 75+ categories from day1. | Every OEM has different counts and categories. This is favoring to specific OEM nos. Hence, We would request to kindly remove this clause. | Please refer the revised specifications given below. |
| **10** | "Specifications – A" Firewall | The Solution should support DNS security in | This clause is favoring to Specific OEM. Hence, we would request to amend the clause to "The Solution | Please refer the revised specifications |

| | | | | |
|---|---|---|---|---|
| | Technical Specifications s, Page No.36, S.No.11-DNS Security | line mode and not proxy mode. Necessary licenses to be included from day 1. | should support DNS security in line mode/proxy mode. Necessary licenses to be included from day 1." | given below. |
| **11** | “Specifications – A” Firewall Technical Specifications s, Page No.36, S.No.11-DNS Security | DNS security 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. | Every OEM has different counts in threat intelligence asking specific favoring to specific OEM. We would request to remove 10M malicious domain from the specifications . | Please refer the revised specifications given below. |
| **12** | “Specifications – A” Firewall Technical Specifications s, Page No.36, S.No.11-DNS Security | The solution should integrate and correlate to provide effective prevention against.<br>New C2 domains, file download source domains, and domains in malicious email links.<br>Integrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators.<br>Should have OEM human-driven adversary tracking and malware reverse engineering, | This clause is Favoring to Specific OEM: Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence<br>Hence, we would request to remove this clause from the specifications s. | The vendor can quote equivalent or better solution. |

| | | | | |
|---|---|---|---|---|
| | | including insight from globally deployed honey pots.<br>Should take inputs from at least 25 third-party sources of threat intelligence. | | |
| **13** | “Specifications – A” Firewall Technical Specifications s, Page No.32, S.No.02-3rd party Test Certification | The proposed firewall vendor must have over 97% of Exploit Block rate in latest NGFW NSS Lab Test report. | NSS Labs already closed and already irrelevant since we are unable to get succeeding certification from them. Hence, we would request to kindly remove this clause. | Please refer the revised specifications given below. |
| **14** | “Specifications – A” Firewall Technical Specifications s, Page No.32, S.No.02-3rd party Test Certification | The proposed vendor must be in the Leader’s or challenger quadrant of the Network Firewalls Gartner Magic Quadrant for latest year report. | As per DPIT notification DPIIT Notification File No- P-45021/2/2017-PP(BE-II) dated 16-09-2020 from the Ministry of India , Make In India product should be given privilege and Gartner/ or any other 3rd party international certificate are not considered.<br>**Request for change:-**<br>The proposed vendor must be in the Gartner's Magic quadrant for the network firewalls as per the latest report.<br>**OR**<br>The proposed vendor should be qualified as a class 1 Make In India vendor as per DPIT guideline. | Please refer the revised specifications given below. |
| **15** | “Specifications – A” Firewall Technical Specifications s, Page No.32, S.No.03-Interface and Connectivity Requiremen | 6 X 10G Copper/RJ45 Day 1 | Every OEM has its standard architecture, kindly make it more generic feature to participate more number of OEM in this bid. We would request to amend the clause to "6 X 10G Copper/ 10 G fiber with RJ45 Trans-receiver from Day 1" | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | t | | | |
| **16** | “Specifications – A”Firewall Technical Specifications s, Page No.32, S.No.03-Interfaceand Connectivity Requirement | 4X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one | Sir, your backend network ports are standard on 10G/ 40G/ 100G QSFP. Whereas, you have asked for 10G/25G which does not make sense because your entire network is on 10G and after link aggregation on your SD-WAN your capacity will increase from 10G. Hence, You should ask for "Minimum 40G of SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one." Today this will not increase your price rather will make it standard for everyone and you will get the best product otherwise everybody will quote 10G product only. | Please refer the revised specifications given below. |
| **17** | “Specifications – A” Firewall Technical Specifications s, Page No.33, S.No.06-Next Gen Firewall Features | Should support capability to create multiple virtual context /instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance | Every OEM has its standard architecture, and parlances we request you to make it generic by putting “Should support capability to create multiple virtual context/instance /virtual zones with physical interfaces, ensure traffic isolation between virtual context/instance/Virtual Zones". Keep it more generic because the definition becomes very OEM specific Hence, we would request to kindly amend the clause to "Should support capability to create multiple virtual context/instance /virtual zones with physical interfaces, ensure traffic isolation between virtual context /instance/Virtual Zones" | Please refer the revised specifications given below. |
| **18** | “Specifications – A” Firewall Technical Specifications s, Page No.34, S.No.06-Next Gen Firewall Features | The solution should provide Configuration Deployment History, Pending Changes and Policy Compare capability before the security policies are deployed on the firewall. It should also provide configuration rollback capacity | Every OEM has its standard architecture, Sir; It is difficult to show what comparison means between different policies it is always better to have web policy comparison/Testing capability. Kindly make it more generic feature to participate more number of OEM in this bid. Hence, we would request to kindly amend the clause to The solution should provide Configuration Deployment History and Web Policy Compare/test capability before the policies are deployed on the firewall. It should also provide configuration rollback | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | to the last good configuration running on the firewall. | capacity to the last good configuration running on the firewall. | |
| **19** | “Specifications – A” Firewall Technical Specifications s, Page No.38, S.No.16 - Logs & Reporting | Bidder has to propose on premise dedicated logging, analytics & reporting solution from same OEM (Virtual /Physical Appliance) from day1, the logging solution to be deployed at Data Center only.<br>In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | Every OEM has its standard architecture, kindly make it more generic feature to participate more number of OEM in this bid. As per latest guideline by Cert-IN data should be reside within geographical border of India. Hence requesting , reports can be stored in India DC which is SOC2 certified and empanelled with MeitY for better and efficient management, feature rich SIEM like details reporting, flexibility in storage increment at any point of time and saving more energy to encourage Go-Green policy.<br>Request for change:-Bidder has to propose on premise dedicated logging, analytics & reporting solution from (Virtual /Physical Appliance/India Cloud) from day1, the logging solution to be deployed at Data Center only.<br>In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | Quote as per tender. |
| | | Required Features:Should Deliver single-pane visibility, also have reporting facility to generate reports on virus | Required Features:Should Deliver single-pane visibility, also have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance | Quote as per tender. |

| | | | | |
|---|---|---|---|---|
| | | detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance reports in different formats. The solution should have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics /event correlation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained models and traffic classifiers. The same should be | reports in different formats. The solution should have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics /event correlation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained models and traffic classifiers. The same should be available on public website to validate the capabilities.**Request for Change: -** Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G From day 1Device L7 Throughput: Minimum 20 GbpsLayer 7 CPS : Minimum: 200K Concurrent Connection : Minimum 25 MillionSSL CPS : minimum 20,000ECC CPS (EC-P256): 12,000 with TLS1.3 Support OR SSL Bulk encryption throughput min 10Gbps | |

| | | | | |
|---|---|---|---|---|
| | | available on public website to validate the capabilities. | | |
| **20** | "Specifications – B" Web Application Firewall with Server Load Balancer, | Additional Query | In the specifications you have asked for Gartner report. We would like to inform you that Gartner has stop publishing report post 2018 for ADC. We would request to remove Gartner report and ask for IDC report for ADC. | *Top 10 brands / OEM as per latest IDC reports / Industry Standards.* |
| **21** | "Specifications – B" Web Application Firewall with Server Load Balancer, Page no.39, S.No.02 | **Traffic Ports support:** 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 7 requests per second: 1300,000 Layer 4 connection per second: 500,000 Concurrent Connection: 38 Million RSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and | Every OEM has its own architecture. Scalability ask within same appliance is favoring specific OEM architecture. We request MP high court specify the required throughput values including scalability requirement and it is highly recommended to Layer 7 throughput of the appliance now a day's most off the applications are HTTP and HTTPS . Ask parameters are favoring specific OEM model and designed such a way to make competition model higher. For fair participation we request relaxation in parameters. ASIC technologies do not required higher memory and throughput to match the desired performance. So Request the processor and memory clause. Also request to relax ports here. Ask ports counts are favoring specific OEM model. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | | |
| **22** | “Specifications – B” Web Application Firewall with Server Load Balancer, Page no.39, S.No.07 | Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | Some of the topologies favoring to specific OEM architecture Suggest relaxing this clause.<br>Request for change:-<br>Following Load Balancing Topologies should be supported: Router Mode, One-Arm Mode, and Direct Server Return Mode deployments , Direct access Mode, Mapping Ports, Client Network Address Translation (Proxy IP) , Assigning Multiple IP Addresses | Please refer the revised specifications given below. |
| **23** | “Specifications – B”Web Application Firewall with Server Load Balancer, Page no.40, S.No.08 | The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use | Hardware appliance also supports virtual context / domains. Request to allow the same.<br>**Request for change:-** The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) OR inbuilt support of virtual domain that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | Open Source /3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protectionfunctionality. Each Virtual Instance contains a complete and separated environment of the Following:a) Resources, b) | be high performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality. Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System |  |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | Configurations, c) Management, d) Operating System |  |  |
| **24** | "Specifications – B" Web Application Firewall with Server Load Balancer, Page no.41, S.No.19 | WAF should have the flexibility to be deployed in the following modes: Reverse proxy Out of Path (OOP) | This clause is Favoring to specific OEM. Hence, we would request to kindly remove Out of Path (OOP). | Yes removed. |
| **25** | "Specifications – B" Web Application Firewall with Server Load Balancer, Page no.39, S.No.02 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.<br>Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps<br>Layer 7 requests per second: 1300,000<br>Layer 4 connection per second: 500,000<br>Concurrent Connection: 38 Million<br>RSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel | Traffic Ports support: As per the present data center /IT infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for ADC/WAF/SLB deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amending this clause.<br>Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. Please amend this clause.<br>Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. Please amend this clause.<br>It is suggested to amend the clause as :-<br>Traffic Ports support: 8 x 10 GE SFP+ from day-1<br>Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps, Layer 7 requests per second : 5 million Layer 4 connections per second: 3 Million RSA CPS(2K Key): 20,000, ECC CPS (EC-P256): 12,000 with TLS1.3 Support, Processor: Intel 12-core CPU or equivalent or better, Concurrent Connections: 40 Million, Processor - Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | 1G RJ45 Management Port and 1G RJ45 Console port. |  |
| **26** | “Specifications –B” Web Application Firewall with Server Load Balancer, Page no.42, S.No.31 | The proposed appliance/software should be EAL2 certified. | We would like to request the honorable tendering committee to amend the clause for wider participation in the bid as "The proposed appliance /software should be EAL2 certified/ Applied for EAL2. Before the supply of the product the OEM should provide the EAL2 certification. | Please refer the revised specifications given below. |
| **27** | “Specifications – B”Web Application Firewall with Server Load Balancer, Page no.42, S.No.34 | Capable of handling complete Full DNS bind records including A, AAAA, etc.for IPv4/IPv6 | In order to switch over the applications traffic like web app, email app etc. the GSLB solution must understand all types of DNS records and not just A or AAAA. Kindly add following functionality for complete Solution. It is suggested to amend this clause as: - The Proposed Solution must have Global Server Load Balancing and should be able to host SRV Records, AAAA Records, A , PTR , MX ,TXT ,SOA, NS, Dname, Dmarc Records and should also support DNSSEC. | Please refer the revised specifications given below. |
| **28** | “Specifications – B” Web Application Firewall with Server Load Balancer, Page no.44, S.No.44 | Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High | IPS is completely different technology even deployment is different. IPS does not come in ADC and comes in network security. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P" | |
| **29** | “Specifications – B” | The proposed appliance should | DDoS protection should be provided with the help of stateless appliance | The vendor may provide DDoS |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Web Application Firewall with Server Load Balancer, Page no.39, S.No.01 | be a dedicated ADC/WAF/SLB appliance having DDoS protection, SSL inspection, and real-time threat intelligence. It should not be part of any Firewall or UTM. | as it doesn't maintain any session table, this is first and foremost criteria to choose DDoS protection appliance. ADC/WAF/SLB is state full appliance; hence DDoS should not be part of ADC/WAF/SLB.<br>Request for change: The proposed appliance should be a dedicated ADC/WAF/SLB appliance having SSL inspection, and real-time threat intelligence. it should not be part of any Firewall or UTM. | Protection with the help of any devices /software if the DDoS protection not available in dedicated ADC/WAF/SLB appliance. |
| **30** | “Specifications – B”Web Application Firewall with Server Load Balancer, Page no.39, S.No.02 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 7 requests per second: 1300,000 Layer 4 connection per second: 500,000Concurrent Connection: 38 MillionRSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power | Layer-7 RPS is not in line with the requirement of Layer-4 CPS, both should be in line with the requirement asked. As these appliances are purpose built appliance, asking the unnecessary RAM and Hard disk will not help for anything, it will unnecessarily increase the overall cost without any requirement.<br>**Request for change:-**Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 7 requests per second: 900,000Layer 4 connection per second: 500,000Concurrent Connection: 38 MillionRSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 SupportProcessor: Intel 12-core CPU, 32GB RAM, minimum 100GB SSD Disk and dual power supply.The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | supply.The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | | |
| **31** | “Specifications – B” Web Application Firewall with Server Load Balancer, Page no.41, S.No.18 | The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | ICSA certification is no longer available, it is discontinued now. **Request for change:-** The proposed solution should be PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | Please refer the revised specifications given below. |
| **32** | “Specifications – B” Web Application Firewall with Server Load Balancer, Page no.43, S.No.44 a | Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and | Signature protection, Anti-Virus should be part of dedicated solution; it can’t be added on top of ADC. **Request for change:-** Application load balance with functionality of Application delivery features, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | through) will be provided by High Court of M.P. | |
| **33** | Section – VII 7. Technical Specificatio ns s:- Network Monitoring System, Page No. 44, S.No.02 | The solution should automatically group servers that work closely together based on analysis of communication between them. | Requesting authority to amend the clause as follows: The solution should automatically group servers that work closely together based on an analysis of communication analysis or grouping criteria such as tags and types between them. | Please refer the revised specifications given below. |
| **34** | Section – VII7. Technical Specificatio | The solution should automatically build | Requesting authority to kindly revise the clause as this is OEM Specific and restrictive for other OEM to participate in this tender, suggested | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | ns s:- "Specifications – C", Network Monitoring System, Page No. 44, S.No.04 | visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | revised clause: " The solution should automatically build visualizations that shows dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities" | |
| **35** | Section – VII 7. Technical Specifications s:- "Specifications – C", Network Monitoring System, Page No. 45-46, S.No.36 | The solution should support extensive monitoring capabilities from an OS (Linux, Windows)/ platform standpoint and should provide capabilities for customer to develop, deploy customized monitoring requirements | Kindly amend the clause as follows: The solution should support extensive monitoring capabilities from an OS (Linux, Windows) and platform standpoint, and should provide options to deploy customized monitoring requirements. | Please refer the revised specifications given below. |
| **36** | Section – VII 7. Technical Specifications s:- "Specifications – C", Network Monitoring System, Page No. | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated | This clause is restrictive other eligible bidders to participate in the bid. Hence, we would request to kindly remove this clause. | Yes removed. |

| | | | | |
|---|---|---|---|---|
| | 48, S.No.74 | assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | | |
| **37** | Section – VII<br>7. Technical Specifications s:- "Specifications – C", Network Monitoring System, Page No. 49, S.No.86 | Consider options for transferring licenses between devices or reallocating licenses as needs change. | We understand that the license used for a network device should also be applicable to a server device when needed, provided the network device is removed from monitoring and provisioning on the server. This would allow the same license to be used for monitoring the server device. Could you please confirm if our understanding is correct? | Yes it refer the same meaning |
| **38** | Section – VII<br>7. Technical Specifications s:- "Specifications – C", Network Monitoring System, Page No. 49 | Suggestion to additional clause | The proposed NMS solution should be aligned with ITIL framework principles, certified with ITIL4 for Monitoring & Event Management and Capacity & Performance Management processes, and must include comprehensive documentation demonstrating compliance with these standards to ensure best practices in service management and operational excellence | No change. |
| **39** | Section – VII<br>7. Technical Specifications s:- "Specifications – C", | Suggestion to additional clause | The proposed NMS solution must comply with recognized security standards, including ISO 27001:2013/ ISO 27034, and CIS (Center for Internet Security) certifications, to ensure robust security management, secure software development, and | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Network Monitoring System, Page No. 49 | | adherence to best practices in information security. | |
| **40** | Section – VII Clause No- 7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-44 | The solution should automatically group servers that work closely together based on analysis of communication between them | Request you to modify the OEM specific clause as:The solution should automatically/Manually group servers that work closely together based on analysis of communication between them | Please refer the revised specifications given below. |
| **41** | Section – VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-44 | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | Please refer the revised specifications given below. |
| **42** | Section – VII Clause No-7. Technical Specificatio | The solution should be able to automatically detect software’s that are end of | Request you to modify the specific clause as:<br>The solution should be able to automatically/manually detect software’s that are end of support, | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | ns s Specifications – C” Network Monitoring System Page No.-44 | support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. | end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery.<br>As multiple software does not provide the required data on any standard protocol so please modify the clause as suggested | |
| **43** | Section – VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-45 | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to | Request you to provide more details on the software/application from which EMS application need to integrate | The bidder is requested to visit the High Court of M.P., Jabalpur for getting the real time details of same before the submission of bid document. |

| | | | | |
|---|---|---|---|---|
| | | third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | | |
| **44** | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-45 | The solution should be able to track connectivity between network endpoints and display the delay between nodes | As per our understanding here need to monitor the latency of all the nodes from application server, please clarify | Quote as per tender document. |
| **45** | Section – VII Clause No- 7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-48 | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | The required features is not the standard ask of NMS solution and can be achieved via ITSM solution, so please confirm here whether new ITSM need to propose here or NMS will be integrated with existing running ITSM solution.If Existing please provide OEM and version details of the ITSM solution. | Please refer the revised specifications given below. |
| **46** | Section – | It should be | The required features is not the | No change. |

| | | | | |
|---|---|---|---|---|
| | VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-44 | possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any node of the application. | standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | |
| **47** | | Additional | Request you to please provide the required details of the IT Infrastructure which will be monitored in NMS solution<br>1) No. Of servers:<br>i) Physical Server ii) VMs<br>iii) Physical server on which virtualization platform running.<br>2) No. & Make Of Network devices<br>i) Router/Switches/Firewall<br>ii) Wireless Controller /Wifi AP<br>iii) Storage<br>3) No. & Name Of Applications<br>4) No. Of containers. Or any other IP devices | The bidder is requested to visit the High Court of M.P., Jabalpur for getting the real time details of same before the submission of bid document. |
| **15. Business Automation (I) Pvt. Ltd.** | | | | |
| 1 | Pre-Qualification Terms | The bidder must be a certified company with the following ISO certifications:<br>○ **ISO 9001 :** Quality Management Systems<br>○ **ISO14001 :** Environmental Management Systems<br>○ **ISO 2000:** IT Service Management (or equivalent, such as ISO | Certification must be current and applicable to the services/products provided. Bidders are required to submit valid certification documents as part of their pre-qualification submission. | Quote as per tender document. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | 27001 for Information Security Management)<br>○ **ISO 27001 :** Information Security Management Systems |  |  |
| 2 |  | Certification Validity | The ISO certifications should be valid at the time of bid submission and must remain valid throughout the contract period. | Quote as per tender document. |
| 3 |  | Certification Bodies | Certifications must be issued by accredited and recognized certification bodies. | Quote as per tender document. |
| 4 |  | Non-Compliance | Failure to provide the required certifications or documentation may result in disqualification from the bidding process. | Quote as per tender document. |
| **16. Echelon Edge Pvt. Ltd.** |  |  |  |  |
| **1** | Specifications – C, Clause No 4, Page 44. | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | The term **"automatically build visualizations"** interprets that the proposed solution platform should be capable to provide visualizations that shows dependency between switches, routers, physical/virtual host Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. Please confirm whether our understanding is correct. | Please refer the revised specifications given below. |
| **2** | Specificatio | The Discovery | We understand that the proposed | Yes |

| | | | | |
|---|---|---|---|---|
| | ns – C, Clause No 7, Page 44. | solution should come with real-time dashboards that collate and present data that allows organizations to make decision on consolidation, re-use of infrastructure, detecting infrastructure that has never been used etc. | solution platform should support organizations to make correct & optimize decisions by providing real-time dashboards that collate and present data.<br>Could you please confirm if our understanding is correct? | |
| **3** | Specifications – C, Clause No 8, Page 44. | The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management | Since the clause already specifies that the "EMS/NMS platform must be integrated with a vulnerability management solution to identify blind spots in node security that may be overlooked by the vulnerability management system," we request that the scope of vulnerability detection be removed from the EMS/NMS requirements. Instead, we propose making it a separate clause to facilitate broader participation in the EMS/NMS scope. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | that are found to be active in discovery. | | |
| **4** | Specifications – C, Clause No 10, Page 44. | The solution should be able to do Virtual systems discovery (including Microsoft Hyper-V, vmware, etc.) Furthermore, it should support discovery of modern day DevOps platforms such as containers such as Docker, Runc, AIX WPARs and management solutions such as Kubernetes, Docker Swarm, Cloud Foundry and Open Shift. | Please confirm if any DevOps platforms are currently in use. If not, we kindly request that the clause be amended as follows: "The solution should be capable of discovering and monitoring virtual systems (including Microsoft Hyper-V, VMware, etc.) and management solutions such as Kubernetes, Docker Swarm, and Cloud Foundry." | Please refer the revised specifications given below. |
| **5** | Specifications – C, Clause No 17, Page 45. | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third | Please confirm whether protocols such as XML, SOAP, or SNMP Trap are currently in use. Additionally, let us know if there is an existing UNMS that needs to be integrated. If neither is applicable, we kindly request amending the clause to: "The solution should offer multiple integration methods for customers to integrate their own systems. Integration should support both northbound and southbound communication using various options, like REST API." | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML |  |  |
| **6** | Specifications – C, Clause No 66, Page 47. | System should support separate Rule Engine based alarms apart from the generic threshold.<br>a. Should have capability to configure Device Group based, Node Based, Resources/Interface based, and Aggregation link based.<br>b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information<br>c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms<br>d. Rules should have option configure the breach based on min, max and average values.<br>e. Should have option to configure rules n repeat counters<br>f. Should have | To encourage wider participation, we request amending the clause as follows:<br><br>"The system should have built-in functionality to define rules for alarms and monitoring, including real-time network flow, traffic utilization, and protocol distribution. It should support threshold-based alarms and monitoring for the following components:<br>a) Disk utilization<br>b) Bandwidth utilization<br>c) CPU utilization<br>d) Interface utilization" | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | options to select custom alarm and clear alarm messages for individual configured rules<br>g. Should have option to send severity levels like error, warning and information<br>h. Notifications support based on configured rules | | |
| **7** | Specifications – C, Clause No 74, Page 48. | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events, automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | The term "automatically assign deadlines to events" relates to SLA and escalation management, which typically requires an ITSM (IT Service Management) platform. Could you please confirm if our understanding is correct? | Yes removed. |
| **8** | Specificatio | Specify a base | Could you please confirm that a total | Quote as per |

| | | | | |
|---|---|---|---|---|
| | ns – C, Clause No 82, Page 49. | license for monitoring a minimum of 500 devices /application (Any kind of). Ensure the license is scalable up to 3,000 devices or applications without requiring a complete reinstallation or new licenses | of 3,000 device licenses should be considered from day one for preparing optimized hardware sizing and commercial proposals? If this is correct, could you please provide a breakdown of the device types and counts for additional device considerations? | tender document. Initially there is requirement of 500 licenses and the system should be scalable up to 3,000 devices or applications without requiring a complete reinstallation or new licenses. |
| **17. M/s Orbit Techsol India Pvt. Ltd.** | | | | |
| 1 | Specifications B, Page no. 39, Point no.2 | Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps | Due to license capping the OEMs have the advantage to quote higher for the incremental license which is not cost effective to customer. Hence request you to amend the point as "The ADC+WAF should be fully populated with the license throughput of 40 Gbps from Day-1." | Please refer the revised specifications given below. |
| 2 | Specifications B, Page no. 39, Point no.2 | Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. | To derive the performance number from the specific compute numbers does not decide performance of the device at all due to Different architecture, ASICS, FTGA cards etc have different hardware requirement which cannot be generalized for performance. Request you to change the required Processor to Intel Xeon 8-core or higher. | Please refer the revised specifications given below. |
| **18. M/s MDP Infra (India) Pvt. Ltd.** | | | | |
| 1 | Specifications – A - Firewall Technical Specifications s/ 4-Hardware Architecture | The appliance hardware should be a multicore CPU architecture and should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic | Reason for change: - Security appliance should be evaluated based on their security effectiveness, features, and functionality, rather than their architecture. The current clause seems to favor PC-based architecture, potentially excluding ASIC OEMs from the tender. We would like to emphasize that ASIC technology is no longer proprietary, as many leading OEMs are adopting it for its superior performance. Please refer to the URL below, which highlights that ASIC is not exclusive to Fortinet. Therefore, we request the | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one.<br>The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution | removal of this clause and suggest that MP High court to consider architectures based on their performance and security effectiveness.<br>https://community.cisco.com/t5/networking-blogs/the-new-era-of-wan-an-asic-innovation-story/ba-p/4175243<br>https://www.paloaltonetworks.com/network-security/hardware-firewall-innovations<br>https://blog.checkpoint.com/security/check-point-software-introduces-the-worlds-fastest-firewall-delivering-20-times-better-price-performance-to-the-worlds-most-demanding-datacenters/<br>Request for Change (NEW CLAUSE):<br>- The appliance hardware should be a multicore CPU architecture or should be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM. The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution |  |
| 2 | Specifications – A - Firewall Technical Specifications s/ 4-Hardware Architecture | OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one. | Reason for change: - ASCI solution does not require higher memory and CPU to deliver the desire functionality. Only PC based architecture require high memory. We suggest removing this clause as it is favoring single OEM devices. We empesize MP High court team to evaluate the Firewall solution based on the performance parameters Not memory and cPU<br>Request for Change (NEW CLAUSE):<br>- OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one or or should be proprietary ASIC based in nature to make sure all the security capabilities are provided without degradation from day one. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| 3 | Specifications – A - Firewall Technical Specifications s/5 Performance & Scalability | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | Reason for change: - Every OEM has different ways to measure the throughput values. We request to changes so all major OEM match this and can participate<br>Request for Change (NEW CLAUSE): - The NGFW throughput of the firewall should be a minimum 15 (enterprise mix /Real world with logging enabled ) OR Application throughput measured with 64K http minimum 20Gbps. Threat prevention throughput minimum 10Gbps (Enterprise Mix / Real World with logging enabled) | Please refer the revised specifications given below. |
| 4 | | It is highly recommended to ask SSL inspection throughput. This is important parameters to size the right box. Because lower SSL inspection throughput can degrade the performance while complete inspection of the packet is enabled. | Request for Change (NEW CLAUSE): - Minimum 10Gbps of SSL inspection throughput and 500K SSL inspection concurrent session support | Please refer the revised specifications given below. |
| 5 | | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions | Reason for change: - Most of the OEM is publish the connection per second and concurrent session in TCP. It's highly recommended on the basis of the ports count that the connections requirement must be higher so devices not become bottle neck. Asking the lower connections is favoring specific OEM model.<br>Request for Change (NEW CLAUSE): | Please refer the revised specifications given below. |
| 6 | Specifications – A - Firewall Technical | NGFW Firewall should support at least 150,000 connections per | | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Specifications s/6 -Next Gen Firewall Features | second L3/L4 or New Layer 7 connections per second – Min 90000 | - Min 500K Connection per Second and 5M concurrent connections | |
| 7 | | Should support more than 19,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's | Reason for change: - favoring to specific OEM signature count.<br>Request for Change (NEW CLAUSE): Request to make changes and allow min 10000 Signatures. | Please refer the revised specifications given below. |
| 8 | | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 75+ categories | Reason for change: - Every OEM has different counts and categories. This is favoring to specific OEM nos.<br>Request for Change (NEW CLAUSE): - Request to remove this clause | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | from day1. | | |
| 9 | Specifications – A - Firewall Technical Specifications s/11- DNS Security | The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1. | Reason for change: - Favouring to Specific OEM.<br>Request for Change (NEW CLAUSE): - The Solution should support DNS security in line mode/proxy mode. Necessary licenses to be included from day 1. | Please refer the revised specifications given below. |
| 10 | | DNS security 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. | Reason for change: - Every OEM has different counts in threat intelligence asking specific favoring to specific OEM.<br>Request for Change (NEW CLAUSE): - Request to remove 10M malicious domain | Please refer the revised specifications given below. |
| 11 | | The solution should integrate and correlate to provide effective prevention against. New C2 domains, file download source domains, and domains in malicious email links.<br>Integrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators.<br>Should have OEM human-driven adversary tracking and malware reverse engineering, including insight | Reason for change: - Favoring to Specific OEM: Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots.<br>Should take inputs from at least 25 third-party sources of threat intelligence<br>Request for Change (NEW CLAUSE): - Request to remove this clause | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence. | | |
| 12 | Specifications – B Web Application Firewall with Server Load Balancer/Point 2/Page no.39 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.<br>Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps<br>Layer 7 requests per second: 1300,000<br>Layer 4 connection per second: 500,000<br>Concurrent Connection: 38 Million RSA CPS (2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance | Traffic Ports support: As per the present data centre/It infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for ADC/WAF/SLB deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amending this clause.<br>Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. Please amend this clause.<br>Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. Please amend this clause.<br>It is suggested to amend the clause as :-<br>Traffic Ports support: 8 x 10 GE SFP+ from day-1<br>Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps<br>Layer 7 requests per second : 5 million<br>Layer 4 connections per second: 3 Million<br>RSA CPS(2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU or equivalent or better<br>Concurrent Connections: 40 Million<br>Processor - Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | | |
| 13 | Specifications – B Web Application Firewall with Server Load Balancer/Point 6/Page no.40 | The proposed ap pliance should s upport the below metrics:<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | Different OEM has different terminology and technique to achieve similar function. We would like to request the honorable tendering committee to use vendor agnostic terminology for wider participation.<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash/Equivalent<br>— Weighted Hash/Equivalent<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | Please refer the revised specifications given below. |
| 14 | Specifications – B Web Application Firewall with Server Load Balancer/Point 7/Page no.40 | Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses | Virtual Matrix Architecture feature is specific to one ADC OEM. Kindly remove this clause for wider participation and for other points please allow similar or equivalent feature metrics for broader participation. Following Load Balancing Topologies should be supported:<br>• Client Network Address Translation (Proxy IP) /Equivalent<br>• Mapping Ports /Equivalent<br>• Direct Server Return /Equivalent<br>• One Arm Topology Application /Equivalent<br>• Direct Access Mode /Equivalent<br>• Assigning Multiple IP Addresses /Equivalent<br>• Immediate and Delayed Binding /Equivalent | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | • Immediate and Delayed Binding |  |  |
| 15 | Specifications –B Web Application Firewall with Server Load Balancer/Point 31/Page no.43 | The proposed appliance/software should be EAL2 certified. | For wider participation, We would like to request the honorable tendering committee to amend the clause as requested.<br>"The proposed appliance/software should be EAL2 certified/Make in India" | Please refer the revised specifications given below. |
| 16 | Specifications –B Web Application Firewall with Server Load Balancer/Point 34/Page no.43 | Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | In order to switch over the applications traffic like web app, email app etc. the GSLB solution must understand all types of DNS records and not just A or AAAA. Kindly add following functionality for complete Solution. It is suggested to amend this clause as :-<br>The Proposed Solution must have Global Server Load Balancing and should be able to host SRV Records, AAAA Records, A , PTR , MX ,TXT ,SOA, NS, Dname, Dmarc Records and should also support DNSSEC. | Please refer the revised specifications given below. |
| 17 | Specifications – B Web Application Firewall with Server Load Balancer/Point 44 a/Page no.44 | Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support | IPS is completely different technology even deployment is different. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics, Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support<br>and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support.<br>Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | Jabalpur.<br>The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P" | |
| 18 | Specifications – C" Network Monitoring System | The solution should be able to do Virtual systems discovery (including Microsoft Hyper-V, vmware, etc.) Furthermore, it should support discovery of | Please rephrase this as "The solution should be able to do Virtual systems discovery (including Microsoft Hyper-V, vmware, etc.) Furthermore, it should support discovery of modern day DevOps platforms such as containers and management solutions such as Kubernetes, Docker Swarm, and Open Shift." | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | modern day DevOps platforms such as containers such as Docker, Runc, AIX WPARs and management solutions such as Kubernetes, Docker Swarm, Cloud Foundry and Open Shift. |  |  |
| 19 | Specifications – C" Network Monitoring System | Discovers in-depth configuration data for storage systems, pools, volumes, disks drives, LUNS, File Systems | This section is related to Storage Device management and it is written under "Network Monitoring System" section, hence requesting you to remove this point from Network Monitoring System section and be included in "Storage Device requirement", where Element Management System is embedded & packaged by OEM, along with the Storage devices for monitoring physical and virtual storage infrastructure. | Yes removed. |
| 20 | Specifications – C" Network Monitoring System | The solution should support monitoring various attributes (at least 50+) in Tomcat, Web Sphere MQ, Apache HTTP, IIS, and WAS. | Please rephrase this as "The solution should support monitoring various attributes in Tomcat, Web Sphere MQ, Apache HTTP, IIS, and WAS." | Yes changed. |
| 21 | Specifications – C" Network Monitoring System | The solution should be able to report on hardware details (like CPU, memory, fan state, power etc.) of servers from multi vendors like IBM,<br>HP, Cisco, Dell and also VMware Hosts. | The Hardware Element Manager is embedded & packaged by OEM which is benchmarked by OS to capture the core elements in the event of hardware or software malfunctions, crashes, failures etc. Hence, requesting you to remove these points from Network Monitoring System section and be included in "Server Hardware requirement". In order to have single pane of glass, the meaningful events from Hardware Element Manager can be integrated into Network Monitoring System for event consolidation purposes. | No change. The vendor can quote better solution. |

| | | | | |
|---|---|---|---|---|
| 22 | Specifications – C” Network Monitoring System | The solution should be able to gather capacity data from vCenter, HMC, Physical servers, etc. Generate report and provide recommendation. | Please rephrase this as "The solution should be able to gather capacity data from vCenter, Physical servers, etc. Generate report and provide recommendation." | Yes changed. |
| 23 | Specifications – C” Network Monitoring System | The solution should be able to monitor disk elements like RAID controllers, hard disks, RAIDs, failure prediction, availability of the volumes. | The Hardware Element Manager is embedded & packaged by OEM which is benchmarked by OS to capture the core elements in the event of hardware or software malfunctions, crashes, failures etc. Hence, requesting you to remove these points from Network Monitoring System section and be included in "Server Hardware requirement". In order to have single pane of glass, the meaningful events from Hardware Element Manager can be integrated into Network Monitoring System for event consolidation purposes. | The vendor can quote better solution / option. |
| 24 | Specifications – C” Network Monitoring System | The solution should be able to monitor environment metrics like temperature, internal voltages, power supplies, fans. | The Hardware Element Manager is embedded & packaged by OEM which is benchmarked by OS to capture the core elements in the event of hardware or software malfunctions, crashes, voltage failures etc. Hence, requesting you to remove these points from Network Monitoring System section and be included in "Server Hardware requirement". In order to have single pane of glass, the meaningful events from Hardware Element Manager can be integrated into Network Monitoring System for event consolidation purposes. | The vendor can quote better solution / option. |
| 25 | Specifications – C” Network Monitoring System | The solution should be able to monitor critical hardware components like processors, memory modules, ECC | The Hardware Element Manager is embedded & packaged by OEM which is benchmarked by OS to capture the core elements in the event of hardware or software malfunctions, crashes, ECC failures, voltage etc. Hence, requesting you to remove these points from Network | The vendor can quote better solution / option. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | errors, failure prediction. | Monitoring System section and be included in "Server Hardware requirement". In order to have single pane of glass, the meaningful events from Hardware Element Manager can be integrated into Network Monitoring System for event consolidation purposes. |  |
| 26 | Specifications – C” Network Monitoring System | Storage Monitoring | This section is related to Storage Device management and it is written under "Network Monitoring System" section, hence requesting you to remove this point from Network Monitoring System section and be included in "Storage Device requirement", where Element Management System is embedded & packaged by OEM, along with the Storage devices for monitoring physical and virtual storage infrastructure. | The vendor can quote better solution. |
| 27 | Specifications – C” Network Monitoring System | Logging/Reporting/Alert/threshold | This section is related to Log management and it is written under "Network Monitoring System" section, hence requesting you to remove these point from Network Monitoring System section and be included in "Additional Capability requirement" | No change. |
| 28 | Specifications – C” Network Monitoring System | Capacity Reservations: tool should allow management of resource allocations and reservations (for services, applications or other needs), identify resource shortages and provide information for further analysis or procurement | The Hardware Element Manager is embedded & packaged by Server / Storage / Network OEM which is benchmarked by OEM to capture the core elements like Hardware alerts, crashes, capacity reserves etc. Hence, requesting you to remove these points from Network Monitoring System section and be included in "Additional Capability requirement". In order to have single pane of glass, the meaningful events from Hardware Element Manager can be integrated into Network Monitoring System for event consolidation purposes. | Optional. |
| 29 | Specifications – C” Network Monitoring System |  | **Suggestion: -** The proposed EMS solution should adhere to Micro services and thus be built on modern container technologies, and have an options to deploy on classic mode (non-containerized) as well as containerized (like Docker, | The vendor can quote better solution / higher side. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | Kubernetes) mode. The solution should either support built-in Kubernetes technology or Bring Your Own Kubernetes (BYOK) platform provided by the bidder. +D36 **Reason for Suggestion: -** Containers are a newer technology and it run isolated from each other, with each of them possessing its own level of security and remaining unharmed. Traditional applications are not properly isolated from each other within a VM, giving scope for a malicious program to penetrate and control others. As the government has some of the most sensitive information in the devices, services, and other products used by them must be at the highest level of security at all times. |  |
| 30 | Specifications – C” Network Monitoring System |  | **Suggestion: -** The proposed EMS OEM must have necessary ISO 27001, ISO 27034 certification and FIPS 140-2 compliance to ensure security compliances. **Reason for Suggestion: -** The proposed EMS OEM must have necessary ISO certifications and FIPS compliance to ensure security compliances. FIPS 140-2 compliant, which ensures that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. | Please refer the revised specifications given below. |
| 31 | Specifications – C” Network Monitoring System |  | **Suggestion: -** The proposed NMS solution should provide out of the box Risk Visibility Dashboards of network infrastructure. With this risk visibility dashboard, we see the most offending devices in the group along with the types of unauthorized access attempts, and the percentage of non-compliant devices. Please confirm if the stated network compliance requirement is desired as part of NMS specifications s? | The vendor can quote higher side /better solution. |
| 32 | Specifications – C” Network Monitoring System |  | **Suggestion: -** The proposed NMS solution should have diagnostic analytics capability that able to visually correlate performance and configuration changes of all network | The vendor can quote higher side /better solution. |

| | | | | |
|---|---|---|---|---|
| | | | issues. It overlays real-time network configuration change events on network performance graphs to correlate and reduce troubleshooting time. Please confirm if the stated network diagnostics requirement is desired as part of NMS specifications s? | |
| 33 | Specifications – C" Network Monitoring System | | **Suggestion: -** The proposed NMS solution should be capable of managing upto 30K devices from a single instance , should be able to have 1 mil discovered interfaces. Please confirm if the proven network scalability is desired as part of NMS specifications s? | The vendor can quote higher side /better solution. |
| 34 | Specifications – C" Network Monitoring System | | **Suggestion: -** The solution provides ready-to-use, out-of-the-box network focused orchestration content built using industry standards and vendor best practices that can be easily ported between dev, test and production environments. Please confirm if the stated network automation requirement is desired as part of NMS specifications s? | The vendor can quote higher side /better solution. |
| **19. M/s Intek Micro Systems Pvt. Ltd.** | | | | |
| 1 | Web Application Firewall with Server Load Balancer/Point 2/Page no.39 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.<br>Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps<br>Layer 7 requests per second: 1300,000 | Traffic Ports support: As per the present data center /It infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for ADC/WAF/SLB deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amending this clause.<br>Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. Please amend this clause.<br>Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. Please amend this clause.<br>It is suggested to amend the clause as :-<br>Traffic Ports support: 8 x 10 GE SFP+ from day-1 | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Layer 4 connection per second: 500,000<br>Concurrent Connection: 38 Million<br>RSA CPS (2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps<br>Layer 7 requests per second : 5 million<br>Layer 4 connections per second: 3 Million<br>RSA CPS(2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU or equivalent or better<br>Concurrent Connections: 40 Million<br>Processor - Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | |
| 2 | Web Application Firewall with Server Load Balancer /Point 6 /Page no.40 | The proposed ap pliance should s upport the below metrics:<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | Different OEM has different terminology and technique to achieve similar function. We would like to request the honorable tendering committee to use vendor agnostic terminology for wider participation.<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash/Equivalent<br>— Weighted Hash/Equivalent<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | Please refer the revised specifications given below. |
| 3 | Web Application | Following Load Balancing | Virtual Matrix Architecture feature is specific to one ADC OEM. Kindly | Please refer the revised |

| | | | | |
|---|---|---|---|---|
| | Firewall with Server Load Balancer/Point 7/Page no.40 | Topologies should be supported:<br>Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | remove this clause for wider participation and for other points please allow similar or equivalent feature metrics for broader participation<br>Following Load Balancing Topologies should be supported:<br>• Client Network Address Translation (Proxy IP) /Equivalent<br>• Mapping Ports /Equivalent<br>• Direct Server Return /Equivalent<br>• One Arm Topology Application /Equivalent<br>• Direct Access Mode /Equivalent<br>• Assigning Multiple IP Addresses /Equivalent<br>• Immediate and Delayed Binding /Equivalent | specifications given below. |
| 4 | Web Application Firewall with Server Load Balancer /Point 31/Page no.43 | The proposed appliance/software should be EAL2 certified. | For wider participation, We would like to request the honorable tendering committee to amend the clause as requested.<br>"The proposed appliance/software should be EAL2 certified/Make in India" | Please refer the revised specifications given below. |
| 5 | Web Application Firewall with Server Load Balancer/Point 34/Page no.43 | Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | In order to switch over the applications traffic like web app, email app etc. the GSLB solution must understand all types of DNS records and not just A or AAAA. Kindly add following functionality for complete Solution. It is suggested to amend this clause as :-<br>The Proposed Solution must have Global Server Load Balancing and should be able to host SRV Records, AAAA Records, A, PTR, MX, TXT, SOA, NS, Dname, Dmarc Records and should also support DNSSEC. | Please refer the revised specifications given below. |
| 6 | Web Application Firewall with Server Load Balancer/Po | Application load balance with functionality of Application delivery features , | IPS is completely different technology even deployment is different. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | int 44 a/Page no.44 | Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support.<br>Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur.<br>The WAF/ADC should support to store all log of minimum 8months period on external | load balance with functionality of Application delivery features, Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur.<br>The WAF/ADC should support to store all log of minimum 8months period<br>on external storage such as NAS/SAN. The required external storage<br>(Hitachi VSP E590H through) will be provided by High Court of M.P" | |

| | | | | |
|---|---|---|---|---|
| | | storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | | |
| **20. M/s CCS Computers Pvt Ltd.** | | | | |
| 1 | Section – VII Clause No-7. Technical Specificatio ns s Specificatio ns – C" Network Monitoring System Page No.-44 | The solution should automatically group servers that work closely together based on analysis of communication between them | Request you to modify the OEM specific clause as:<br>The solution should automatically/Manually group servers that work closely together based on analysis of communication between them | Please refer the revised specifications given below. |
| 2 | Section – VII Clause No-7. Technical Specificatio ns s Specificatio ns – C" Network Monitoring System Page No.-44 | The solution should automatically build visualizations that shows dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | The required features is not the standard ask of EMS module and to achive this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
| 3 | Section – VII Clause No- 7. Technical Specifications s Specifications – C" Network Monitoring System Page No.- 44 | The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. | Request you to modify the specific clause as:<br>The solution should be able to automatically/manually detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery.<br>As multiple software does not provide the required data on any standard protocol so please modify the clause as suggested | Please refer the revised specifications given below. |
| 4 | Section –VII Clause No- 7. Technical Specifications s Specifications – C" Network Monitoring System Page No.- 45 | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, | Request you to provide more details on the software/application from which EMS application need to integrate | The bidder is requested to visit the High Court of M.P., Jabalpur for getting the real time detail of same before the submission of bid document. |

| | | | | |
|---|---|---|---|---|
| | | XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | | |
| 5 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-45 | The solution should be able to track connectivity between network endpoints and display the delay between nodes | As per our understanding here need to monitor the latency of all the nodes from application server, please clarify | Quote as per tender document. |
| 6 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-48 | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to | The required features is not the standard ask of NMS solution and can be achieved via ITSM solution, so please confirm here whether new ITSM need to propose here or NMS will be integrated with existing running ITSM solution.<br>If Existing please provide OEM and version details of the ITSM solution. | Removed. |

| | | | | |
|---|---|---|---|---|
| | | combine a set of different events into one major event | | |
| 7 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.- 44 | It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any<br>node of the application. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | No change. |
| 8 | | Additional | Request you to please provide the required details of the IT Infrastructure which will be monitored in NMS solution.<br>1) No. Of servers :<br>i) Physical Server<br>ii) VMs<br>iii) Physical server on which virtualization platform running.<br>2) No. & Make Of Network devices<br>i) Router/Switches/Firewall<br>ii) Wireless Controller /Wi-Fi AP<br>iii) Storage<br>3) No. & Name Of Applications<br>4) No. Of containers.<br>Or any other IP devices | Already clarified above. |
| 9 | Web Application Firewall with Server Load Balancer/Point 2/Page no.39 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be | Traffic Ports support: As per the present data centre/IT infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for ADC/WAF/SLB deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amending this clause.<br>Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | used). All transceivers (SM) from day1.<br>Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps<br>Layer 7 requests per second: 1300,000<br>Layer 4 connection per second: 500,000<br>Concurrent Connection: 38 Million<br>RSA CPS (2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | per second requirement is lower side. please amend this clause.<br>Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. Please amend this clause.<br>It is suggested to amend the clause as :-<br>Traffic Ports support: 8 x 10 GE SFP+ from day-1<br>Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps<br>Layer 7 requests per second : 5 million<br>Layer 4 connections per second: 3 Million<br>RSA CPS(2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU or equivalent or better<br>Concurrent Connections: 40 Million<br>Processor - Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | |
| 10 | Web Application Firewall with Server Load Balancer/Point 6/Page no.40 | The proposed ap pliance should s upport the below metrics:<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least | Different OEM has different terminology and technique to achieve similar function. We would like to request the honorable tendering committee to use vendor agnostic terminology for wider participation.<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash/Equivalent<br>— Weighted Hash/Equivalent<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin, | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | — Response Time,<br>— Bandwidth, etc | |
| 11 | Web Application Firewall with Server Load Balancer/Point 7/Page no.40 | Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | Virtual Matrix Architecture feature is specific to one ADC OEM. Kindly remove this clause for wider participation and for other points please allow similar or equivalent feature metrics for broader participation.<br>Following Load Balancing Topologies should be supported:<br>• Client Network Address Translation (Proxy IP) /Equivalent<br>• Mapping Ports /Equivalent<br>• Direct Server Return /Equivalent<br>• One Arm Topology Application /Equivalent<br>• Direct Access Mode /Equivalent<br>• Assigning Multiple IP Addresses /Equivalent<br>• Immediate and Delayed Binding /Equivalent | Please refer the revised specifications given below. |
| 12 | Web Application Firewall with Server Load Balancer /Point 31 /Page no.43 | The proposed appliance/software should be EAL2 certified. | For wider participation, We would like to request the honorable tendering committee to amend the clause as requested.<br>"The proposed appliance/software should be EAL2 certified/Make in India" | Please refer the revised specifications given below. |
| 13 | Web Application Firewall with Server Load Balancer/Point 34/Page no.43 | Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | In order to switch over the applications traffic like web app, email app etc. the GSLB solution must understand all types of DNS records and not just A or AAAA. Kindly add following functionality for complete Solution. It is suggested to amend this clause as :-<br>The Proposed Solution must have Global Server Load Balancing and | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | | should be able to host SRV Records, AAAA Records, A , PTR , MX , TXT, SOA, NS, Dname, Dmarc Records and should also support DNSSEC. | |
| 14 | Web Application Firewall with Server Load Balancer/Point 44 a/Page no.44 | Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the | IPS is completely different technology even deployment is different. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur.<br>The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P" | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | | |
| **21. M/s ITSC** | | | | |
| 1 | Specifications – B" Web Application Firewall with Server Load Balancer Clause No 1 Page 39 | The proposed appliance should be a dedicated ADC/WAF/SLB appliance having DDoS protection, SSL inspection, and real-time threat intelligence, it should not be part of any Firewall or UTM. | DDoS protection should be provided with the help of stateless appliance as it doesn't maintain any session table, this is first and foremost criteria to choose DDoS protection appliance. ADC/WAF/SLB is state full appliance; hence DDoS should not be part of ADC/WAF/SLB. Suggested Clause: The proposed appliance should be a dedicated ADC/WAF/SLB appliance having SSL inspection, and real-time threat intelligence. It should not be part of any Firewall or UTM | The vendor may provide DDoS Protection with the help of any devices /software if the DDoS protection not available in dedicated ADC/WAF/SLB appliance. |
| 2 | Specifications – B" Web Application Firewall with Server Load Balancer Clause No 2 Page 39 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally, should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. Device L4 Throughput: 20 Gbps and | Layer-7 RPS is not in line with the requirement of Layer-4 CPS, both should be in line with the requirement asked. As these appliances are purpose-built appliance, asking the unnecessary RAM and Hard disk will not help for anything, it will unnecessarily increase the overall cost without any requirement. Suggested Clause: Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally, should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1. Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 7 requests per | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | scalable upto 40 Gbps Layer 7 requests per second: 1300,000 Layer 4 connection per second: 500,000 Concurrent Connection: 38 Million RSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | second: 900,000 Layer 4 connection per second: 500,000 Concurrent Connection: 38 Million RSA CPS (2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU, 32GB RAM, minimum 100GB SSD Disk and dual power supply. The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | |
| 3 | Specifications – B" Web Application Firewall with Server Load Balancer Clause No 18 Page 41 | The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | ICSA certification is no longer available, it is discontinued now. Suggested Clause: The proposed solution should be PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | Please refer the revised specifications given below. |
| 4 | Specifications – B" Web Application Firewall with Server Load | Application load balance with functionality of Application delivery features, Antivirus, IP | Signature protection, Anti-Virus should be part of dedicated solution; it can't be added on top of ADC. Suggested Clause: Application load balance with functionality of Application delivery features, IP Reputation, WAF Security, Credential | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Balancer Clause No 44 a Page 43 | Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero-day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipment's must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as | Stuffing Defense, Zero-day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipment's must come with 5-year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | |

| | | | | |
|---|---|---|---|---|
| | | NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | | |
| 5 | Specifications - A Firewall Technical Specifications Clause no 2 Pg 32 | The proposed firewall vendor must have over 97% of Exploit Block rate in latest NGFW NSS Lab Test report. | The NSS lab has last published the report in 2019. The Lab is no longer operational. Hence we request you to modify the clause as suggested. Suggested Clause: "The firewall solution be should be NSS labs recommended / SE Labs recommended or equivalent" | Removed. |
| 6 | Specifications - A Firewall Technical Specifications s Clause no 3 Pg 32 | 6 X 10G Copper/RJ45 Day 1 8 X 1/10G SFP/SFP+ Day 1 with LR/SM transceivers and 8x3m patch cords. 4X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one Minimum 2 x 10G HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management Port | The asked interfaces are high in number and this will lead to price escalation. We request you to modify the clause as suggested to allow us to participate and be price competitive. Suggested Change: 8x1G Copper / RJ45 Day 1, 8x1/10G/25G SFP/SFP+ Day 1 with 4x10G and 4x25G SR / MM transceivers and 8 x 3m patch cords from day 1. The firewall should have a free slot for future expansion to support 40/100 interfaces as needed. | Please refer the revised specifications given below. |
| 7 | Specifications - A Firewall Technical Specifications s Clause no 16 Pg 38 | "Bidder has to propose on premise dedicated logging, analytics & reporting solution from same OEM (Virtual /Physical Appliance) from day1, the logging solution | Our logging appliance has certain storage. The log size will depend on the type of logging enabled and the volume of logs. For exporting the logs to external storage, there is a need for syslog server. We request you to provide a syslog server which will be mapped to the external storage. | The syslog server will be provided by the High Court. |

| | | | | |
|---|---|---|---|---|
| | | to be deployed at Data Center only. In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P.<br>Required Features:<br>Should Deliver single-pane visibility, also have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance reports in different formats. The solution should | | |

| | | | | |
|---|---|---|---|---|
| | | have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics /event correlation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained models and traffic classifiers. The same should be available on public website to validate the capabilities". | | |
| **Pre-Bid Query For The Network Monitoring System** | | | | |
| 1 | "Specifications – C" Network Monitoring System/ Servers &System Monitoring/ 35/Pg No.45 | The solution should allow monitoring of Server Status and Availability, CPU Utilization, Memory Utilization, Process Monitoring, File System Monitoring, Disk | Please consider remove "2008.2012", Only OEM supported O.S can be supported | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Utilization of RHEL/Centos, SUSE, Ubuntu servers/Windows 2008, 2012,2016,2019, 2022. | | |
| 2 | “Specifications – C” Network Monitoring System/ Servers & System Monitoring/ 17/Pg No.45 | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | Please consider removing "XML, SOAP& Trap" as RestAPI based integration is the industry best practice and modify the point to "Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI on each module level. Any faultdetails should be able to send to third party CRM, Customer Portal,UNMS or even EMS if needed." | Please refer the revised specifications given below. |
| 3 | “Specifications – C” Network Monitoring System/ Servers & System Monitoring/ 40/Pg No.46 | The solution should be able to gather capacity data from vCenter, HMC, Physical servers, etc. Generate report and provide recommendation | Please elaborate what kind of recommendations is expected from the solution? | Please refer the revised specifications given below. |
| 4 | “Specifications – C” Network Monitoring System/ | The proposed solution should be able to monitor the availability, | Please consider removing end point devices like desktop to "The proposed solution should be able to monitor the availability, health and performance of physical | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Servers & System Monitoring/ Pg No.43 | health and performance of physical servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, end point devices like desktop, Kiosks, display boards, URL monitoring, other snmp enabled devices like UPS and AC from single dash board. | servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, Kiosks, display boards, URL monitoring, other snmp/ping enabled devices like UPS and AC from single dash board." | |
| 5 | “Specifications – C” Network Monitoring System/ Storage Monitoring/ 40/Pg No.46 | The solution should show storage growth rates and project when the storage capacity will be reached | Please consider removing this point | Yes removed. |
| 6 | “Specifications – C” Network Monitoring System/Logging/Reporting/Alert/threshold/65/Pg No.47 | Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement | Different OEM's have different level of severity definitions. | Please refer the revised specifications given below. |
| 7 | “Specifications – C” Network Monitoring System/ | Capacity Reservations: tool should allow management of resource | Please consider removing this specifications . | Yes made Optional. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | System/ Another Features/72 /Pg No.48 | allocations and reservations (for services, applications or other needs), identify resource shortages and provide information for further analysis or procurement |  |  |
| 8 | “Specifications – C” Network Monitoring System/ Licensing/80/Pg No.49 | The licenses should be perpetual with 05 years support /updates /upgrade. | Please consider modifying to "The licenses should be On Prem Subscription with 05 years support /updates /upgrade." | Please refer the revised specifications given below. |
| 9 | “Specifications – C” Network Monitoring System/ Note/4/Pg No.49 | The bidder has to quote only 01 product of single make / brand at a time and not multiple brands for same item. | Please consider removing this specifications as EMS based OEM's do not provide solutions for Web Application Firewall with Server Load Balancer. | Yes removed. |
| 10 | “Specifications – C” Network Monitoring System/ Discovery/15/Pg No.44 | Provides provision to draw & map user specific network diagram | Please consider modifying the specifications to "The tool should enable business users or administrators to efficiently design and modify the service model (network diagram) using templates " | Please refer the revised specifications given below. |
| 11 | Additional points to be considered | The bidder should be allowed to quote for individual line item | L1 should be considered for the individual line item. | Yes accepted. |
| 12 | Additional points to be considered | Product demonstration should be called before the finalization of the Technical bid | This will help in evaluating the product as per the requirement of the High Court. | Yes accepted. |
| **22. M/s SISL Infotech Private Limited** |  |  |  |  |
| 1 | Section - VII 7.Technical Specifications / Specifications - B/ Web | Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps | Due to license capping the OEMs have the advantage to quote higher for the incremental license which is not cost effective to customer. Hence request you to amend the point as "The ADC+WAF should be fully populated with the license throughput | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Application Firewall with Server Load Balancer / Point No.2 Page No. 39 | | of 40 Gbps from Day-1" | |
| 2 | Section - VII 7.Technical Specifications / Specifications - B/ Web Application Firewall with Server Load Balancer / Point No.2 Page No. 39 | Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. | To derive the performance number from the specific compute numbers does not decide performance of the devices at all due to Different architecture, ASICS, FTGA cards etc have different hardware requirement which cannot be generalized for performance. Request you to change the required processor to Intel Xeon 8-core or higher. | Please refer the revised specifications given below. |
| 3 | Section - VII 7.Technical Specifications / Specifications - A/ Firewall Technical Specificatio ns s / Point No.4 Page No. 32 | The appliance hardware should be a multicourse CPU architecture and should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security | Security appliance should be evaluated based on their security effectiveness, features, and functionality, rather than their architecture. The current clause seems to favor PC-based architecture, potentially excluding ASIC OEMs from the tender. We would like to emphasize that ASIC technology is no longer proprietary, as many leading OEMs are adopting it for its superior performance. Please refer to the URL below, which highlights that ASIC is not exclusive to Fortinet. Therefore, we request the removal of this clause and suggest that MP High court to consider architectures based on their performance and security effectiveness.<br>Therefore Request to amend to new clause as below:<br>The appliance hardware should be a multicore CPU architecture or should be proprietary ASIC based in nature & should be open architecture based | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | capabilities are provided without degradation from day one. The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution | on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM<br>The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution |  |
| 4 | Section - VII 7.Technical Specifications / Specifications - A/ Firewall Technical Specifications s / Point No.4<br>Page No. 32 | OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one. | ASCI solution does not require higher memory and CPU to deliver the desire functionality. Only PC based architecture require high memory. We suggest removing this clause as it is favoring single OEM devices. We emphasize MP High court team to evaluate the Firewall solution based on the performance parameters Not memory and CPU.<br>Therefore request to amend to new clause as:<br>OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one or or should be proprietary ASIC based in nature to make sure all the security capabilities are provided without degradation from day one. | Please refer the revised specifications given below. |
| 5 | Section - VII 7.Technical Specifications / Specifications - A/ Firewall Technical Specifications s / Point No.5<br>Page No. 32 | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention | Every OEM has different ways to measure the throughput values. We request to changes so all major OEM match this and can participate Therefore request to amend to new clause as:<br>The NGFW throughput of the firewall should be a minimum 15 (enterprise mix /Real world with logging enabled) OR Application throughput measured with 64K http minimum 20Gbps. Threat prevention throughput minimum 10Gbps ( Enterprise Mix / Real World with logging enabled) | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | /NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | | |
| 6 | Section - VII<br>7.Technical Specifications / Specifications - A/ Firewall Technical Specifications s / Point No.5<br>Page No. 32 | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions<br>NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 connections per second – Min 90000 | Most of the OEM is publish the connection per second and concurrent session in TCP. It's highly recommended on the basis of the ports count that the connections requirement must be higher so device not becomes bottle neck. Asking the lower connections is favoring specific OEM model.<br>Therefore request for modifying to Min 500K Connection per Second and 5M concurrent connections | Please refer the revised specifications given below. |
| 7 | Section - VII<br>7.Technical Specifications / Specifications - A/ Firewall Technical Specifications s / Point No.6<br>Page No. 33 | Should support more than 19,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's | Favoring to specific OEM signature count.<br>Therefore request for modifying to allow min 10000 Signatures. | Please refer the revised specifications given below. |
| 8 | Section - VII<br>7.Technical Specificatio | Should support Reputation- and category-based | Every OEM has different counts and categories. This is favoring to specific OEM nos. | Please refer the revised specifications |

| | | | | |
|---|---|---|---|---|
| | ns / Specifications - A/ Firewall Technical Specifications s / Point No.7 Page No. 35 | URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 75+ categories from day1. | Request to remove this clause | given below. |
| 9 | Section - VII 7.Technical Specifications / Specifications - A/ Firewall Technical Specifications s / Point No.11 Page No. 36 | The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1. | Favoring to Specific OEM Therefore request to amend to new clause as:<br>The Solution should support DNS security in line mode/proxy mode. Necessary licenses to be included from day 1. | Please refer the revised specifications given below. |
| 10 | Section - VII 7.Technical Specifications / Specifications - A/ Firewall Technical Specifications s / Point No.11 Page No. 36 | DNS security 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. | Every OEM has different counts in threat intelligence asking specific favoring to specific OEM.<br>Request to remove 10M malicious domain | Please refer the revised specifications given below. |
| 11 | Section - VII 7.Technical Specifications / Specifications - A/ Firewall Technical Specificatio | The solution should integrate and correlate to provide effective prevention against. New C2 domains, file download source domains, and | Favoring to Specific OEM: Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | ns s / Point No.11 Page No. 36 | domains in malicious email links.<br>Integrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots. Should take inputs from at least 25 third-party sources of threat intelligence. | Request to remove this clause. | |
| 12 | Section – VII Clause No-7. Technical Specificatio ns s Specificatio ns – C" Network Monitoring System Page No.-44 | The solution should automatically group servers that work closely together based on analysis of communication between them | Request you to modify the OEM specific clause as:<br>The solution should automatically /Manually group servers that work closely together based on analysis of communication between them | Please refer the revised specifications given below. |
| 13 | Section – VII Clause No-7. Technical Specificatio ns s Specificatio ns – C" Network Monitoring System Page No.- | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | 44 | storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | | |
| 14 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-44 | The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. | Request you to modify the specific clause as:<br>The solution should be able to automatically /manually detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery.<br>As multiple software does not provide the required data on any standard protocol so please modify the clause as suggested | Please refer the revised specifications given below. |
| 15 | Section – | Solution offers | Request you to provide more details | Please refer the |

| | | | | |
|---|---|---|---|---|
| | VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-45 | multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | on the software/application from which EMS application need to integrate | revised specifications given below. |
| 16 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-45 | The solution should be able to track connectivity between network endpoints and display the delay between nodes | As per our understanding here need to monitor the latency of all the nodes from application server, please clarify | Please refer the revised specifications given below. |
| 17 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated | The required features is not the standard ask of NMS solution and can be achieved via ITSM solution, so please confirm here whether new ITSM need to propose here or NMS will be integrated with existing running ITSM solution.<br>If Existing please provide OEM and version details of the ITSM solution. | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Page No.- 48 | assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event |  |  |
| 18 | Section – VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.- 44 | It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any<br>node of the application. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | Please refer the revised specifications given below. |
| 19 |  | Additional | Request you to please provide the required details of the IT Infrastructure which will be monitored in NMS solution<br>1) No. Of servers:<br>i) Physical Server ii) VMs<br>iii) Physical server on which virtualization platform running.<br>2) No. & Make Of Network devices<br>i) Router /Switches Firewall<br>ii) Wireless Controller /Wifi AP<br>iii) Storage<br>3) No. & Name Of Applications | Please visit High Court of M.P. for information. |

| | | | | |
|---|---|---|---|---|
| | | | 4) No. Of containers.<br>Or any other IP devices | |
| 20 | Section-II Point No. 2.15.2(ii) Page No. 10 & 11 | Experience in Supply, Installation, commissioning, Maintenance of firewall, WAF, NMS tool and similar IT equipments during last 05 years ending last day of month previous to the month of publication of this tender, should be either of the following:-<br>(a) Three similar completed work costing not less than the amount equal to 40% of the estimated cost.<br>OR<br>(b) Two similar completed work costing not less than the amount equal to 50% of the estimated cost.<br>OR<br>(c) One similar completed work costing not less than the amount equal to 80% of the estimated cost.<br>Similar works means: Supply, installation and System Integration of firewall, WAF, NMS tool and | We understand that bidder need to show similar experience of supply, installation and system integration of Firewall, WAF & NMS tool and similar IT equipments through one, two and three PO as per given option. We also understand that experience of all stated category can be shown in multiple order as well as per given option.<br>Please confirm. | Yes, but to have experience as per the tender document.<br>In this regard the decision of the High Court shall be final. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | similar IT equipments. |  |  |
| 21 | Section - VII 7.Technical Specifications / Specifications - B/ Web Application Firewall with Server Load Balancer / Point No.7 Page No. 39 | Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | Virtual Matrix Architecture feature is specific to one ADC OEM. Kindly remove this clause for wider participation and please allow similar or equivalent feature metrics for broader participation. Following Load Balancing Topologies should be supported:<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | Please refer the revised specifications given below. |
| 22 | Section - VII 7.Technical Specifications / Specifications -B / Web Application Firewall with Server Load Balancer / Point No.31 Page No. 42 | The proposed appliance/software should be EAL2 certified. | We are currently in the process of obtaining our EAL 2 certification. In order to facilitate wider participation kindly allow us so that during the bidding time we can submit the undertaking for the same. It is suggested to amend the clause as" The proposed appliance/software should be EAL2 certified or EAL 2 Applied" | Please refer the revised specifications given below. |
| 23 | Section - VII 7.Technical Specifications / Specifications - B/ Web Application Firewall with Server Load | Application load balance with functionality of Application delivery features ,<br>Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing | IPS is completely different technology even deployment is different. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | Balancer / Point No.44 Page No. 43 | Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP | Bot protection, logs, High Availability and reporting from day 1.<br>OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF /ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P" | |

| | | | | |
|---|---|---|---|---|
| | | E590H through) will be provided by High Court of M.P. | | |
| **23. M/s Tekno Solutions Pvt. Ltd.** | | | | |
| **“SPECIFICATIONS –A” Firewall Technical Specifications** | | | | |
| 1 | Section – VII, Clause No- 7. Technical Specifications s, Page No. - 32, Point No. - 5 | Performance & Scalability:<br>The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | Considering the current requirement and future scalability for MP High Court, it is recommended to increase the throughput of NGFW ad Threat Prevention. It would also take care of the periodical spike in the traffic and higher throughput requirement for the contract period as well. Request MP High Court to modify / amend the clause as below:<br>The NGFW throughput of the firewall should be a minimum 28 Gbps with 64 KB including application identification and firewalling enabled with real world/enterprise/ production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, antispyware, sandboxing, user identification, file blocking, DNS security and logging enabled should be 15 Gbps considering 64 KB HTTP transaction size. | Please refer the revised specifications given below. |
| | | Performance & Scalability:<br>NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions | For better throughput and performance and to be inline with the throughput, please ammed the clause as below:<br>NGFW Firewall should support at least 2.5 Million Layer 7 Concurrent sessions measured utilizing HTTP transactions or 20 Million Layer 3 / 4 concurrent sessions. | Please refer the revised specifications given below. |
| | | Performance & Scalability:<br>NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 connections per second – Min 90,000 | For better throughput and performance and to be inline with the throughput, we recommend amending the clause as below:<br>NGFW Firewall should support at least 2 Million connections per second L3/L4 or New Layer 7 connections per second – Min 225K measured with application override, utilizing 1 byte HTTP transactions. | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
| 2 | Section – VII, Clause No- 7. Technical Specifications s, Page No. - 36, Point No. - 10 | Support:<br>OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The NGFW should be proposed with 5 years onsite support and subscription license for NGFW, NGIPS, Anti Virus, Anti Spyware, URL Filtering, DNS, VPN and Anti botnet | For a better visibility of the various licenses to be proposed / quoted, please ammend the clause as below:<br><br>OEM should be present in India from at least 5 years and should be 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, Threat Protection, APT Protection (Zero Day Protection with integrated Sandboxing), URL Filtering and DNS Security from day 1. The solution shall support bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns for future use. | Please refer the revised specifications given below. |
| 3 | Section – VII, Clause No- 7. Technical Specifications s, Page No. - 37, Point No. - 14 | Automation & Incident Response:<br>The Proposed system shall support automation response based on following events:<br>Compromised Hosts detected<br>Configuration Change<br>Event Log<br>High CPU<br>License Expiry<br>Email Alert<br>IP Ban | These are the features generally part of the Security Automation tool such as SOAR and the Firewall management could provide an insight for the below events and alert the analysts. Please remove the section or modify as below:<br>Monitor and send email alerts for below events:<br>System<br>Threats<br>Zero day / unknown malware<br>traffic logs | Please refer the revised specifications given below. |
| 4 | Section – VII, Clause No- 7. Technical Specificatio | Device Storage: Minimum 800GB SSD | Since these are hardware appliances, it comes with a fixed storage size, different vendor models would have different size of storage based on the models. Also since the RFP is also | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | ns s, Page No. - 38, Point No. - 15 | | asking for Management server which would have more storage space to store the logs and configs a regular storage size SSD is adequete on the firewall, it is recommended to change the clause as below:<br>Minimum 400 GB SSD. | |
| **“SPECIFICATIONS –B” Web Application Firewall with Server Load Balancer** | | | | |
| 1 | Section – VII, Clause No- 7. Technical Specifications s, Page No. - 39, Point No. - 2 | Traffic Ports support: 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.<br>Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps<br>Layer 7 requests per second: 1300,000<br>Layer 4 connection per second: 500,000<br>Concurrent Connection: 38 Million<br>RSA CPS (2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. | Traffic Ports support: As per the present data centre / It infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for ADC/WAF/SLB deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amending this clause.<br>Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. Please amend this clause.<br>Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. Please amend this clause.<br>It is suggested to amend the clause as: -<br>Traffic Ports support: 8 x 10 GE SFP+ from day-1<br>Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps<br>Layer 7 requests per second: 5 million<br>Layer 4 connections per second: 3 Million<br>RSA CPS(2K Key): 20,000<br>ECC CPS (EC-P256): 12,000 with TLS1.3 Support<br>Processor: Intel 12-core CPU or equivalent or better<br>Concurrent Connections: 40 Million<br>Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | | |
| 2 | Section – VII, Clause No- 7. Technical Specifications s, Page No. - 39, Point No. - 6 | The proposed ap pliance should s upport the below metrics:<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc. | Different OEM has different terminology and technique to achieve similar function. We would like to request the honorable tendering committee to use vendor agnostic terminology for wider participation.<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash/Equivalent<br>— Weighted Hash/Equivalent<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | Please refer the revised specifications given below. |
| 3 | Section – VII, Clause No- 7. Technical Specifications s, Page No. - 39, Point No. - 7 | Following Load Balancing Topologies should be supported:<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP | Virtual Matrix Architecture feature is specific to one ADC OEM. Kindly remove this clause for wider participation and for other points please allow similar or equivalent feature metrics for broader participation<br>Following Load Balancing Topologies should be supported:<br>• Client Network Address Translation (Proxy IP) /Equivalent<br>• Mapping Ports /Equivalent<br>• Direct Server Return /Equivalent<br>• One Arm Topology Application /Equivalent<br>• Direct Access Mode /Equivalent<br>• Assigning Multiple IP Addresses /Equivalent<br>• Immediate and Delayed Binding /Equivalent | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | Addresses<br>• Immediate and Delayed Binding | | |
| 4 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 42, Point No. - 31 | The proposed appliance/software should be EAL2 certified. | For wider participation, We would like to request the honorable tendering committee to amend the clause as requested.<br>"The proposed appliance/software should be EAL2 certified/Make in India" | Please refer the revised specifications given below. |
| 5 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 42, Point No. - 34 | Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | In order to switch over the applications traffic like web app, email app etc. the GSLB solution must understand all types of DNS records and not just A or AAAA. Kindly add following functionality for complete Solution. It is suggested to amend this clause as :-<br>The Proposed Solution must have Global Server Load Balancing and should be able to host SRV Records, AAAA Records, A, PTR, MX, TXT, SOA, NS, Dname, Dmarc Records and should also support DNSSEC. | Please refer the revised specifications given below. |
| 6 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 43, Point No. - 44 / a | Support: Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed | IPS is completely different technology even deployment is different. Kindly remove the IPS feature in the specifications s for the wider participations of OEM. It is suggested to amend the clause as "Application load balance with functionality of Application delivery features, Antivirus, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, DLP, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | solution should support 24 x 7 x 365 OEM TAC support and advance Next Business Day Hardware replacement.<br>The proposed equipments must come with 5 year warranty and onsite support.<br>Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8 months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through will be provided by High Court of M.P. | Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P" | |
| **"Specifications – C" Network Monitoring System** | | | | |
| 1 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 44, Point No. - 2 | The solution should automatically group servers that work closely together based on analysis of communication between them | Request you to modify the OEM specific clause as:<br>The solution should automatically /Manually group servers that work closely together based on analysis of communication between them | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| 2 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 44, Point No. - 4 | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | Please refer the revised specifications given below. |
| 3 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 44, Point No. - 8 | The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. .Lastly, it should integrate with a | Request you to modify the specific clause as:<br>The solution should be able to automatically/manually detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery.<br>As multiple software does not provide the required data on any standard protocol so please modify the clause as suggested. | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. |  |  |
| 4 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 44, Point No. - 12 | It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any node of the application. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate. | No change |
| 5 | Section – VII, Clause No- 7. Technical Specificatio ns s, Page No. - 48, Point No. - 74 | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling | The required features is not the standard ask of NMS solution and can be achieved via ITSM solution, so please confirm here whether new ITSM need to propose here or NMS will be integrated with existing running ITSM solution.<br>If Existing please provide OEM and version details of the ITSM solution. | Removed. |

| | | | | |
|---|---|---|---|---|
| | | duplicate events, provide event correlation capabilities to combine a set of different events into one major event | | |
| 6 | | Additional | Request you to please provide the required details of the IT Infrastructure which will be monitored in NMS solution<br>1) No. Of servers:<br>i) Physical Server<br>ii) VMs<br>iii) Physical server on which virtualization platform running.<br>2) No. & Make Of Network devices<br>i) Router/Switches/Firewall<br>ii) Wireless Controller/Wi-Fi AP<br>iii) Storage<br>3) No. & Name Of Applications<br>4) No. Of containers.<br>Or any other IP devices | The bidder is requested to visit the High Court of M.P., Jabalpur for getting the real time detail of same before the submission of bid document. |
| **24. M/s Path Infotech** | | | | |
| 1 | “Specifications – C” Network Monitoring System/ Servers & System Monitoring/ 35/Pg No.45 | The solution should allow monitoring of Server Status and Availability, CPU Utilization, Memory Utilization, Process Monitoring, File System Monitoring, Disk Utilization of RHEL/Centos, SUSE, Ubuntu servers/Windows 2008, 2012,2016,2019, 2022. | Please consider remove "2008.2012", Only OEM supported O.S can be supported | Please refer the revised specifications given below. |
| 2 | “Specifications – C” Network Monitoring System/ Servers & System | Solution offers multiple integration methods which can be used by customers for integrating their | Please consider removing "XML, SOAP & Trap" as RestAPI based integration is the industry best practice and modify the point to "Solution offers multiple integration methods which can be used by customers for integrating their own | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Monitoring/ 17/Pg No.45 | own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed." |  |
| 3 | “Specifications – C” Network Monitoring System/ Servers & System Monitoring/ 40/Pg No.46 | The solution should be able to gather capacity data from vCenter, HMC, Physical servers, etc. Generate report and provide recommendation | Please elaborate what kind of recommendations is expected from the solution? | Please refer the revised specifications given below. |
| 4 | “Specifications – C” Network Monitoring System/ Servers & System Monitoring/ Pg No.43 | The proposed solution should be able to monitor the availability, health and performance of physical servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, end point devices like desktop, Kiosks, display | Please consider removing end point devices like desktop to "The proposed solution should be able to monitor the availability, health and performance of physical servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, Kiosks, display boards, URL monitoring, other snmp/ping enabled devices like UPS and AC from single dash board." | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | boards, URL monitoring, other snmp enabled devices like UPS and AC from single dash board. | | |
| 5 | “Specifications – C” Network Monitoring System/ Storage Monitoring Monitoring/ 40/Pg No.46 | The solution should show storage growth rates and project when the storage capacity will be reached | Please consider removing this point | Removed. |
| 6 | Specifications – C” Network Monitoring System/ Logging/Reporting/Alert /threshold /65/Pg No.47 | Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement | Different OEM's have different level of severity definitions. | Please refer the revised specifications given below. |
| 7 | “Specifications – C” Network Monitoring System/ Other Features/72 /Pg No.48 | Capacity Reservations: tool should allow management of resource allocations and reservations (for services, applications or other needs), identify resource shortages and provide information for further analysis or procurement | Please consider removing this specifications . | Optional. |
| 8 | “Specifications – C” Network Monitoring System/ Licensing/8 | The licenses should be perpetual with 05 years support /updates /upgrade. | Please consider modifying to "The licenses should be On Prem Subscription with 05 years support /updates /upgrade." | Please refer the revised specifications given below. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 0/Pg No.49 |  |  |  |
| 9 | “Specifications – C” Network Monitoring System/ Note/4/Pg No.49 | The bidder has to quote only 01 product of single make / brand at a time and not multiple brands for same item. | Please consider removing this specifications as EMS based OEM's do not provide solutions for Web Application Firewall with Server Load Balancer. | Yes accepted. |
| 10 | “Specifications – C” Network Monitoring System/ Discovery/15/Pg No.44 | Provides provision to draw & map user specific network diagram | Please consider modifying the specifications to "The tool should enable business users or administrators to efficiently design and modify the service model(network diagram) using templates | Please refer the revised specifications given below. |
| **25. M/s Trend Micro** |  |  |  |  |
| 1 | Section 7 / Clause 7 / Page 31 | RFP has asked for Firewall, Web application Firewall and NMS | RFP has asked for NGFW (Next Generation Firewall) which is a combination of Firewall, NIPS, Anti-APT i.e. all is fitting in a single box. We propose to have dedicated Network Intrusion Prevention System along with Next Generation Firewall to avoid single point of failure - Whenever throughput increases, by default the box capacity will decrease as it is working with all the modules of FW, NIPS & Anti-APT or in worst case NGFW will bypass the NIPS & Anti-APT & will offer basic Firewall functionality only. These problems of NGFWs are publically available on web.<br>We request to consider our recommendation for dedicated purpose built NIPS appliance. | Quote as per tender. |
| 2 | Section 7 / Clause 7 / Page 31 | RFP has asked for Firewall, Web application Firewall and NMS | Even in recent Supreme court RFP of Data Center for ICT enablement: GEM/2024/B/4564249; Next Generation IPS is there which mentions that NIPS should be a Dedicated appliance (NOT a part of Router, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Appliance).<br>We request to consider our recommendation for dedicated purpose built NIPS appliance. | Quote as per tender. |
| 3 | Section 7 / Clause 7 / Page 31 | RFP has asked for Firewall, Web application | Moreover, we propose to have dedicated Network Intrusion Prevention System along with Next | Quote as per tender. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | Firewall and NMS | Generation Firewall to avoid single point of failure.<br>NGFW is a single box with same underlying OS; if it is compromised my perimeter security is broken. So dedicated NIPS is required |  |
| 4 | Section 7 / Clause 7 / Page 31 | RFP has asked for Firewall, Web application Firewall and NMS | NGFW has very less threat signature compared with NIPS. We request to consider our recommendation for dedicated purpose built NIPS appliance. | Quote as per tender. |
| 5 | Section 7 / Clause 7 / Page 31 | RFP has asked for Firewall, Web application Firewall and NMS | Lot of times Firewall is bypassed (sometimes it goes in auto bypass mode) to let the traffic through and then there is no protection at North South Interface.<br>We request to consider our recommendation for dedicated purpose built NIPS appliance. | Quote as per tender. |
| **26. M/s A10 Networks Inc** |  |  |  |  |
| **3.30 Link Load Balancer-HW solution** |  |  |  |  |
| 1 | The LLB must be deployed in Active-Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA. Proposed solution shall be horizontally/ vertically scalable in future via software and/or hardware with minimum scalability | Due to license capping the OEMs will take advantage to quote higher for the incremental license which is not cost effective to customer. Hence request you to amend the point as "The LLB must be deployed in Active-Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA. Proposed solution shall be horizontally/vertically scalable in future via software and/or hardware with | The LLB must be deployed in Active-Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA. Proposed solution shall be horizontally/vertically scalable in future via software and/or hardware with minimum scalability support of 80Gbps L4 throughput considering the redundancy of one load balancer unit. The LLB shall be dual stack (IPv4 & IPv6) ready and HA should be supported on both IPV4 and IPV6. | No change. |

| | | | | |
|---|---|---|---|---|
| | support of 80Gbps L4 throughput considering the redundancy of one load balancer unit. The LLB shall be dual stack (IPv4 & IPv6) ready and HA should be supported on both IPV4 and IPV6. | minimum scalability support of 80Gbps L4 throughput considering the redundancy of one load balancer unit from Day-1. The LLB shall be dual stack (IPv4 & IPv6) ready and HA should be supported on both IPV4 and IPV6. " | | |
| 2 | The LLB should have a minimum L4 throughput of 40 Gbps. | Request you to remove this point as this is contradicting with point no. 3. | The LLB should have a minimum L4 throughput of 40 Gbps. | Quote as per tender and clarification published. |
| **3** | The proposed solution should have minimum 1.2 million L4 TCP connections / second and 2.4 Million HTTP requests / second | Due to connection reuse the Layer 4 CPS numbers are high compared to Layer4 CPS numbers which are 1/10th of the L4 TPS numbers. Hence request you to amend the clause as "The proposed solution should have minimum 120K L4 TCP connections / second". | The proposed solution should have minimum 1.2 million L4 TCP connections / second and 2.4 Million HTTP requests / second | No change. |
| **3.31 Link Load Balancer for DR** | | | | |
| 4 | The LLB must be deployed in Active- | Due to license capping the OEMs will take advantage to | The LLB must be deployed in Active-Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA. | Quote as per tender. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA. Proposed solution shall be horizontally/vertically scalable in future via software and/or hardware with minimum scalability support of 40Gbps L4 throughput considering the redundancy of one load balancer unit. The LLB shall be dual stack (IPv4 & IPv6) ready, and HA should be supported on both IPV4 and IPV6. | quote higher for the incremental license which is not cost effective to customer. Hence request you to amend the point as "The LLB must be deployed in Active-Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA. Proposed solution shall be horizontally/vertically scalable in future via software and/or hardware with minimum scalability support of 40Gbps L4 throughput considering the redundancy of one load balancer unit from Day-1. The LLB shall be dual stack (IPv4 & IPv6) ready and HA should be supported on both IPV4 and IPV6. " | Proposed solution shall be horizontally/vertically scalable in future via software and/or hardware with minimum scalability support of 40Gbps L4 throughput considering the redundancy of one load balancer unit. The LLB shall be dual stack (IPv4 & IPv6) ready, and HA should be supported on both IPV4 and IPV6. |  |
| **3.32 Hardware Server Load Balancer** |  |  |  |  |
| 5 | The solution (along with its tenant/virtual instance) | As per pt no.3 the appliance Layer 7 throughput asked is of 10 | The solution (along with its tenant/virtual instance) must be deployed in Active-Standby mode of HA from day one and proposed solution shall also | Quote as per tender. |

| | | | | |
|---|---|---|---|---|
| | must be deployed in Active-Standby mode of HA from day one and proposed solution shall also support Active-Active mode of HA and should provide seamless takeover in-case if one device fails. Proposed solution shall be horizontal scalable in future via software and/or hardware with minimum scalability support of 40 Gbps SSL throughput considering the redundancy of one load balancer unit. The SLB shall be dual stack (IPv4 & IPv6) ready, and HA should be supported on both | Gbps whereas point no. 17 states SSL throughput of 40Gbps. SSL adds overhead due to SSL/TLS encryption of around 30-50%. At the beast for a 10 Gbps appliance we can consider 6 Gbps of SSL throughput.<br>Request you to reconsider the SSL throughput which is inline to the Layer 7 throughput asked. | support Active - Active mode of HA and should provide seamless takeover in-case if one device fails. Proposed solution shall be horizontal scalable in future via software and/or hardware<br>with minimum scalability support of 40 Gbps SSL throughput considering the<br>redundancy of one load balancer unit. The SLB shall be dual stack (IPv4 & IPv6) ready, and HA should be supported on both IPV4 and IPV6. | |

| | | | | |
|---|---|---|---|---|
| | IPV4 and IPV6. | | | |
| 6 | The proposed WAF solution should be ICSA and PCI compliant. | Request you to amend the clause as The proposed WAF solution should be ICSA/ISO /IEC 27001:2013/SOC 2 Type 2 and PCI compliant for wider participation from the WAF OEM`s. | The proposed WAF solution should be ICSA and PCI compliant. | Please refer the revised specifications given below. |
| **Web Application Firewall with Server Load Balancer** | | | | |
| 7 | Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps | | Due to license capping the OEMs have the advantage to quote higher for the incremental license which is not cost effective to customer. Hence request you to amend the point as "The ADC+WAF should be fully populated with the license throughput of 40 Gbps from Day-1." | Quote as per tender. |
| 8 | Processor: Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply. | | To derive the performance number from the specific compute numbers does not decide performance of the device at all due to Different architecture, ASICS, FTGA cards etc have different hardware requirement which cannot be generalized for performance. Request you to change the required Processor to Intel Xeon 8-core or higher. | Quote as per tender. |
| **27. M/s gstbhopalb** | | | | |
| 1 | Section–VII Clause No - 7. Technical Specifications s Specifications – C” Network Monitoring System Page No.- 44, Point no. 2 | The solution should automatically group servers that work closely together based on analysis of communication between them | Request you to modify the OEM specific clause as:<br>"The solution should automatically /Manually group servers that work closely together based on analysis of communication between them." | Please refer the revised specifications given below. |
| 2 | Section– VII Clause No- | The solution should | The required features is not the standard ask of EMS module and to | Please refer the revised |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-44, Point no. 4 | automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | specifications given below. |
| 3 | Section– VII Clause No-7. Technical Specifications s Specifications – C” Network Monitoring System Page No.-44, Point no. 8 | The solution should be able to automatically detect software’s that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management | Request you to modify the specific clause as:<br>"The solution should be able to automatically /manually detect software’s that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery."<br>As multiple software does not provide the required data on any standard protocol so please modify the clause as suggested | Please refer the revised specifications given below. |

| | | | | |
|---|---|---|---|---|
| | | solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. | | |
| 4 | Section– VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-45, Point no. 17 | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | Request you to provide more details on the software/application from which EMS application need to integrate | Please refer the revised specifications given below. |
| 5 | Section– VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-45, Point no. 29 | The solution should be able to track connectivity between network endpoints and display the delay between nodes | As per our understanding here need to monitor the latency of all the nodes from application server, please clarify | Quote as per tender. |
| 6 | Section– VII | Configurations: | The required features is not the | Removed. |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-48, Point no. 74 | create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | standard ask of NMS solution and can be achieved via ITSM solution, so please confirm here whether new ITSM need to propose here or NMS will be integrated with existing running ITSM solution.<br>If Existing please provide OEM and version details of the ITSM solution. |  |
| 7 | Section– VII Clause No-7. Technical Specifications s Specifications – C" Network Monitoring System Page No.-44, Point no. 12 | It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any node of the application. | The required features is not the standard ask of EMS module and to achieve this solution dedicated APM tool will be required so we request you to remove this clause for wider participate | No change. |
| 8 |  | Additional | Request you to please provide the required details of the IT Infrastructure which will be monitored in NMS solution | The bidder is requested to visit the High Court of M.P., Jabalpur for |

| | | | | |
|---|---|---|---|---|
| | | | 1) No. Of servers:<br>i) Physical Server<br>ii) VMs<br>iii) Physical server on which virtualization platform running.<br>2) No. & Make Of Network devices<br>i) Router/Switches/Firewall<br>ii) Wireless Controller /Wi-Fi AP<br>iii) Storage<br>3) No. & Name Of Applications<br>4) No. Of containers.<br>Or any other IP devices | getting the real time detail of same before the submission of bid document. |

## “Specifications – A”
## Firewall Technical Specifications

| S. No. | Feature | Technical Specifications | Revised Specifications after clarification /query | Compliance Yes / No with Remarks (if any) |
|---|---|---|---|---|
| 1 | Type | Next Generation Enterprise Firewall | | |
| 2 | 3rd party Test Certification | The proposed firewall vendor must have over 97% of Exploit Block rate in latest NGFW NSS Lab Test report. | Removed | |
| | | The proposed vendor must be in the Leader’s or challenger quadrant of the Network Firewalls Gartner Magic Quadrant for latest year report. | The proposed vendor must be in the Leader’s or challenger quadrant of the Network Firewalls Gartner Magic Quadrant for latest year report OR Top 5 OEMs in Network Firewalls (NGFW) according to the latest report from IDC (International Data Corporation). | |
| 3 | Interface and Connectivity Requirement | 6 X 10G Copper/RJ45 Day 1 | Minimum 6x1G copper or fiber from day1. (In case of fiber, the vendor have to provide the appropriate no. of transceivers and patch cords) | |
| | | 8 X 1/10G SFP/SFP+ Day 1 with LR/SM transceivers and 8x3m patch cords. | Minimum 4 X 1/10G SFP/SFP+ Day 1 with LR/SM transceivers and 8x3m patch cords. | |
| | | 4X 10/25Gig SFP28 Ports with 4 nos. of LR transceivers and 4x3m patch cords from Day one | Minimum 2X 10/25Gig SFP28 Ports or Minimum 2x 40/100G QSFP28 ports with appropriate nos. of LR/SM transceivers and 4x3m patch cords from Day one | |

| | | | | |
|---|---|---|---|---|
| | | Minimum 2 x 10G HA port in addition to requested data ports, Dedicated 1 X 10/100/1000 RJ45 Management Port | Minimum 1 x 1G HA port in addition to requested data ports or higher, Dedicated 1 X 10/100/1000 RJ45 Management Port | |
| | | Should have support 2x40/100G for future use. | Removed | |
| 4 | Hardware Architecture | The appliance based security platform should provide Next-Gen Firewall functionality like IPS, Application Control, URL and content filtering and Anti-malware functionality in a single appliance from day one. | No Change | |
| | | The appliance hardware should be a multicore CPU architecture and should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one. | The appliance hardware should be a multicore CPU architecture or should be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect &scale against dynamic latest security threats. The appliance hardware should have a hardened operating system from the OEM and should support minimum of 64GB of RAM to make sure all the security capabilities are provided without degradation from day one or should be proprietary ASIC based in nature to make sure all the security capabilities are provided without degradation from day one. | |
| | | The firewall should have integrated redundant fan and dual redundant hot swappable power supply to remove any single point of failure in the solution | The firewall should have integrated redundant fan and dual redundant power supply to remove any single point of failure in the solution | |
| 5 | Performance & Scalability | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise/ | The NGFW throughput of the firewall should be a minimum 20 Gbps with application identification and firewalling enabled with real world/enterprise mix/ | |

| | | | | |
|---|---|---|---|---|
| | | production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 12 Gbps. | production traffic with logging enabled. The Threat Prevention/NGIPS throughput after enabling IPS, AVC, antimalware, sandboxing with logging enabled should be 10 Gbps. | |
| | | The firewall should provide 12 Gbps of IPSEC VPN throughput | No Change. | |
| | | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions | NGFW Firewall should support at least 1400,000 Layer 7 Concurrent sessions/connections. | |
| | | NGFW Firewall should support at least 150,000 connections per second L3/L4 or New Layer 7 connections per second – Min 90,000 | No Change. | |
| | | High Availability: Active/Active and Active/Passive and should support session state synchronization among firewalls from day 1. | No Change. | |
| 6 | Next Gen Firewall Features | Firewall should support creating security policies with source/destination zones, network subnets/ranges, relocation objects, ports/protocols, applications, user/group attributes, URL/URL categories and action on traffic. The actions on the traffic should be to allow, alert, block, block and continue, reset. The firewall should provide time based polices with options for reccurrecing schedule or one time schedule. | Firewall should support creating security policies with source/destination zones, network subnets/ranges, relocation objects or geo location objects, ports/protocols, applications, user/group attributes, URL/URL categories and action on traffic. The actions on the traffic should be to allow, alert, block, block and continue, reset or the actions on the traffic should be to accept, drop, ask, inform, reject, user auth, client auth etc. The firewall should provide time based polices with options for reccurrecing schedule or one time schedule. | |
| | | The firewall should supports NAT's like source NAT, destination NAT, U-Turn NAT. Firewall should support | The firewall should supports NAT's like source NAT, destination NAT, U-Turn NAT or hairpin or loopback or better option. Firewall should support | |

| | | | | |
|---|---|---|---|---|
| | | Nat66, Nat 64 or Nat46 functionality | Nat66, Nat 64 or Nat46 functionality | |
| | | Solution should provides capabilities like dynamic real-time metrics based, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls. | No Change | |
| | | The solution should provide the following routing capabilities: OSPF, EIGRP, BGP, RIP, Multicast, Static, | No Change | |
| | | Route Tracking(SLA) PBR, ISIS, BFD, ECMP, VRF, Application based Routing | No Change | |
| | | Should support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance | Should support capability to create multiple virtual context/instance. | |
| | | The solution should be able to provide contextual information about the hosts and the network subnets present such that the admins are able to capture all the required information and build the security profiles based on the details shown on the solution. The details captured should consist of the following: IOC's , MAC addresses, IP address, Applications, Ports &protocols, vulnerabilities etc. | The solution should be able to provide contextual information about the hosts and the network subnets present such that the admins are able to capture all the required information and build the security profiles based on the details shown on the solution. The details captured should consist of the following: IOC's , IP address, Applications, Ports &protocols, vulnerabilities etc. | |
| | | Should support capability to integrate with other security solutions to receive contextual | No Change | |

| | | | | |
|---|---|---|---|---|
| | | information like security group tags/names. | | |
| | | Should support more than 4000+ (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency | No Change | |
| | | Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. | No Change | |
| | | Should support more than 19,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's. | Should support more than 15,000 (excluding custom signatures) IPS signatures or more. Solution should be able to passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence. The signatures should also have categorization based on MITRE TTP's. | |
| | | The firewall solution should have the following capabilities to make sure the current solution is future ready for technologies like WAN routing, SASE etc. The firewall should have application aware routing with HTTP and ICMP ping, ZTNA based clientless access to applications from day1. | No Change | |
| | | The firewall solution should have capabilities like Application Aware | No Change | |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  | Routing, Health Monitoring, DIA, Dual ISP, Data interface Management for simplified branch capabilities |  |  |
|  |  | Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports. | No Change |  |
|  |  | The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box. The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic. | No Change |  |
|  |  | The solution should have ML/AI capability to detect client apps and process. Moreover it should be able identify malicious encrypted traffic even when it is destined for a trustworthy service. This is required to help administrators control specific applications and improve network security | No Change |  |
|  |  | The solution should provide traffic hit count, Rule Conflict Detection (Redundant &Shadowed) and policy warning for streamlining firewall policies. | The solution should provide traffic hit count. Rule Conflict Detection (Redundant &Shadowed) and policy warning for streamlining firewall policies is optional. |  |
|  |  | The solution should provide Change Management capability for the organizations needs to implement more formal processes for configuration changes, | Removed. |  |

| | | | | |
|---|---|---|---|---|
| | | including audit tracking and official approval before changes are deployed. | | |
| | | Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control. | No Change | |
| | | The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor. Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist. The solution should have the capability to detect MD5, SHA256 and SHA512 traffic hashes to detect any malicious traffic pattern | No Change | |
| | | The solution should provide Configuration Deployment History, Pending Changes and Policy Compare capability before the security policies are deployed on the firewall. It should also provide configuration rollback capacity to the last good configuration running on the firewall. | The solution should provide Configuration Deployment History, Pending Changes and Policy Compare /**test** capability before the security policies are deployed on the firewall. It should also provide configuration rollback capacity to the last good configuration running on the firewall. | |
| | | The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection. | No Change | |

| | | | | |
|---|---|---|---|---|
| | | The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.). | No Change | |
| | | Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location | No Change | |
| | | The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. | No Change | |
| | | Should be IPv6 Logo or USGv6 certified | No Change | |
| 7 | URL Filtering Features | Should support Open based Application ID / Custom Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly | No Change | |
| | | Should must support URL threat intelligence feeds to protect against threats | No Change | |
| | | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 250 million of URLs in more than 75+ categories from day1. | Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies. | |
| 8 | Anti-APT / Malware Features | Should support the capability of providing network-based detection | Should support the capability of providing network-based detection of malware by | |

| | | | | |
|---|---|---|---|---|
| | | of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis. | checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis. | |
| | | Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP | No Change | |
| 9 | Management | Proposed solution shall have required subscription like Threat Intelligence for proper functioning | No Change | |
| | | The management platform must be accessible via a web-based interface and ideally with no need for additional client software and must provide centralized logging and reporting functionality | No Change | |
| | | The management platform must be a dedicated OEM appliance or VM (bidder to consider Required computing / hardware resource) running on server. | No Change | |
| | | The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows | No Change | |
| | | The management platform must be capable of role-based administration, enabling different sets of | No Change | |

| | | | | |
|---|---|---|---|---|
| | | views and configuration capabilities for different administrators subsequent to their authentication. | | |
| | | Should support troubleshooting techniques like Packet tracer and capture | No Change | |
| | | The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. The management platform support running on-demand and scheduled reports | No Change | |
| | | The management platform must support multiple mechanisms for issuing alerts (e.g.,SNMP,e-mail, SYSLOG). | No Change | |
| | | The centralized management platform must not have any limit in terms of handling logs per day | No Change | |
| | | The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. | No Change | |
| | | The management platform must risk reports like advanced malware, attacks and network | No Change | |
| 10 | Support | The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as | No Change | |

| | | | | |
|---|---|---|---|---|
| | | Security Information and Event Managers (SIEMs), and log management tools. | | |
| | | OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The NGFW should be proposed with 5 years onsite support and subscription licenses for NGFW, NGIPS, Anti Virus, Anti Spyware, URL Filtering, DNS, VPN and Anti Botnet. | No Change | |
| 11 | DNS Security | The Solution should support DNS security in line mode and not proxy mode. Necessary licenses to be included from day 1. | The Solution should support DNS security from day1. | |
| | | Solution should maintain a database containing a list of known botnet command and control (C&C) addresses which should be updated dynamically. | No Change. | |
| | | DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control. | DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control. | |
| | | DNS security 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. | DNS security should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence. | |
| | | It should prevent against new malicious domains and enforce consistent protections for millions of emerging domains. | No Change. | |
| | | The solution should integrate and correlate to | The solution should integrate and correlate to provide | |

| | | | | |
|---|---|---|---|---|
| | | provide effective prevention against.<br>New C2 domains, file download source domains, and domains in malicious email links.<br>Integrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators.<br>Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots.<br>Should take inputs from at least 25 third-party sources of threat intelligence. | effective prevention against.<br>New C2 domains, file download source domains, and domains in malicious email links or equivalent or better.<br>Integrate with URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators or equivalent or better.<br>Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honey pots.<br>Should take inputs from at least 25 third-party sources of threat intelligence or equivalent or better. | |
| | | Should have simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries. | No Change. | |
| | | Solution should prevent against DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection | No Change. | |
| | | The solution should have capabilities to neutralize DNS tunneling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers. | The solution should have capabilities to neutralize DNS tunneling. | |
| | | The solution should have 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 | No Change. | |

| | | | | |
|---|---|---|---|---|
| | | Command and control and quickly identify infected users. | | |
| 12 | SD-WAN | Proposed firewall should support for internet links load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss, | | |
| | | Support for WAN Link-Load balancing and Fail-over with 4 Links or more. | No Change. | |
| | | Integrated Traffic Shaping functionality for both inbound and outbound traffic. | Integrated Traffic Shaping functionality for outbound traffic. | |
| | | The proposed firewall should support SD-Wan functionality for application aware traffic control | No Change. | |
| 13 | VPN | The proposed system shall comply/support industry standards, supports without additional external solution, hardware or modules: IPSEC VPN , PPTP VPN, L2TP VPN,SSL VPN | No Change. | |
| | | The system shall support 2 forms of site-to-site VPN configurations: Route based IPSec tunnel ,Policy based IPSec tunnel | No Change. | |
| | | The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN. | No Change. | |
| | | The proposed system shall support TWO modes of SSL VPN operation: | No Change. | |
| | | Web-only mode: for thin remote clients equipped with a web browser only and support web application such as: HTTP/HTTPS, SMB/CIFS, SSH, RDP. | No Change. | |

| | | | | |
|---|---|---|---|---|
| | | Tunnel mode, for remote computers that run a variety of client and server applications | No Change. | |
| | | The proposed solution shall support to a minimum of 2000 concurrent IPSEC-VPN and 1000 concurrent SSL-VPN users from day 1 | No Change. | |
| 14 | Automation & Incident Response | The Proposed system shall support automation response based on following events:<br>Compromised Hosts detected<br>Configuration Change<br>Event Log<br>High CPU<br>License Expiry<br>Email Alert<br>IP Ban | The Proposed system shall support automation response based on following events:<br>Compromised Hosts detected,<br>Configuration Change,<br>Event Log,<br>High CPU,<br>License Expiry,<br>Email Alert,<br>IP Ban, or the proposed system shall monitor and send email alerts for events such as system threats, unknown malware, traffic logs etc. | |
| 15 | Device Storage | Minimum 800GB SSD | Minimum 400GB SSD | |
| 16 | Logs & Reporting | Bidder has to propose on premise dedicated logging, analytics & reporting solution from same OEM (Virtual /Physical Appliance) from day1, the logging solution to be deployed at Data Center only.<br>In Case of Virtual Appliance, bidder to consider Required computing / hardware resource for the VM. The firewall should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P.<br>**Required Features:** | No Change. | |

| | | | | |
|---|---|---|---|---|
| | | Should Deliver single-pane visibility, also have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate Predefined or customized Advance reports in different formats. The solution should have configurable options to schedule the report generation. Log retention customization by category. Solution should offer Centralized NOC/SOC Visibility for the Attack Surface. Bidder has to include any additional license for analytics/event corelation from day1. The solution should machine learning capability to detect the exploit and not depend on the vulnerabilities with trained models and traffic classifiers. The same should be available on public website to validate the capabilities. | | |
| 17 | Installation and Migration | The bidder must migrate the existing configuration and policies from the SonicWall NSA6600 firewall to the new one and provide six days of training on the configuration and management of all key security aspects to the technical team of the High Court of Madhya Pradesh, Jabalpur | No Change. | |

# “Specifications – B”
# Web Application Firewall with Server Load Balancer

| S. No. | Specifications s | Revised after clarification | Compliance (Yes/No) with Remarks (if any) |
|---|---|---|---|
| | **Web Application Firewall with Server Load Balancer** | | |
| 1 | The proposed appliance should be a dedicated ADC/WAF/SLB appliance having DDoS protection, SSL inspection, and real-time threat intelligence. it should not be part of any Firewall or UTM. | No Change. | |
| 2 | **Traffic Ports support:** 4 x 10 GE Fiber, 4 x 1G GE Fiber and 4 x 1G Copper Port from day-1. Additionally should have 8 x 1GE Fiber for future use (Break-Out should not be used). All transceivers (SM) from day1.<br>**Device L4 Throughput**: 20 Gbps and scalable upto 40 Gbps<br>**Layer 7 requests per second:** 1300,000<br>**Layer 4 connection per second:** 500,000<br>**Concurrent Connection:** 38 Million<br>**RSA CPS(2K Key):** 20,000<br>**ECC CPS (EC-P256):** 12,000 with TLS1.3 Support<br>**Processor:** Intel 12-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | **Traffic Ports support:** Minimum **(**4 x 1/10 G Fiber, 6 x 1G Port) or Minimum (8x1/10G) from day-1 or higher or better. All transceivers (SM) from day1.<br>**Device L4 Throughput**: 20 Gbps and scalable upto 40 Gbps<br>**Layer 7 requests per second:** 1300,000<br>**Layer 4 connection per second:** 500,000<br>**Concurrent Connection:** 38 Million<br>**RSA CPS(2K Key):** 20,000<br>**ECC CPS (EC-P256):** 12,000 with TLS1.3 Support<br>**Processor:** Intel 8-core CPU, 64GB RAM, minimum 480GB SSD Disk and dual power supply.<br>The appliance should have 1 x 1G RJ45 Management Port and 1G RJ45 Console port. | |
| 3 | The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2 | No Change. | |
| 4 | The solution must be able to decrypt SSL web traffic between clients and web servers. | No Change. | |
| 5 | Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1 | No Change. | |

| | | | |
|---|---|---|---|
| 6 | **The proposed appliance should support the below metrics:**<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash,<br>— Tunable Hash,<br>— Weighted Hash,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | **The proposed appliance should support the below metrics:**<br>— Minimum Misses,<br>— Hash,<br>— Persistent Hash or equivalent or better,<br>— Tunable Hash or equivalent or better,<br>— Weighted Hash or equivalent or better,<br>— Least Connections,<br>— Least Connections Per Service,<br>— Round-Robin,<br>— Response Time,<br>— Bandwidth, etc | |
| 7 | **Following Load Balancing Topologies should be supported:**<br>• Virtual Matrix Architecture<br>• Client Network Address Translation (Proxy IP)<br>• Mapping Ports<br>• Direct Server Return<br>• One Arm Topology Application<br>• Direct Access Mode<br>• Assigning Multiple IP Addresses<br>• Immediate and Delayed Binding | **Following Load Balancing Topologies should be supported:**<br>• Virtual Matrix Architecture or equivalent or better,<br>• Client Network Address Translation (Proxy IP)or equivalent or better,<br>• Mapping Ports or equivalent or better,<br>• Direct Server Return or equivalent or better,<br>• One Arm Topology or equivalent or better, Application<br>• Direct Access Mode or equivalent or better,<br>• Assigning Multiple IP Addresses or equivalent or better,<br>• Immediate and Delayed Binding or equivalent or better, | |
| 8 | The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high | The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature (NO Multi-Tenancy) **or inbuilt support of virtual domain** that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability | |

|  |  |  |  |
|---|---|---|---|
|  | performance purpose built next generation multi-tenant (min. 5 virtual instances from Day 1 and scalable upto 10 Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality. **Each Virtual Instance contains a complete and separated environment of the Following:**<br>a) Resources, b) Configurations, c) Management, d) Operating System | to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Should be high performance purpose built next generation multi-tenant (min. **2** virtual instances from Day 1 and scalable upto**4** Virtual Instances) hardware. Platform must have multiple functions including Advance application load balancing and global server load balancing, Network security functionality and complete application protection functionality.<br>**Each Virtual Instance contains a complete and separated environment of the Following:**<br>a) Resources, b) Configurations, c) Management, d) Operating System |  |
| 9 | The proposed Hardware must have Bandwidth Management feature from Day 1 | No Change. |  |
| 10 | The solution should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode using standard/ RFC compliant redundancy protocol like VRRP or equivalent, for HA interconnection over network from day 1. | No Change. |  |
| 11 | The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend | No Change. |  |
| 12 | The solution should have support for multiple VLANs with tagging capability | No Change. |  |
| 13 | The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure | No Change. |  |
| 14 | Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications | No Change. |  |

| | | | |
|---|---|---|---|
| 15 | Should have ability to upgrade/downgrade device software Images. | No Change. | |
| 16 | The device should support following health check types:<br>• Link Health Checks • TCP Health Checks • UDP Health Checks • ICMP Health Checks • HTTP/S Health Checks<br>• TCP and UDP-based DNS Health Checks • TFTP Health Check • SNMP Health Check • FTP Server Health Checks<br>• POP3 Server Health Checks • SMTP Server Health Checks • IMAP Server Health Checks • NNTP Server Health Checks<br>• RADIUS Server Health Checks • SSL HELLO Health Checks • WAP Gateway Health Checks • LDAP/LDAPS Health Checks<br>• Windows Terminal Server Health Checks • ARP Health Checks • DHCP Health Checks • RTSP Health Checks<br>• SIP Health Checks • Virtual Wire Health Checks • DSSP Health Checks • Script-Based Health Checks<br>• Cluster-based Health Checks | No Change. | |
| 17 | Device should be accessed through the below:<br>• Using the CLI<br>• Using SNMP<br>• REST API<br>• Using the Web Based Management | No Change. | |
| 18 | The proposed Solution should have ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | The proposed Solution should have ISO /IEC 27001:2013/SOC 2 Type 2 and PCI compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification. | |
| 19 | WAF should have the flexibility to be deployed in the following modes:<br>Reverse proxy<br>Out of Path (OOP) | WAF should have the flexibility to be deployed in the following modes:<br>Reverse proxy | |
| 20 | Solution should dynamically understand the Changes on the Web/Application Server | No Change. | |

| | | | |
|---|---|---|---|
| 21 | The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures). The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats | No Change. | |
| 22 | The WAF should support the following escalation modes:<br>a) Active, b) Bypass, c) Passive | No Change. | |
| 23 | The solution must have a database of signatures that are designed to detect known problems and attacks on web applications | No Change. | |
| 24 | **Hiding Sensitive Content Parameters:**<br>It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details) | No Change. | |
| 25 | **Auto Policy Optimization** | **Auto Policy Optimization** | |
| a | • Known Types of Attack Protection - Rapid Mode | • Known Types of Attack Protection - Rapid Mode or equivalent or better. | |
| b | • Zero Day Attack Blocking - Extended Mode | • Zero Day Attack Blocking - Extended Mode or equivalent or better. | |
| c | • Working in Learn Mode | • Working in Learn Mode | |
| d | • Auto Discovery | • Auto Discovery | |
| 26 | **Following Threats should be protected by the proposed WAF solution:** | No Change. | |
| a | Parameters Tampering | No Change. | |
| b | Cookie Poisoning | No Change. | |
| c | SQL Injection | No Change. | |
| d | Session Hijacking | No Change. | |
| e | Web Services Manipulation | No Change. | |
| f | Stealth Commands | No Change. | |
| g | Debug Options | No Change. | |
| h | Backdoor | No Change. | |
| f | Manipulation of IT Infrastructure Vulnerabilities | No Change. | |
| g | 3rd Party Mis-configuration | No Change. | |

|  |  |  |  |
|---|---|---|---|
| h | Buffer Overflow Attacks | No Change. |  |
| f | Data Encoding | No Change. |  |
| g | Protocol Piggyback | No Change. |  |
| h | Cross-Site Scripting (XSS) | No Change. |  |
| f | Brute Force Attacks | No Change. |  |
| g | OS Command Injection | No Change. |  |
| h | Cross Site Request Forgery (CSRF) | No Change. |  |
| g | Information Leakage | No Change. |  |
| h | Path (directory) Traversal | No Change. |  |
| f | Predefined resource location | No Change. |  |
| g | Malicious file upload | No Change. |  |
| h | Directory Listing | No Change. |  |
| 27 | **The proposed WAF should support the Activity Tracking, which should include the following:** | No Change. |  |
| a | Dynamic IP | No Change. |  |
| b | Anonymity | No Change. |  |
| c | Scraping | No Change. |  |
| 28 | **Device Fingerprint-based tracking** | No Change. |  |
| a | The Proposed WAF should support Device Fingerprint technology or equivalent by involving various tools and methodologies to gather IP agnostic information about the source. | No Change. |  |
| 29 | The proposed solution should have Signature Update, Attacker Feed and Geo Location database from day1. | No Change. |  |
| 30 | Bidder should propose Centralized Management & Reporting Solution from Day 1. | No Change. |  |
| 31 | The proposed appliance/software should be EAL2 certified. | The proposed appliance/software should be EAL2/**NDPP** certified or better. |  |
| 32 | The appliance should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. | No Change. |  |
| 33 | Global load balancing should support advance functions Authoritative name sever, DNS proxy/DNS NAT/ full DNS server with DNSSec/DNS DDOS/ application load balancing from day one with relevant Licenses. | No Change. |  |
| 34 | Capable of handling complete Full DNS bind records including A, AAAA, etc. for IPv4/IPv6 | The Proposed Solution must have Global Server Load Balancing and should be able to host SRV Records, AAAA Records, A , MX ,TXT ,SOA, |  |

| | | | |
|---|---|---|---|
| | | NS, Dmarcetc Records for IPv4/IPv6and should also support DNSSEC or equivalent or better. | |
| 35 | Should have a Web Vulnerability Scanner feature to detect existing vulnerabilities like SQL Injection, Cross Site Scripting, Source code disclosure, OS Commanding in the web applications. | **Should have integration with third party web Vulnerability scanner or** should have a Web Vulnerability Scanner feature to detect existing vulnerabilities like SQL Injection, Cross Site Scripting, Source code disclosure, OS Commanding in the web applications. | |
| 36 | Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks. | No Change. | |
| 37 | Appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers. | No Change. | |
| 38 | The solution should have configurable persistency features to maintain sessions to the load balanced backend servers | No Change. | |
| 39 | The solution should support a connection draining mode in order to allow maintenance of a protected server without disrupting the client experience with the application | No Change. | |
| 40 | Solution must have the API protection and support Json , XML and Open API | No Change. | |
| 41 | Protection for REST APIs filters malicious inputs in requests with JSON payloads. | No Change. | |
| 42 | **Data Analytics , Logs and Reporting** | No Change. | |
| a | Solution must have analytics functionality which includes logical view / tree view of virtual servers and connectivity. | No Change. | |
| b | Solution must have the various charts static and dynamics for analytics | No Change. | |
| c | Solution must have real time monitoring views or dashboards | No Change. | |
| d | Solution should support realty time logging and reporting functionality | No Change. | |
| e | Solution must have support to configure SNMP | No Change. | |
| 43 | **Integration** | No Change. | |
| a | Solution must support integrations like | No Change. | |

| | | | |
|---|---|---|---|
| | SAP , Cloud platform and SIEM tools | | |
| b | Solution must support REST API | No Change. | |
| c | Solution should support virtual servers or profiles, one for internal traffic and one for external traffic. Configure load balancing rules specific to each domain. Internal traffic can be routed to internal servers, and external traffic to public-facing servers. Should have option to set up separate monitoring and logging profiles for internal and external traffic to track performance and security incidents. | No Change. | |
| d | The solution should be scalable enough to support future growth in traffic and applications. | No Change. | |
| 44 | **Support** | | |
| a | Application load balance with functionality of Application delivery features , Antivirus, IP Reputation, IPS, WAF Security, Credential Stuffing Defense, Zero day prevention , DLP , Analytics ,Bot protection ,logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | Application load balance with functionality of Application delivery features, IP Reputation, WAF Security, Credential Stuffing Defense, Zero day prevention, Analytics, Bot protection, logs, High Availability and reporting from day 1. OEM should be present in India from at least 5 years and Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement. The proposed equipments must come with 5 year warranty and onsite support. Installation, basic configuration (at least 2 domains), and six days of training on essential aspects of the WAF/ADC for the IT team of the High Court of M.P., Jabalpur. The WAF/ADC should support to store all log of minimum 8months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | |

|  |  |  |  |
|---|---|---|---|
| 45 | New Clause: | The proposed solution should provide Behavioral DoS (BADoS) capability to protect against threat/attack by analyzing traffic from day 1 or better. |  |
| 46 | New Clause: | Top 10 brands / OEM as per latest IDC reports / Industry Standards. |  |

## “Specifications – C”<br>Network Monitoring System

| **S. No.** | **The proposed solution should be able to monitor the availability, health and performance of physical servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, end point devices like desktop, Kiosks, display boards, URL monitoring, other snmp enabled devices like UPS and AC from single dash board.** | **Revised after clarification. The proposed solution should be able to monitor the availability, health and performance of physical servers, virtual servers, web service (Apache), database service (MySQL & PGSQL), Network devices like routers, switches, Kiosks, display boards, URL monitoring, other snmp enabled devices like UPS and AC from single dash board.** | **Compliance Yes / No with Remarks (if any)** |
|---|---|---|---|
|  | **Discovery** |  |  |
| 1 | The solution should be able to do a complete discovery of IT environment across distributed (i.e., physical, virtual, network, application, middleware, storage, databases) and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services. This should be aided by 5000+ asset type discovery signatures to detect the DC comprehensively. System should have option for multiple options for discovery including IP address based discovery, IP address range discovery, CSV based discovery for bulk discovery. | No Change. |  |
| 2 | The solution should automatically group servers that work closely together based on analysis of communication between them | The solution should automatically/manually group servers that work closely together based on analysis of communication between them or grouping criteria such as tag and types between them. |  |

|  |  |  |  |
|---|---|---|---|
| 3 | Discovery has to work intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details. | No Change. |  |
| 4 | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. It should also have the capability to detect applications that span from Datacenter and end in a public or a private cloud with interconnects between them. | The solution should automatically build visualizations that show dependency between switches, routers, physical/virtual host, Containers, storages, cluster software, business applications and other entities. |  |
| 5 | The discovery data should be fully auditable as to where it came from and what the method to retrieve that data was. | No Change. |  |
| 6 | The solution should show exactly how the discovery data is obtained (i.e., Audit trail and mechanism to validate the quality of data discovered) | No Change. |  |
| 7 | The Discovery solution should come with real-time dashboards that collate and present data that allows organizations to make decision on consolidation, re-use of infrastructure, detecting infrastructure that has never been used etc. | No Change. |  |
| 8 | The solution should be able to automatically detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. | The solution should be able to automatically/manually detect software's that are end of support, end of extended support and end of life. With respect to OS, it should detect End of support and End of life as well. On Security, It should be able to find the patches installed on servers along with reports on vulnerable ports. Lastly, it should integrate with a vulnerability management solution to detect blind spots in security of nodes missed out in vulnerability management that are found to be active in discovery. |  |
| 9 | The discovery solution should have the ability to capture and report on infrastructure drift in datacenter. | No change. |  |

| | | | |
|---|---|---|---|
| 10 | The solution should be able to do Virtual systems discovery (including Microsoft Hyper-V, vmware, etc.) Furthermore, it should support discovery of modern day DevOps platforms such as containers such as Docker, Runc, AIX WPARs and management solutions such as Kubernetes, Docker Swarm, Cloud Foundry and OpenShift. | The solution should be able to do Virtual systems discovery (including Microsoft Hyper-V, vmware, etc.) Furthermore, it should support discovery of modern day DevOps platforms such as containers such as Docker, Runc, AIX WPARs and management solutions such as Kubernetes, Docker Swarm, and Open Shift. | |
| 11 | Discovers in-depth configuration data for storage systems, pools, volumes, disks drives, LUNS, File Systems | Removed. | |
| 12 | It should be possible to initiate complete discovery of an application and connected components from anywhere in the tree. Therefore it should support top down, bottom up and start anywhere discovery from any node of the application. | No Change. | |
| 13 | The report of inventory of discovered devices should be available to export in .csv format. | No Change. | |
| 14 | Automatically learn IP Networks and their segments, LANs, hosts, switches, routers, firewalls etc. and to establish the connections and to correlate | No Change. | |
| 15 | Provides provision to draw & map user specific network diagram | Provides provision to draw & map user specific network diagram OR The tool should enable business users or administrators to efficiently design and modify the service model (network diagram) using templates | |
| 16 | **Integration and Development** | No Change. | |
| 17 | Solution offers multiple integration methods which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML | The solution should offer multiple integration methods for customers to integrate their own systems. Integration should support both northbound and southbound communication using various options, like REST API. | |
| 18 | **Application monitoring** | No Change. | |
| 19 | The solution should automatically provide real-time view of processes running in systems and in-depth application | No Change. | |

| | | | |
|---|---|---|---|
| | performance statistics after discovery/configuration of applications | | |
| 20 | The solution should automatically provide real-time view of windows event logs including the level of the event logs, event ID, and source. | No Change. | |
| 21 | The solution should be able to put together important parameters of an application, into one single monitoring template that can be uniformly applied to applications on different servers, including<br>- Microsoft servers (e.g. Active Directory, Exchange, SharePoint, and Office Communications Server)<br>- Databases (e.g. Microsoft SQL Server, PGSQL, MySQL etc.)<br>- Major application (e.g. ERP, CRM, etc.) | No Change. | |
| 22 | The solution should support monitoring various attributes(at least 50+) in Tomcat, Web Sphere MQ, Apache HTTP, IIS, and WAS | The solution should support monitoring various attributes in Tomcat, Web Sphere MQ, Apache HTTP, IIS, and WAS | |
| 23 | The solution should support receiving events from Web Methods, IBM HTTP server, Apache Active MQ | No Change. | |
| 24 | The solution should have capability to monitor HTTP service, HTTPS service, FTP server statistics, POP/SMTP services, ICMP services or any customer specific port based systems | No Change. | |
| 25 | **Network Monitoring** | No Change. | |
| 26 | The solution should have network monitoring data available in the same console where every other information is available. | No Change. | |
| 27 | The solution should be able to capture network log errors | No Change. | |
| 28 | The solution should be able to do flow analysis | No Change. | |
| 29 | The solution should be able to track connectivity between network endpoints and display the delay between nodes | No Change. | |
| 30 | The solution should allow query of network events and performance data | No Change. | |
| 31 | The solution should provide network path monitoring | No Change. | |
| 32 | The solution should provide live network topology view | No Change. | |
| 33 | The solution should also provide configuration management on network devices | No Change. | |
| 34 | **Servers/System Monitoring** | No Change. | |

| | | | |
|---|---|---|---|
| 35 | The solution should allow monitoring of Server Status and Availability, CPU Utilization, Memory Utilization, Process Monitoring, File System Monitoring, Disk Utilization of RHEL/Centos, SUSE, Ubuntu servers/Windows 2008, 2012,2016,2019,2022. | The solution should allow monitoring of Server Status and Availability, CPU Utilization, Memory Utilization, Process Monitoring, File System Monitoring, Disk Utilization of RHEL/Centos, SUSE, Ubuntu servers/Windows 2016,2019,2022. | |
| 36 | The solution should support extensive monitoring capabilities from an OS (Linux, Windows)/ platform standpoint and should provide capabilities for customer to develop, deploy customized monitoring requirements | The solution should support extensive monitoring capabilities from an OS (Linux, Windows)/ platform standpoint and should provide capabilities for customer to deploy customized monitoring requirements | |
| 37 | The solution should do performance monitoring of Redhat Open Shift VM/containers and VMware environments, including VMware ESX /ESXi, vSphere, vCenter Server. | No Change. | |
| 38 | The solution should be able to monitor database from different aspects of the system including SQL Statements (memory, I/O , CPU intensive), wait types, server resources, storage I/O`s, virtualization layer, default users status , table spaces status and threshold utilization , raise warning or critical alerts where applicable. | No Change. | |
| 39 | The solution should be able to report on hardware details (like CPU, memory, fan state, power etc.) of servers from multi vendors like IBM, HP, Cisco, Dell and also VMware Hosts. | No Change. | |
| 40 | The solution should be able to gather capacity data from vCenter, HMC, Physical servers, etc. Generate report and provide recommendation. | The solution should be able to gather capacity data from vCenter, Physical servers, etc. and generate report for analysis. | |
| 41 | The solution should be able to monitor disk elements like RAID controllers, hard disks, RAIDs, failure prediction, availability of the volumes. | The vender can quote better solution. | |
| 42 | The solution should be able to monitor environment metrics like temperature, internal voltages, power supplies, fans. | No Change. | |

| | | | |
|---|---|---|---|
| 43 | The solution should be able to monitor critical hardware components like processors, memory modules, ECC errors, failure prediction. | No Change. | |
| 44 | **Storage Monitoring** | No Change. | |
| 45 | The solution should be able to monitor performance and capacity of physical and virtual storage infrastructure | No Change. | |
| 46 | The solution should be able to provide real-time, in-depth performance statistics after discovery/configuration of devices, including but not limited to:<br>- Array performance<br>- Controller Performance<br>- LUN performance<br>- Disk performance | **Removed** | |
| 47 | The solution should provide hardware health information for the storage array. | No Change. | |
| 48 | The solution should show statistics like Total IO/sec, service time, IO response time, queue length etc. | No Change. | |
| 49 | The solution should show storage growth rates and project when the storage capacity will be reached | No Change. | |
| 50 | The solution should be able to analyze the data coming from Dell EMC and Hitachi disk arrays, including:<br>- Storage units, Extent pools, Ranks, Storage volume.<br>- File Systems: Available and consumed capacity, list of CIFS shared, list of NFS exports, number of operations, data traffic, and so on.<br>- Physical Disks: Disk time utilization, number of operations, presence, traffic, response time, status, and so on.<br>- Storage Pools: Subscribed and consumed capacity, over subscription operation, number of operations, data traffic, and so on.<br>- Storage Systems: Available and subscribed capacity, number of operations, number of ports, number of operations, data traffic, status, and so on.<br>- Volumes: Consumed capacity, disk time utilization, list of hosts, host visible capacity, number of operations, paths, number of operations, data traffic, response times, status, time since last activity, and so on.<br>- Hardware components: fans, power supplies. | No Change. | |

| | | | |
|---|---|---|---|
| 51 | The solution should automatically map VMs and logical connections to physical storage environment to enable root-cause analysis | No Change. | |
| 52 | The solution should be able to monitor and manage multi-vendor storage systems with the same tool to detect performance issues and take proactive actions, | No Change. | |
| 53 | Logging/Reporting/Alert/threshold | No Change. | |
| 54 | The proposed solution should support to store all log of minimum 6 months period on external storage such as NAS/SAN. The required external storage (Hitachi VSP E590H through) will be provided by High Court of M.P. | No Change. | |
| 55 | Ensure logs are retained for at least six months with options for longer retention | No Change. | |
| 56 | The system should allow for customizable reports on performance, security events, and compliance. | No Change. | |
| 57 | Capability to schedule automated report generation and distribution via email or other channels. | No Change. | |
| 58 | Provide real-time analysis and reporting dashboards for immediate insights. | No Change. | |
| 59 | Enable real-time alerts for critical events, with customizable thresholds and conditions. | No Change. | |
| 60 | Support for alerts via email, SMS, or other communication channels. | No Change. | |
| 61 | Include options for escalating alerts based on severity and response time. | No Change. | |
| 62 | System should support global threshold and it should have option to define individual resource/interface statistics level threshold | No Change. | |
| 63 | Detect & highlight faults (abnormal situations) in near real-time occurring anywhere within the monitored IT Infrastructure | No Change. | |
| 64 | Provides Filtering, De-duplication, Holding, Suppression and Correlation capability to let user focus on the critical event that affects the business and business processes | No Change. | |
| 65 | Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement | Provides Severity definition, will handle events automatically and inform the designated person as per operational requirement | |
| 66 | System should support separate Rule Engine based alarms apart from the generic threshold.<br>a. Should have capability to configure | The system should have built-in functionality to define rules for alarms and monitoring, including real-time network | |

| | | | |
|---|---|---|---|
| | Device Group based, Node Based, Resources/Interface based, and Aggregation link based.<br>b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information<br>c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms<br>d. Rules should have option configure the breach based on min, max and average values.<br>e. Should have option to configure rules n repeat counters<br>f. Should have options to select custom alarm and clear alarm messages for individual configured rules<br>g. Should have option to send severity levels like error, warning and information<br>h. Notifications support based on configured rules | flow, traffic utilization, and protocol distribution. It should support threshold-based alarms and monitoring for the following components:<br>a) Disk utilization<br>b) Bandwidth utilization<br>c) CPU utilization<br>d) Interface utilization. | |
| 67 | Provides alarm suppression with hold time and aid in prevention of flooding | No Change. | |
| 68 | Supports instant diagnosis of the node status through Ping, Telnet and SNMP walk | No Change. | |
| 69 | **Other Features** | No Change. | |
| 70 | Cover geographically distributed networks through multi-level scalable distributed deployment architecture. | No Change. | |
| 71 | The tool should have option to be deployed in HA mode (High Availability) for redundancy purpose. | No Change. | |
| 72 | Capacity Reservations: tool should allow management of resource allocations and reservations (for services, applications or other needs), identify resource shortages and provide information for further analysis or procurement | Optional. | |
| 73 | Event Record & Classification: possible to generate event for all the monitoring devices, tool be used to define thresholds to generate events, collect from 3rd party using REST API , on regular interval Polling API and collect events from 3rd party system, classify them , assign different levels of severity to events | No Change. | |

| | | | |
|---|---|---|---|
| 74 | Configurations: create rules that automatically assign deadlines to events based on their impact on services or on end-users, create rules that perform automated assignment of events to the corresponding teams, create rules that control automated notification of interested stakeholders about events , automatically handling duplicate events, provide event correlation capabilities to combine a set of different events into one major event | Removed | |
| 75 | Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc. as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters. | No Change. | |
| 76 | System should have capability to configure business, non-business hours or custom time polling. This configuration should be available for every device as well as every component in the device. | No Change. | |
| 77 | Provision to disable and enable the polling of specific type of devices | No Change. | |
| 78 | System should have capability to configure the maintenance period for any device. When device is in maintenance period there is no polling done and the SLA clock on the device is stopped. | No Change. | |
| 79 | Provide a notification mechanism that allows administrator to define what notification channel to be used in different time of days, and able to trigger multiple notifications to alert multiple person and actions | No Change. | |
| 80 | System should provide many different types of topology representation. To perform the following:<br>1. Display physical connections of the different devices being monitored in the system.<br>2. Display flat maps of the entire network or networks in a single view<br>3. Display customer maps based on user configurations<br>4. Display maps based on geo locations | No Change. | |
| 81 | Licensing | No Change. | |
| 82 | Specify a base license for monitoring a minimum of 500 devices /application (Any | No Change. | |

| | | | |
|---|---|---|---|
| | kind of). Ensure the license is scalable up to 3,000 devices or applications without requiring a complete reinstallation or new licenses | | |
| 83 | Define costs for incremental license additions (per 100 devices/application(any kind)) | No Change. | |
| 84 | The bidder must provide all necessary hardware or compute resources required to manage and operate the monitoring system effectively, including servers, storage, and networking components, as per the specified scale of monitoring up to 3,000 devices or applications. | No Change. | |
| 85 | Ensure the software includes a robust license management tool to track and manage licenses as the environment grows. | No Change. | |
| 86 | Consider options for transferring licenses between devices or reallocating licenses as needs change. | No Change. | |
| 87 | The bidder must provide all necessary hardware or compute resources required to manage and operate the proposed monitoring system effectively, including servers, storage, and networking components, as per the specified scale of monitoring up to 3,000 devices /application (any kind) with required warranty/support. | No Change. | |
| 88 | The licenses should be perpetual with 05 years support/ updates/ upgrade. | The licenses should be On Prem Subscription with 05 years support and updates /upgrade. | |
| 89 | New Clause: | The proposed NMS solution must comply with recognized security standards, including ISO 27001:2013/ ISO 27034, OR CIS (Center for Internet Security) certifications, to ensure robust security management. | |

**Note:-**

1. **The tentative overall project cost has been revised to Rs. 05 Crore. Hence, the EMD has been increased to Rs. 10 Lakh from previous Rs. 03 Lakh and condition 2.15.2 of the tender document will change accordingly.**

2. The delivery and installation time is maximum 60 days to complete the project from date of ***Letter of Acceptance / Letter of Intent.***
3. The specifications s mentioned in tender document are minimum and the vendor may quote equivalent or higher specifications s for the products as mentioned in the tender document.
4. The total price of commercial bid inclusive of all taxes & expenses for 05 (Five) years on-site maintenance & support shall be taken as the basis for evaluation of commercial bids. In case of any discrepancy in the tax factor, the basic product price shall be taken in to consideration for finalization of bids.
5. The above clarifications are for all the prospective bidders for their tender reference and necessary action.
6. All future correspondence / clarifications / addendum / corrigendum shall be available on the website of the High Court of Madhya Pradesh i.e. www.mphc.gov.in and Government e-procurement portal www.mptenders.gov.in.
7. All the pages of the bids and Annexure's are to be sealed and signed by the authorized officers of the company / vendor.
8. All prospective bidders are requested to submit the bid with all relevant documents in sequenced manner, without fail.
9. The vendor to provide appropriate number of transceivers (fiber /copper) and fiber patch cords as per the number of ports in the quoted device from day 1.
10. All fiber transceivers should be single mode. The vendor can provide multimode transceivers in pair instead of single mode.

11. The decision of the High Court of Madhya Pradesh in selection/finalization of firm/vendor shall be final and no objection in this regard shall be entertained.
12. **The last date for online tender submission is hereby extended till 21st October, 2024 by 6:00 P.M., hard copy submission is 22nd October, 2024 by 5:00 P.M. and technical bid opening on 23rd October, 2024 at 11:30 A.M.**

**Sd/-**
**REGISTRAR GENERAL**