Corrigendum No. – I

Dt.: 04.11.2023

Tender Enquiry No- TPCODL/CCG/23-24/041

Tender Subject – Rate Contract for SITC of DDOS and WAF

Corrigendum Summary:

Tender Clause Reference	Remarks
A] Tender Clause 1.3	Extension of Bid submission date by 10 days

Note : See the details as listed underneath

A] Clause 1.3: Revised Calendar of Event shall be as follows:

(d)	Last Date of Posting Consolidated replies to all the pre-bid queries as received	05.11.2023, 18:00 Hours
(e)	Last date and time of receipt of Bids	14.11.2023, 18:00 Hours

NOTE : All Other Terms & Conditions of the tender shall remain unchanged as per NIT document, GCCs and Pre-bid reply.

Approved By,

Sd/-

(**Head – Centralized Contracts Group**)

S.No	Clause	Query	BA's Response	CCG RESPONES
1	Page No. 8/ Qualification Criteria	The bidder should have executed similar works (DDOS / WAF) for Supply, installation, Testing & commissioning for a single order value of Rs.3 Cr or Rs.5Cr for Cumulative 2 Orders or for Rs.10 Core for Cumulative 5 Orders each during the last 3 years.Copy of work order / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL/ TPSODL / TPWODL for supply of similar product, performance feedback of the same will be solely considered irrespective of the	Request you to please do the amendment on this Clause and write it as "The bidder should have executed similar works for Supply, installation, Testing & commissioning for a single order value of Rs.3 Cr or Rs.5Cr for Cumulative 2 Orders or for Rs.10 Core for Cumulative 5 Orders each during the last 3 years.Copy of work order / completion certificate to be submitted in this regard.	It will be as per NIT but complete of at least 1 Project of WAP / DDOS in DC Implementation environment should be present in previous work experience.
2	Page No. 9/ Qualification Criteria	Bidder should be a company registered in India to provide sales and 24x7 support in India with an office in Bhubaneswar/ Cuttack or any Local tie up with Firm presence in Bhubaneswar/ Cuttack. Bidder should submit the undertaking and details of address in this regards	Request you to please do the amendment on this Clause and write it as "The bidder should be a company registered in India with an office in Orissa. Bidder should submit the undertaking and details of address in this regard. In case of BA not having office in Odisha, they shall open new office in Odisha within 3 months of Release of Contract	Accepted along with below stipulations :- 1. OEM should Submit Compliance & Unpriced BoQ on their own Letter Head. 2.Installation to be carried out by OEM Personnel or OEM Authorized Person/Bidder but OEM needs to share the declaration against the same on their Letter head as taking
3	Page No. 10/ Evaluation Criteria	The bids will be evaluated commercially on an individual item basis (all-inclusive lowest cost at itemlevel) for the complete tender as calculated in Schedule of Items[Annexure I].	Request you to please do the amendment on this Clause and write it as "The Bidder can participate sperately which will allow to qoute for DDOS & WAF as per their feasibility.	The Clause will be amended as The Bidder should quote in Lot wise & the combination of the Lots will be as follows- Lot-1 :DDOS Lot-2: WAF BA Can Participate either or both LOT based on their competency. But EMD will be applicable as per

4	Page No. 20/ Point No. 4/ ANNEXURE II Technical Specification DDOS	Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP	Request you to please increase the ports and write it as Inspection Ports: 8 x 10 SFP+ and 8 x 1G SFP, the devices will be on HA and it has required min. 2 ports for connectivity and for feature expansion also.	No change in clause. This is minimum technical requirement. Bidders are free to add additional features.
5	Page No. 21/ Point No.15/ ANNEXURE II Technical Specification DDOS	The Proposed Solution should protect against Zero Day DDoS Attacks within few seconds, without any manual intervention.	Request you to please do the amendment and write it as "The Proposed Solution should protect against Zero Day DDoS Attacks in real time signature/footprint creation within 20 seconds, without any	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
6	Page No. 21/ Point No.21/ ANNEXURE II Technical Specification DDOS	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	Request you to please do the amendment and write it as "For Future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks. OEM own scrubbing Centre should based in INDIA". Also OEM should have its own scrubbing centre in INDIA, it should not be from third party. It will help to keep baseline information in sync between appliance and scrubbing centre in INDIA only which will	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
7	ANNEXURE II Technical Specifications DDOS : Clause No :4; Page no : 20	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Mitigation Throughput: 20Gbps Legitimate throughput handling: 2Gbps from day-1 and scalable up to 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	DDoS Flood Attack Prevention Rate: 25MPPS System Throughput: 40Gbps Ports: 8 x 10 SFP+ and 4 x 1GbE SFP Bypass port. Management: SSH CLI, Direct Console DB9 CLI, SNMP, Single Console per Cluster, XML-RPC, Out of Band Management – RJ45/DB9 * Data should be publically available : Very important bypass port was missing, along with some important parameters for management. So, We would like to	No change in clause. This is minimum technical requirement. Bidders are free to add additional features.

8	ANNEXURE II Technical Specifications DDOS : Clause No :5; Page no : 20	System should support horizontal and vertical port scanning behavioural protection	System should support horizontal and vertical port scanning behavioural protection or System should protect against port scanning of vulnerable services on a system, and mitigate DoS attacks, Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	This clause to be read as: System should support horizontal and vertical port scanning behavioural protection or System should protect against port scanning of vulnerable services on a system, and mitigate DoS attacks.
9	ANNEXURE II Technical Specifications DDOS : Clause No :6; Page no : 20	BEHAVIORAL ANALYSIS using behavioural algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioural algorithms and stateless solution to detect and defend against threats at L3-7.	BEHAVIORAL ANALYSIS using behavioural algorithms and automation to defend against IoT botnet threats. And DNS DDoS Mitigation. The solution should utilize behavioural algorithms and stateless solution to detect and defend against threats at L3-7, Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to	Lot-2: WAF
10	ANNEXURE II Technical Specifications DDOS : Clause No :10; Page no : 21	System should support DNS Challenge and DNS Rate Limit.	System should support DNS Challenge/DNS source verification and DNS Rate Limit, Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	This clause can be read as "System should support DNS Challenge/DNS Source Verification and DNS Rate Limit"
11	ANNEXURE II Technical Specifications DDOS : Clause No :11; Page no : 21	System should support HTTP Challenge Response authentication without Scripts	System should support HTTP Challenge Response authentication without Scripts/Client authentication - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider	Accepted Clause can be read as "System should support HTTP Challenge Response authentication without Scripts/client authentication"

12	ANNEXURE II Technical Specifications DDOS : Clause No :12; Page no : 21	System should have SIP Flood Protection, UDP and UDP Fragmented Flood.	The system should have TCP/UDP/ICMP DDoS mitigation : TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Fragment Flood, TCP Slow Connection, TCP Abnormal Connection - Please amend the clause to protect from most common and	All kind of protection has already been asked in the specifications. No Change, As per the RFP
13	ANNEXURE II Technical Specifications DDOS : Clause No :13; Page no : 21	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures apart from custom Signatures from Day 1.	System should support In-Line/Bridge mode, SPAN Port/TAP mode, Out-of-Path deployment modes from day 1. System should have capability to allow custom signature creation apart from inbuilt signatures 3000 from day 1 - We would like to Request the Honourable tendering committee to amend the clause as different OEM use different terminology for same function and quality of the signature is more important than the number of signatures.	Sufficient number of signature is very important to address known attacks. The asked deployment mode is minimum requirement. Clause Amended. Clause can be read as "System should support In-Line/Bridge, SPAN Port/TAP Mode, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt
14	ANNEXURE II Technical Specifications DDOS : Clause No :16; Page no : 21	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection	The appliance should support Dynamic profiling, Automatic DDoS profile, Manual DDoS Profile, Application & network DDoS profile, Dynamic refreshing of automatic DDoS profile based on learning results.-Different OEM has different profile types and names. So, We would like to Request the Honourable tendering committee to use generic terminology to cover all type of profiling and amend the clause as requested for wider participation.	This clasue to be read as solution must provide proetection against following types of attacks: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection There are different kinds of attacks which falls under DDoS attack, in order to mitigate these attacks vendor should have dedicated security engines. This is minimum technical requirement. Bidders may provide

15	ANNEXURE II Technical Specifications WAF : Clause No :1; Page no : 22	Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security with integrated functionalities of Application Load Balancer and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	The proposed Network Function Appliance should be multi-tenanted appliance and have capabilities to run multiple 3rd party and open source independent virtual instance of Network functions with dedicated Hardware resources for future requirements and scalability in the same appliance. Each virtual instance contains a complete and separated environment of resources, configuration, management, OS and have capability to host open source virtual network Functions and CentOS & Ubuntu to incorporate new technologies in the same appliance. - We would like to Request the Honourable tendering committee to amend the clause as requested to get flexibility to incorporate	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
16	ANNEXURE II Technical Specifications WAF : Clause No :4; Page no : 22	The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be complete in all respect. 10gig interface should be	The Web Application Firewall shall have at least 04 nos. 10G SFP+ ports complying to IEEE 802.3 standard. - We would like to request the tendering committee to amend the clause for better interoperability.	Accepted: This clause to be read as "Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10
17	ANNEXURE II Technical Specifications WAF : Clause No :5; Page no : 22	The Web Application Firewall shall have minimum 02 nos. 40Gig ports and at least 02 nos. 25Gig ports from day 01	Clause no 4, 5 , 6 is contradicting, please cla	Tender Clause Stands. Follow ammended clause 4.
18	ANNEXURE II Technical Specifications WAF : Clause No :6; Page no : 22	The Web Application Firewall shall have 4 x 10G, 2 x 25G, 2 x 40G Transceivers module/SFP populated from day 01	Clause no 4, 5 , 6 is contradicting, please cla	Tender Clause Stands. Follow ammended clause 4.
19	ANNEXURE II Technical Specifications WAF : Clause No :7; Page no : 22	The Web Application Firewall shall have a 100/1000 Base Tx Port for out of bound management.	The Web Application Firewall shall have a 100/1000 Base T Port for out of bound management.- We would like to request the tendering committee to amend the clause as 100/1000 Base T ports are widely used and provide better interoperability.	Accepted. Tender clause is to be read as follows : "The Web Application Firewall shall have a 100/1000 Base T Port for

20	ANNEXURE II Technical Specifications WAF : Clause No :12; Page no : 23	The Web Application Firewall shall be capable of working with AC Power supply with a Voltage varying from 170 –240 Volts at 50 +/- 2 Hz.	The Web Application Firewall shall be capable of working with AC Power supply with a Voltage varying from 90 –264 Volts at 47-63 Hz.- We would like to request the tendering committee to amend the clause	No Change. The Clause remains same.
21	ANNEXURE II Technical Specifications WAF : Clause No :13; Page no : 23	The Web Application Firewall shall support 19” Rack mounting with 1U form factor.	The Web Application Firewall shall support 19” Rack mounting with 1U/2U form factor. - Different OEM have different manufacturing strategy and models So, we would like to request the tendering committee to amend the clause as	Accepted. Tender clause is to be read as follows : "The Web Application Firewall shall support 19” Rack mounting with
22	ANNEXURE II Technical Specifications WAF : Clause No :4; Page no : 23	The Web Application Firewall Solution shall have minimum 10 Million HTTP request / second.	The Web Application Firewall Solution shall have minimum 5 Million HTTP request / second. - Performance parameters are not inline with other performance requirements, So, we would like to request the tendering committee to amend the	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
23	ANNEXURE II Technical Specifications WAF : Clause No :5; Page no : 23	The WAF shall support minimum 60,000 RSA and 30,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	The WAF shall support minimum 40,000 RSA and 25,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.- Performance parameters are not inline with other performance requirements, So, we would like to request the tendering	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
24	ANNEXURE II Technical Specifications WAF : Clause No :6; Page no : 23	The Application Delivery Controller shall support minimum of 30 Gbps SSL throughput and hardware compression of 30Gbps.	The Application Delivery Controller shall support minimum of 30 Gbps SSL throughput and hardware compression of 25Gbps.- Performance parameters are not inline with other performance requirements, So, we would like to request the tendering committee to amend the	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

25	ANNEXURE II Technical Specifications WAF : Clause No :8; Page no : 24	The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration withautomation and CI/CD tools including Ansible, Jenkins, and Terraform.	The software solution must support Programmability to support Automation using XML-RPC, RESTful API.- Ansible, terraform, & Jenkins Pipeline are suite of plugins, and mainly used for software coding and testing purpose. We would like to request the tendering committee to amend the clause as requested for wider	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
26	ANNEXURE II Technical Specifications WAF : Clause No :10; Page no : 24	Should support virtualization with its own hypervisor (NOT any third party or open source) that virtualizes the Device resources—including CPU, memory, management and configuration. The proposed device should have 8 Virtual Instances from Day 1 scalable to 20 using license upgrade.	Should support virtualization with its own hypervisor (NOT any third party or open source) that virtualizes the Device resources—including CPU, memory, management and configuration. The proposed device should have 8 Virtual Instances from Day 1,scalable to 32 without any additional license. - We would like to request the tendering committee to amend the clause as requested to get better flexibility and best techno-	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
27	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No :1; Page no : 24	The Web Application Firewall shall have integration with REDHAT OpenShift Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from same make as WAF. It should not be third party or	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
28	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :1; Page no : 24	The Controller/Container Plugin shall support both Nodeport and ClusterIP mode of deployment and also as an Ingress service.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

29	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :3; Page no : 24	The Controller/Container Plugin shall support Application Delivery Controller orchestration to dynamically create and manage WAF objects.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
30	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :4; Page no : 24	The Controller/Container Plugin shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
31	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :5; Page no : 24	The Web Application Firewall shall be capable to forward traffic to container cluster via NodePort and ClusterIP.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
32	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :6; Page no : 24	The Controller/Container Plugin shall support the configuration of advanced services like Web application firewalls through declarative syntax.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
33	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :7; Page no : 25	The Controller/Container Plugin shall support integration using latest Container network interface (CNI) for the container platform.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

34	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No :8; Page no : 25	The Web Application Firewall shall support NodePort mechanism for integration with kubernetes services.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
35	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :9; Page no : 25	The Web Application Firewall shall support BGP for integration with kubernetes services.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
36	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :10; Page no : 25	The Web Application Firewall shall support overlay network like VxLAN/Geneve for integration with kubernetes services	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
37	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No :11; Page no : 25	WAF should integrates with REDHAT Openshift container orchestration environments to dynamically create L4/L7 services on WAF, and load balance network traffic across the services. Monitoring the orchstration API server, Solution should be able to modify the WAF configuration based on changes made to containerized	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
38	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :12; Page no : 25	Installation of Controller/Container Plugin should be using Operators on OpenShift Cluster and Helm charts.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

39	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No :13; Page no :25	Controller/Container Plugin should use open shift route resources and support route annotations.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
40	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :14; Page no : 25	Controller/Container Plugin should use multiple Virtual IP addresses	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
41	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No :15; Page no : 25	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should registers to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
42	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :2; Page no : 25	The Web Application Firewall Solution shall support the following Load Balancing Features Support for 200 servers Support load balancing algorithms Least connection Ratio Round Robin weighted Least connection	The Web Application Firewall Solution shall support the following Load Balancing Features Support for 200 servers Support load balancing algorithms Least connection Round Robin weighted Least connection - OEM specific terminology, We would like to request the tendering committee to amend the clause as requested for wider participation.	Tender Clause Stands.

43	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No :4; Page no : 26	The Web Application Firewall Solution shall be able to learn the Web Application Structure & elements to address the difficulty of configuring the positive security model.	The Web Application Firewall Solution should have APPLICATION SECURITY VISIBILITY to address the difficulty of configuring the positive security model. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	Tender clause is to be read as follows : "The Web Application Firewall Solution shall be able to learn the Web Application Structure/Application security visibility & elements to address the difficulty of configuring the positive
44	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :5; Page no : 26	The Web Application Firewall Solution in learning mode shall be able to recognize application changes while simultaneously protecting Web applications and learned values shall be used as the configuration for input checking in the positive security model.	The Web Application Firewall Solution should automatically learn the normal traffic to form positive whitelist and refresh the WAF profile dynamically. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
45	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :7; Page no : 26	The Web Application Firewall Solution shall support the following Action Mode: Block Block & Report Report only	The Web Application Firewall Solution shall support the following Action Mode: detect: only records attack logs but not block attacks defend: prevents attacks and records attack logs. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	Tender clause is to be read as follows : "The Web Application Firewall Solution shall support the following Action Mode: Block Block & Report/defend Report only/detect"
46	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :8; Page no : 26	The Web Application Firewall Solution shall support full coverage of OWASP Top 10 web application security risks: A1-Injection A2-Broken Authentication A3-Sensitive Data Exposure A4-XML External Entities (XXE) A5- Broken Access Control A6-Security Misconfiguration A7- Cross-Site Scripting XSS: A8-Inscure Deserialization A9-Using Components with Known Vulnerabilities	The Web Application Firewall Solution shall support full coverage of OWASP top 10. - We would like to request the tendering committee to amend the clause as requested as OWASP top 10 list is dynamic and sufficient for this clause.	This clause to be read as "The Web Application Firewall Solution shall support full coverage of OWASP 2021 or later top 10 web application security risks:"

47	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :9; Page no : 27	The Web Application Firewall Solution shall prevent the Following attacks: XSS SQL injection Directory\path traversal Forceful browsing HTTP response splitting OS command injection LDAP injection SSI injections XPath injection Sensitive information leakage (e.g., CCN, SSN, custom defined) Application DOS / DDOS CSRF Evasion and illegal encoding XML validation Web services method restrictions and validation HTTP RFC violations Form field tampering Parameter tampering From field manipulation Session hijacking Protocol validation XML and Web services protection Web application vulnerabilities Cookie poisoning Application buffer overflow Brute force Access to predictable resource locations Unauthorized navigation	The Web Application Firewall Solution shall prevent the Following attacks: OWASP Top 10, API Security including SOAP, XML and JSON, WASC Classification. • Signature-based defence, preventing SQL injection, XSS, network crawlers, CSRF attacks, leech, Webshell, local/remote file inclusion, command injection, sensitive data leakage, and so on, and supporting one-click signature exclusion. • Identity card information, phone number, email address, bankcard number DLP rules and content filter • CSRF defence, anti-leech, anti-crawling/scanning, unauthorized navigation, predefined resource location. • Positive WAF Security Model and negative security model. • Automatic traffic learning, automatic generation of positive whitelists, defence against “Zero-day” attacks, learning the traffic pattern of only trusted sources HTTP GET Flood, HTTP POST flood, HTTP Slowloris attack, HTTP Slow POST attack, HTTP CC attack, HTTP Packet Anomaly attacks,SMTP and FTP protection • SSL Handshake attack, SSL Renegotiation	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

48	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :11; Page no : 28	The Web Application Firewall Solution shall be able to prevent automated layer 7 DDoS attacks, web scraping, and brute force attacks from being directed to the site.	The Web Application Firewall Solution shall be able to prevent automated layer 7 DDoS attacks, bot, and brute force attacks from being directed to the site.- Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider	No change in clause. This is minimum technical requirement. Bidders are free to quote additional or similar features.
49	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :12; Page no : 28	The Web Application Firewall Solution shall have "anti-automation" protection which can block the automated attacks using hacking tools, scripts, frameworks, etc.	The Web Application Firewall Solution shall have protection from automated attacks using hacking tools, scripts, frameworks, etc. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
50	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :19; Page no : 28	The Web Application Firewall Solution shall support integration with VA scanning tools to imports the XML report and provide a quick fix of the vulnerabilities including Acunetix, Qualys, Rapid 7, IBM Appscan etc. to virtually patch web application vulnerabilities.	The Web Application Firewall Solution shall support integration with VA scanning tools to virtually patch web application vulnerabilities. - The requirement is integration with third-party VA tools for virtual patching, We would like to Request the Honourable tendering committee to	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
51	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :28; Page no : 30	The Web Application Firewall Solution shall support switching the security modules form learning/passive to active/blocking mode.	The Web Application Firewall Solution shall support switching the security modules form learning/passive to active/blocking mode or Similar. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider	Accepted
52	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No :33; Page no : 30	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.	The solution should provide protection from OWASP top 10 attacks.- We would like to Request the Honourable tendering committee to amend the clause as requested for wider participation.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

53	ANNEXURE II Technical Specifications WAF Management & Reporting Clause No :4; Page no : 31	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link.	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link or Via TAC Support. - Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

54	ANNEXURE II Technical Specifications WAF Management & Reporting Clause No :5; Page no : 31	WAF should provide the application visibility and reporting with the below metrics and entity for each application: • Client IP addresses/subnets as well as geographical regions • Total Transactions as well as Average and Max Transactions/sec • Most commonly requested URLs • Server Latency and Page Load times • Virtual Server and Pool server performance • Page Load Time • Response code • OS and Browser • URL details	WAF should provide the application visibility and reporting with the below: • Providing rich event logs to facilitate the replay and audit of attacks. • Providing WAF attack logs, WAF audit logs, HTTP access logs. DDoS warning logs, DDoS attack logs and HTTP filter logs • Supporting admin audit logs to facilitate the auditing against administrators. • Supporting exporting security event logs. • Providing granular and intuitive graphic monitoring. • Displaying system status such as CPU usage, RAM usage, disk usage and throughput. • Displaying attack statistics, covering severity distribution, attack type, attack sources, attack source regions and so on. • Displaying service traffic statistics, including detailed statistics for the traffic of different protocols. • Displaying packet drop statistics including the drop reason statistics. • Displaying service access statistics, including the TopN accessed URLs, client IPs and so on. • Supporting custom monitoring pages by adding desired monitoring graphs. • Supporting exporting monitoring graphs manually and generating monitoring report periodically	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
55	ANNEXURE II Technical Specifications WAF User's access for management.Clause No :4; Page no : 31	The management server must support the archiving and it shall be able to export logs/events using NFS/SMB/SCP/SFTP.	The management server must support the archiving and it shall be able to export logs/events. - Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider participation.	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.

56	ANNEXURE II Technical Specifications WAF User’s access for management.Clause No :7; Page no : 32	The Web Application Firewall shall generate alarms w.r.t. health status of Server/s, security alarms for TCP SYN attacks, DoS attacks, etc.	The Solution can provide Server health status and security alarms for TCP SYN attacks, DoS attacks, etc. - Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
57	ANNEXURE II Technical Specifications WAF Product / OEM Evaluation CriteriaClause No :1; Page no : 33	WAF / WAF’s Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of India.	WAF / WAF’s Operating System should be tested and certified for EAL 2 /ICES-003/ NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of India.- We would like to Request the Honourable	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
58	ANNEXURE II Technical Specifications WAF Product / OEM Evaluation Criteria Clause No :2; Page no : 33	The WAF solution should be in the Gartner's Magic Quadrant of Latest published Gartner Report “Web Application and API Protection”	The WAF solution should be in the Gartner's Magic Quadrant of Latest published Gartner Report or ICSA lab Certified.	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
59	ANNEXURE II Technical Specifications WAF High Availability Clause No :1; Page no : 33	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active using standard VRRP (No Proprietary Protocol). - We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
60	ANNEXURE II Technical Specifications WAF High Availability Clause No :2; Page no : 33	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices with SSL session mirroring.	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices. - Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.

61	ANNEXURE II Technical Specifications DDOS - Clause No 4 of page No 20	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Mitigation Throughput: 20Gbps Legitimate throughput handling: 2Gbps from day-1 and scalable up to 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	DDoS Flood Attack Prevention Rate: 25MPPS System Throughput: 40Gbps Ports: 8 x 10 SFP+ and 4 x 1GbE SFP Bypass port. Management: SSH CLI, Direct Console DB9 CLI, SNMP, Single Console per Cluster, XML-RPC, Out of Band Management – RJ45/DB9 * Data should be publically available - Very important bypass port was missing, along with some important parameters for management. So, We would like to	As appliance has been asked in HA, bypass is not required. MNG port should be redundant in nature as asked appliance can only be managed via MNG port.No change in clause. This is minimum technical requirement. Bidders are free to add additional features.
62	ANNEXURE II Technical Specifications DDOS Clause No 5 of page No 20	System should support horizontal and vertical port scanning behavioural protection	System should support horizontal and vertical port scanning behavioural protection or System should protect against port scanning of vulnerable services on a system, and mitigate DoS attacks.- Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	This clause to be read as: System should support horizontal and vertical port scanning behavioural protection or System should protect against port scanning of vulnerable services on a system, and mitigate DoS attacks.
63	ANNEXURE II Technical Specifications DDOS Clause No 6 of page No 20	BEHAVIORAL ANALYSIS using behavioural algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioural algorithms and stateless solution to detect and defend against threats at L3-7.	BEHAVIORAL ANALYSIS using behavioural algorithms and automation to defend against IoT botnet threats. And DNS DDoS Mitigation. The solution should utilize behavioural algorithms and stateless solution to detect and defend against threats at L3-7. -Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to	The asked requirement is minimum, vendor can quote accordingly. No Change, As per the RFP
64	ANNEXURE II Technical Specifications DDOS Clause No 10 of page No 21	System should support DNS Challenge and DNS Rate Limit.	System should support DNS Challenge/DNS source verification and DNS Rate Limit.- Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	This clause can be read as "System should support DNS Challenge/DNS Source Verification and DNS Rate Limit"

65	ANNEXURE II Technical Specifications DDOS Clause No 11 of page No 21	System should support HTTP Challenge Response authentication without Scripts	System should support HTTP Challenge Response authentication without Scripts/Client authentication.-Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider	Accepted Clause can be read as "System should support HTTP Challenge Response authentication without Scripts/client authentication"
66	ANNEXURE II Technical Specifications DDOS Clause No 12 of page No 21	System should have SIP Flood Protection, UDP and UDP Fragmented Flood.	The system should have TCP/UDP/ICMP DDoS mitigation : TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Fragment Flood, TCP Slow Connection, TCP Abnormal Connection-Please amend the clause to protect from most common and	All kind of protection has already been asked in the specifications. No Change, As per the RFP
67	ANNEXURE II Technical Specifications DDOS Clause No 13 of page No 21	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures apart from custom Signatures from Day 1.	System should support In-Line/Bridge mode, SPAN Port/TAP mode, Out-of-Path deployment modes from day 1. System should have capability to allow custom signature creation apart from inbuilt signatures 3000 from day 1.-We would like to Request the Honourable tendering committee to amend the clause as different OEM use different terminology for same function and quality of the signature is more important than the number of signatures.	Sufficient number of signature is very important to address known attacks. The asked deployment mode is minimum requirement. Clause Amended. Clause can be read as "System should support In-Line/Bridge, SPAN Port/TAP Mode, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt

68	ANNEXURE II Technical Specifications DDOS Clause No 16 of page No 21	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection	The appliance should support Dynamic profiling, Automatic DDoS profile, Manual DDoS Profile, Application & network DDoS profile, Dynamic refreshing of automatic DDoS profile based on learning results. -Different OEM has different profile types and names. So, We would like to Request the Honourable tendering committee to use generic terminology to cover all type of profiling and amend the clause as requested for wider participation.	This clasue to be read as solution must provide proetection against following types of attacks: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection There are different kinds of attacks which falls under DDoS attack, in order to mitigate these attacks vendor should have dedicated security engines. This is minimum technical requirement. Bidders may provide
69	ANNEXURE II Technical Specifications WAF Clause No 1 of page No 22	Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security with integrated functionalities of Application Load Balancer and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	The proposed Network Function Appliance should be multi-tenanted appliance and have capabilities to run multiple 3rd party and open source independent virtual instance of Network functions with dedicated Hardware resources for future requirements and scalability in the same appliance. Each virtual instance contains a complete and separated environment of resources, configuration, management, OS and have capability to host open source virtual network Functions and CentOS & Ubuntu to incorporate new technologies in the same appliance.-We would like to Request the Honourable tendering committee to amend the clause as requested to get flexibility to incorporate	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

70	ANNEXURE II Technical Specifications WAF Clause No 4 of page No 22	The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be complete in all respect. 10gig interface should be	The Web Application Firewall shall have at least 04 nos. 10G SFP+ ports complying to IEEE 802.3 standard. -We would like to request the tendering committee to amend the clause for better interoperability.	Accepted: This clause to be read as "Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10
71	ANNEXURE II Technical Specifications WAF Clause No 5 of page	The Web Application Firewall shall have minimum 02 nos. 40Gig ports and at least 02 nos. 25Gig ports from day 01	Clause no 4, 5 , 6 is contradicting, please cla	Tender Clause Stands. Follow ammended clause 4.
72	ANNEXURE II Technical Specifications WAF Clause No 6 of page	The Web Application Firewall shall have 4 x 10G : 2 x 25G: 2 x 40G Transceivers module/SFP populated from day 01	Clause no 4, 5 , 6 is contradicting, please cla	Tender Clause Stands. Follow ammended clause 4.
73	ANNEXURE II Technical Specifications WAF Clause No 7 of page No 22	The Web Application Firewall shall have a 100/1000 Base Tx Port for out of bound management.	The Web Application Firewall shall have a 100/1000 Base T Port for out of bound management. - We would like to request the tendering committee to amend the clause as 100/1000 Base T ports are widely used and provide better interoperability.	Accepted. Tender clause is to be read as follows : "The Web Application Firewall shall have a 100/1000 Base T Port for
74	ANNEXURE II Technical Specifications WAF Clause No 12 of page No 23	The Web Application Firewall shall be capable of working with AC Power supply with a Voltage varying from 170 –240 Volts at 50 +/- 2 Hz.	The Web Application Firewall shall be capable of working with AC Power supply with a Voltage varying from 90 –264 Volts at 47-63 Hz. - We would like to request the tendering committee to amend the clause	No Change. The Clause remains same.
75	ANNEXURE II Technical Specifications WAF Clause No 13 of page No 23	The Web Application Firewall shall support 19” Rack mounting with 1U form factor.	The Web Application Firewall shall support 19” Rack mounting with 1U/2U form factor. - Different OEM have different manufacturing strategy and models So, we would like to request the tendering committee to amend the clause as	Accepted. Tender clause is to be read as follows : "The Web Application Firewall shall support 19” Rack mounting with
76	ANNEXURE II Technical Specifications WAF Clause No 4 of page No 23	The Web Application Firewall Solution shall have minimum 10 Million HTTP request / second.	The Web Application Firewall Solution shall have minimum 5 Million HTTP request / second. - Performance parameters are not inline with other performance requirements, So, we would like to request the tendering committee to amend the	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.

77	ANNEXURE II Technical Specifications WAF Clause No 5 of page No 23	The WAF shall support minimum 60,000 RSA and 30,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	The WAF shall support minimum 40,000 RSA and 25,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
78	ANNEXURE II Technical Specifications WAF Clause No 6 of page No 23	The Application Delivery Controller shall support minimum of 30 Gbps SSL throughput and hardware compression of 30Gbps.	The Application Delivery Controller shall support minimum of 30 Gbps SSL throughput and hardware compression of 25Gbps. - Performance parameters are not inline with other performance requirements, So, we would like to request the tendering committee to amend the	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
79	ANNEXURE II Technical Specifications WAF Clause No 9 of page No 24	The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration withautomation and CI/CD tools including Ansible, Jenkins, and Terraform.	The software solution must support Programmability to support Automation using XML-RPC, RESTful API.-Ansible, terraform, & Jenkins Pipeline are suite of plugins, and mainly used for software coding and testing purpose. We would like to request the tendering committee to amend the clause as requested for wider	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
80	ANNEXURE II Technical Specifications WAF Clause No 10 of page No 24	Should support virtualization with its own hypervisor (NOT any third party or open source) that virtualizes the Device resources—including CPU, memory, management and configuration. The proposed device should have 8 Virtual Instances from Day 1 scalable to 20 using license upgrade.	Should support virtualization with its own hypervisor (NOT any third party or open source) that virtualizes the Device resources—including CPU, memory, management and configuration. The proposed device should have 8 Virtual Instances from Day 1,scalable to 32 without any additional license. - We would like to request the tendering committee to amend the clause as requested to get better flexibility and best techno-	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
81	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 1 of page No 24	The Web Application Firewall shall have integration with REDHAT OpenShift Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from same make as WAF. It should not be third party or	We would like to request the tendering committee to remove this clause for wider participation. - We would like to request the tendering committee to amend the clause as requested to get better flexibility and best techno-commercial product available in the market.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

82	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No2 of page No 24	The Controller/Container Plugin shall support both Nodeport and ClusterIP mode of deployment and also as an Ingress service.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
83	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 3 of page No 24	The Controller/Container Plugin shall support Application Delivery Controller orchestration to dynamically create and manage WAF objects.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
84	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 4 of page No 24	The Controller/Container Plugin shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
85	ANNEXURE II Technical Specifications WAF Native and Kubern etes integration Features:Clause No 5 of page No 24	The Web Application Firewall shall be capable to forward traffic to container cluster via NodePort and ClusterIP.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
86	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 6 of page No 24	The Controller/Container Plugin shall support the configuration of advanced services like Web application firewalls through declarative syntax.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

87	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 7 of page No 25	The Controller/Container Plugin shall support integration using latest Container network interface (CNI) for the container platform.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
88	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 8 of page No 25	The Web Application Firewall shall support NodePort mechanism for integration with kubernetes services.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
89	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No 9 of page No 25	The Web Application Firewall shall support BGP for integration with kubernetes services.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
90	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features: Clause No 10 of page No 25	The Web Application Firewall shall support overlay network like VxLAN/Geneve for integration with kubernetes services	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
91	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No 11 of page No 25	WAF should integrates with REDHAT Openshift container orchestration environments to dynamically create L4/L7 services on WAF, and load balance network traffic across the services. Monitoring the orchstration API server, Solution should be able to modify the WAF configuration based on changes made to containerized	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

92	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No 12 of page No 25	Installation of Controller/Container Plugin should be using Operators on OpenShift Cluster and Helm charts.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
93	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No 13 of page No 25	Controller/Container Plugin should use open shift route resources and support route annotations.	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
94	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No 14 of page No 25	Controller/Container Plugin should use multiple Virtual IP addresses	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
95	ANNEXURE II Technical Specifications WAF Native and Kubernetes integration Features:Clause No 15 of page No 25	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should registers to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource	We would like to request the tendering committee to remove this clause for wider participation.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

96	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No 2 of page No 25	The Web Application Firewall Solution shall support the following Load Balancing Features Support for 200 servers Support load balancing algorithms Least connection Ratio Round Robin weighted Least connection	The Web Application Firewall Solution shall support the following Load Balancing Features Support for 200 servers Support load balancing algorithms Least connection Round Robin weighted Least connection - OEM specific terminology, We would like to request the tendering committee to amend the clause as requested for wider participation.	Tender Clause Stands.
97	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 4 of page No 26	The Web Application Firewall Solution shall be able to learn the Web Application Structure & elements to address the difficulty of configuring the positive security model.	The Web Application Firewall Solution should have APPLICATION SECURITY VISIBILITY to address the difficulty of configuring the positive security model. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	Tender clause is to be read as follows : "The Web Application Firewall Solution shall be able to learn the Web Application Structure/Application security visibility & elements to address the difficulty of configuring the positive
98	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 5 of page No 26	The Web Application Firewall Solution in learning mode shall be able to recognize application changes while simultaneously protecting Web applications and learned values shall be used as the configuration for input checking in the positive security model.	The Web Application Firewall Solution should automatically learn the normal traffic to form positive whitelist and refresh the WAF profile dynamically. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
99	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements:Clause No 7 of page No 26	The Web Application Firewall Solution shall support the following Action Mode: Block Block & Report Report only	The Web Application Firewall Solution shall support the following Action Mode: detect: only records attack logs but not block attacks defend: prevents attacks and records attack logs. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	Tender clause is to be read as follows : "The Web Application Firewall Solution shall support the following Action Mode: Block Block & Report/defend Report only/detect"

100	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 8 of page No 26	The Web Application Firewall Solution shall support full coverage of OWASP Top 10 web application security risks: A1-Injection A2-Broken Authentication A3-Sensitive Data Exposure A4-XML External Entities (XXE) A5- Broken Access Control A6-Security Misconfiguration A7- Cross-Site Scripting XSS: A8-Inscure Deserialization A9-Using Components with Known Vulnerabilities	The Web Application Firewall Solution shall support full coverage of OWASP top 10. - We would like to request the tendering committee to amend the clause as requested as OWASP top 10 list is dynamic and sufficient for this clause.	This clause to be read as "The Web Application Firewall Solution shall support full coverage of OWASP 2021 or later top 10 web application security risks:"

101	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 9 of page No 27	The Web Application Firewall Solution shall prevent the Following attacks: XSS SQL injection Directory\path traversal Forceful browsing HTTP response splitting OS command injection LDAP injection SSI injections XPath injection Sensitive information leakage (e.g., CCN, SSN, custom defined) Application DOS / DDOS CSRF Evasion and illegal encoding XML validation Web services method restrictions and validation HTTP RFC violations Form field tampering Parameter tampering From field manipulation Session hijacking Protocol validation XML and Web services protection Web application vulnerabilities Cookie poisoning Application buffer overflow Brute force Access to predictable resource locations Unauthorized navigation	The Web Application Firewall Solution shall prevent the Following attacks: OWASP Top 10, API Security including SOAP, XML and JSON, WASC Classification. • Signature-based defence, preventing SQL injection, XSS, network crawlers, CSRF attacks, leech, We would like to Request the Honourable tendering committee to amend the clause requested as its using generic terminology and attack names. Webshell, local/remote file inclusion, command injection, sensitive data leakage, and so on, and supporting one-click signature exclusion. • Identity card information, phone number, email address, bankcard number DLP rules and content filter • CSRF defence, anti-leech, anti-crawling/scanning, unauthorized navigation, predefined resource location. • Positive WAF Security Model and negative security model. • Automatic traffic learning, automatic generation of positive whitelists, defence against “Zero-day” attacks, learning the traffic pattern of only trusted sources HTTP GET Flood, HTTP POST flood, HTTP Slowloris attack, HTTP Slow POST attack	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
102	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 11 of page No 28	The Web Application Firewall Solution shall be able to prevent automated layer 7 DDoS attacks, web scraping, and brute force attacks from being directed to the site.	The Web Application Firewall Solution shall be able to prevent automated layer 7 DDoS attacks, bot, and brute force attacks from being directed to the site.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional or similar features.

103	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 12 of page No 28	The Web Application Firewall Solution shall have "anti-automation" protection which can block the automated attacks using hacking tools, scripts, frameworks, etc.	The Web Application Firewall Solution shall have protection from automated attacks using hacking tools, scripts, frameworks, etc. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
104	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 19 of page No 28	The Web Application Firewall Solution shall support integration with VA scanning tools to imports the XML report and provide a quick fix of the vulnerabilities including Acunetix, Qualys, Rapid 7, IBM Appscan etc. to virtually patch web application vulnerabilities.	The Web Application Firewall Solution shall support integration with VA scanning tools to virtually patch web application vulnerabilities. - The requirement is integration with third-party VA tools for virtual patching, We would like to Request the Honourable tendering committee to	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
105	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 28 of page No 30	The Web Application Firewall Solution shall support switching the security modules form learning/passive to active/blocking mode.	The Web Application Firewall Solution shall support switching the security modules form learning/passive to active/blocking mode or Similar. - Different OEM has different terminology for similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as requested for wider	Accepted
106	ANNEXURE II Technical Specifications WAF Web Application Firewall Solution Functional Requirements: Clause No 33 of page No 30	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.	The solution should provide protection from OWASP top 10 attacks. - We would like to Request the Honourable tendering committee to amend the clause as requested for wider participation.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

107	ANNEXURE II Technical Specifications WAF Management & Reporting Clause No 4 of page No 31	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link.	The solution should provide online troubleshooting and traffic analysis tool where the administrator can take a snapshot of the config and upload it on web based diagnostic tool to check the health and vulnerability of the solution with the recommended solution provided on the knowledge base link or Via TAC Support - Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

108	ANNEXURE II Technical Specifications WAF Management & Reporting Clause No 5 of page No 31	WAF should provide the application visibility and reporting with the below metrics and entity for each application: • Client IP addresses/subnets as well as geographical regions • Total Transactions as well as Average and Max Transactions/sec • Most commonly requested URLs • Server Latency and Page Load times • Virtual Server and Pool server performance • Page Load Time • Response code • OS and Browser • URL details	WAF should provide the application visibility and reporting with the below: • Providing rich event logs to facilitate the replay and audit of attacks. • Providing WAF attack logs, WAF audit logs, HTTP access logs. DDoS warning logs, DDoS attack logs and HTTP filter logs • Supporting admin audit logs to facilitate the auditing against administrators. • Supporting exporting security event logs. • Providing granular and intuitive graphic monitoring. • Displaying system status such as CPU usage, RAM usage, disk usage and throughput. • Displaying attack statistics, covering severity distribution, attack type, attack sources, attack source regions and so on. • Displaying service traffic statistics, including detailed statistics for the traffic of different protocols. • Displaying packet drop statistics including the drop reason statistics. • Displaying service access statistics, including the TopN accessed URLs, client IPs and so on. • Supporting custom monitoring pages by adding desired monitoring graphs. • Supporting exporting monitoring graphs manually and generating monitoring report periodically.	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
109	ANNEXURE II Technical Specifications WAF User's access for management. Clause No 4 of page No 31	The management server must support the archiving and it shall be able to export logs/events using NFS/SMB/SCP/SFTP.	The management server must support the archiving and it shall be able to export logs/events. Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.

110	ANNEXURE II Technical Specifications WAF User’s access for management. Clause No 7 of page No 32	The Web Application Firewall shall generate alarms w.r.t. health status of Server/s, security alarms for TCP SYN attacks, DoS attacks, etc.	The Solution can provide Server health status and security alarms for TCP SYN attacks, DoS attacks, etc. Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
111	ANNEXURE II Technical Specifications WAF Product / OEM Evaluation Criteria Clause No 1 of page No 33	WAF / WAF’s Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of India.	WAF / WAF’s Operating System should be tested and certified for EAL 2 /ICES-003/ NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of India. We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
112	ANNEXURE II Technical Specifications WAF Product / OEM Evaluation Criteria Clause No 2 of page No 33	The WAF solution should be in the Gartner's Magic Quadrant of Latest published Gartner Report “Web Application and API Protection”	The WAF solution should be in the Gartner's Magic Quadrant of Latest published Gartner Report or ICSA lab Certified. We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
113	ANNEXURE II Technical Specifications WAF High Availability Clause No 1 of page No 33	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active using standard VRRP (No Proprietary Protocol). We would like to Request the Honourable tendering committee to amend the clause	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
114	ANNEXURE II Technical Specifications WAF High Availability Clause No 2 of page No 33	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices with SSL session mirroring.	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices. Different OEM has different approach to achieve similar functions. So, We would like to Request the Honourable tendering committee to amend the clause as	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.

115	ANNEXURE II/ 3/Page -20	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or IPS or any StateFul Appliance). It is always recommended to have a dedicated DDOS stateless solution as the statfull devices like FW,ADC, IPS are succeptable to state exaustion attacks. which is very known DDOS attack and can be only taken care with a dedicated purpose built stateless DDOS device. As IPS is missing in the statement where IPS are layer 2 devices which works on signatures and are placed post DDOS as DDOS is the extreme perimeter device to protect the whole infra of DC including IPS,FW from all	Stateless hardware has already been asked to address DDoS attack. No change in clause. This is minimum technical requirement.

116	ANNEXURE II/ 4/Page -20	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Mitigation Throughput: 20Gbps Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) scalable to 35 mpps This mitigation throughput does not make any sense in this case. This should be removed. Legitimate throughput handling: 2Gbps from day-1 and scalable upto 20Gbps Inspection Ports: 4 x 10 SFP+ and 4 x 1G SFP supporting internal bypass for sofware and hardware failure on all the inspection interfaces to achieve faster network convergence in High Availability/Resilient Deployment In terms of asked thropughpt scalability mpps scalability should be available with the appliance to avoid any future replacement of appliance for upgrade purposes. This should be given either as scalable or from day 1 Beyond 2Gbps Attack On prem device will not work whatever be it's capacity. To protect from any size of attack, ISP clean pipe (cloud DDoS protection) is must along with on prem device. With this customer should not worry about size of attack. Attack size cant be defined. We do not mention the mitigation size as the practicality is legitimate throughput irrespective of the attack size. As asked 2 Gbps of clean traffic always will be given back protecting 20 or 40 gbps of attack size	Bypass is only relevant in case of single appliance requirement whereas here appliance has been asekd in HA. Bypass feature will bypass the traffic throught same appliance if it fails which will create security hole despite another HA appliance is still working in the network. Mitigation thoughput is asked to mitigate Attack traffic as appliance is asked with 10G port, attack traffic till 10G can easily come via each 10G connectivity. No change in clause. This is minimum technical requirement. Bidders may provide better options accordingly.

117	ANNEXURE II/ 6/Page -20	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms and stateless solution to detect and defend against threats at L3-7.	BEHAVIORAL ANALYSIS using behavioral algorithms/challange-response/http authentication to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms/challange response/http authentication and stateless solution to detect and defend against threats at L3-7. OEM specific language as every oem has its own way of preventing the attacks. OEM specific language as every oem has its own way of preventing the attacks.	The asked requirement is minimum, vendor can quote accordingly. No Change, As per the RFP
118	ANNEXURE II/ 7/Page -20	Behavioral DoS (Behavioral Denial of Service) Protection should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection should include: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood	Behavioral DoS (Behavioral Denial of Service) Protection/challenge response/http auth should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. OEM specific language as every oem has its own way of preventing the attacks.	DDoS appliance should be capable enough to address all kinds of attack including TCP, UDP, ICMP and IGMP. No change in clause. This is minimum technical requirement.
119	ANNEXURE II/ 9/Page -21	Positive Security Model should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic	Positive Security Model should have advanced behavior-analysis/challenge response/http authentication technologies to separate malicious threats from legitimate traffic OEM specific language as every oem has its own way of preventing the attacks.	Accepted Clause can be read as "Positive Security Model should have advanced behavior-analysis/challenge response/http authentication technologies to separate malicious threats from

120	ANNEXURE II/ 13/Page -21	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures apart from custom Signatures from Day 1.	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures/IOCs apart from custom Signatures from Day 1. DDOS solutions works on the IOCs where signature are part of IPS/FW devices. We being the global leader in DDOS do specific research on the DDOS IOCs which are not limited to 5k but are approx 1 million. This point is related to IPS. Anways the same has been asked in both Internal and Perimeter firewall. This point is favoring	Sufficient number of signature is very important to address known attacks. The asked deployment mode is minimum requirement. Clause Amended. Clause can be read as "System should support In-Line/Bridge, SPAN Port/TAP Mode, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures apart from custom
121	ANNEXURE II/ 16/Page -21	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection	The appliance should have the capability to create multiple security protection profile groups to protect different type of server types by creating different granular countermeasures for them. OEM specific names, however it should have the granularity to create different groups of servers like ftp, dns , web for their specific thresholds etc	This clasue to be read as solution must provide proetection against following types of attacks: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection There are different kinds of attacks which falls under DDoS attack, in order to mitigate these attacks vendor should have dedicated security engines. This is minimum technical requirement. Bidders may provide
122	ANNEXURE II/ 20/Page -21	The solution should provide Geo-Location blocking, Active Attacker Feeds and Signature Update Service from day-1	DDOS solutions works on the IOCs where signature r are part of IPS/FW devices. We being the global leader in DDOS do specific research on the DDOS IOCs which are not limited to 5k but are approx 1 million.	No change in clause. This is minimum technical requirement. Bidders may provide better options accordingly.

123	ANNEXURE II/ 21/Page -22	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	The solution should support Integration with cleanpipe service of atleast 2 ISPs in India and OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks where DDOS appliance should support cloud singalling to singal upstream ISP to start the mitigation in case	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
124	Missing Important Clause	Pls add the clause as " Supports over 3 Million IOC Blocking via integration with 3rd Party TIP"	next gen DDOS supports protection to the first entry to the organization and the last exit for the internal network. Where it should support millions IOCs via third party platforms integrations for the most effective security framwork and protection. CERT-IN too provides IOCs for the same purposes where that integration should be supported by all the security	As per the RFP
125	Missing Important Clause	Pls add the clause as " The proposed system must support automatic cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation."	It is important for organization to have Automatic Cloud Signaling between On-Premise and Cloud Scrubbing Service. In this context organization should have flexibility to choose from maximum possible ISP that support Automatic Cloud Signaling with On-Premise appliance rather than be restricted to few ISP/MSSP	As per the RFP
126	Missing Important Clause	Pls add the clause as " OEM Anti-DDoS Solution should be deployed and used by at least 4 Tier 1 (class A) Internet service providers (ISPs) in India to protect their own Core infrastructure from DDoS attacks"	as the bandwidth is provided by the ISPs where scrubbing should be possible at the ISP front which are Teir 1 ISPs in India to have the volumetric layer 4 attacks at their level itself. It is always recommended to have clean pipe from ISP and on prem devices to block the attacks upto layer 7.	As per the RFP
127	Missing Important Clause	Please add the clause as " System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability .	STIX/TAXII are open standards to get the feeds for more richness of security devices and is openly supported by the security OEMs. This is a must to have function for any security device and is also supported by CERT-IN for providing their IOCs/Feeds which can be automatically ingested using	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

128	For future Use: The solution	For future Use: The solution should support Integration with OEM own cloud/Integration with Third Party based Scrubbing Centers in case of Bandwidth Saturation attacks.	Every OEM might not have their own scrubbing centers but they have integration/joint venture model with third party and provide more strength in mitigating the attacks as compared to	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
129	Bidder should propose Separate Centralized Management & Reporting Solution from Day 1.	Bidder should propose Centralized Management/local Web UI to manage the appliance & additional Reporting Solution from Day 1.	Local WebUI option must be provided as this is more easy option to manage.	Tender clause is to be read as follows : "The WAF appliance should have GUI and CLI access for
130		System should support horizontal and vertical port scanning behavioral protection.	This point is related to IPS. Anways the same has been asked in both Internal and Perimeter firewall. This point is favoring particular as they provide IPS in their DDOS	This clause to be read as: System should support horizontal and vertical port scanning behavioural protection or System should protect against port scanning of vulnerable services on a system, and mitigate DoS attacks.
131	Technical Specification for WAF , Page 22 , Serial Number 1	Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security with integrated functionalities of Application Load Balancer and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not	Since the ask in the RFP is of a WAF we request you to modify the cluase to - Proposed hardware platform should be of high performance, highly scalable, and purpose-built Web Application Firewall. Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
132	Technical Specification for WAF , Page 22 , Serial Number 4	The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be complete in all respect. 10gig interface should be upgradeable to 25Gig by changing transceivers only.	The modules present in WAF is fixed. Upgradeable modules are vendor spcific. Hence we reqeust yout to modify the clause to - The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be complete in all respect. Please remove the clause of 25G Ports as you have already	Accepted: This clause to be read as "Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber."

133	Technical Specification for WAF , Page 22 , Serial Number 5	The Web Application Firewall shall have minimum 02 nos. 40Gig ports and at least 02 nos. 25Gig ports from day 01	We request you to remove this clause is this is specific to ADC vendors.Please remove the clause of 25G Ports as you have already asked for 40G Options in	Tender Clause Stands. Follow ammended clause 4.
134	Technical Specification for WAF , Page 22 , Serial Number 6	The Web Application Firewall shall have 4 x 10G : 2 x 25G: 2 x 40G Transceivers module/SFP populated from day 01	The Web Application Firewall shall have 4 x 10G SFP populated from Day 1. Please remove the clause of 25G Ports as you have already asked for 40G Options in	Tender Clause Stands. Follow ammended clause 4.
135	Technical Specification for WAF , Page 23 , Serial Number 9	The number of ports specified vide item no. 2, 3, 4, & 5 are excluding the physical ports required for High Availability Cluster.	Please update the port requirements as per the pre bid queries.	This clause can be read as "The number of ports specified vide item no. 4, 5 & 6 are excluding the physical ports required for High
136	Technical Specification for WAF , Page 23 , Serial Number 14	The Web Application Firewall shall support 19" Rack mounting with 1U form factor.	The Web Application Firewall shall support Rack mounting with 2U form factor.	Accepted. Tender clause is to be read as follows : "The Web Application Firewall shall support 19" Rack mounting with
137	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number 1	The Solution shall have minimum 40 Gbps L4-L7 throughput.	The ask is for a WAF but thr throughput that you have askjed for is L4/L7 throuput. We don't have L4/L7 throughtput. We only measure WAF throughput and thre is an big difference in WAF throughput vs L4/L7 throughput. We request you to modify the cluase to - The solution shall have a minimum WAF throughput of 2Gbps. If any OEM has L4/L7 throughput mentioned	Accepted Tender clause is to be read as follows : "The Solution shall have minimum 40 Gbps L4-L7 throughput or WAF throughput of 2Gbps"
138	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Web Application Firewall Solution shall have minimum 50 Million concurrent TCP connections.	Please remove this clause as this is applicalbe for ADC Specifications and not need for WAF.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional
139	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Web Application Firewall Solution shall have minimum 04 Lakh L4 TCP connections / second.	Please remove this clause as this is applicalbe for ADC Specifications and not need for WAF.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional
140	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Web Application Firewall Solution shall have minimum 10 Million HTTP request / second.	Please remove this clause as this is applicalbe for ADC Specifications and not need for WAF.	No change in clause. This is minimum technical requirement. Bidders may provide better

141	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number 5	The WAF shall support minimum 60,000 RSA and 30,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	The WAF shall support minimum 22,000 RSA OR 30,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
142	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Application Delivery Controller shall support minimum of 30 Gbps SSL throughput and hardware compression of	We request you to remove this clause as this is not needed for WAF. This is used for ADC.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional
143	Technical Specification for WAF , Page 24 , Solution Capabilities, Serial Number 9	The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration withautomation and CI/CD tools including	We request you to remove this clause as this is a vendor specific ask.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
144	Technical Specification for WAF , Page 24 , Solution Capabilities, Serial Number 10	Should support virtualization with its own hypervisor (NOT any third party or open source) that virtualizes the Device resources—including CPU, memory, management and configuration.The proposed device should have 8 Virtual	Since the ask is for a Hardware WAF, there is no reason to ask for virtualization. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
145	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 1	The Web Application Firewall shall have integration with REDHAT OpenShift Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from same make as WAF. It should not be third party or	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
146	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 2	The Controller/Container Plugin shall support both Nodeport and ClusterIP mode of deployment and also as an Ingress service.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

147	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 3	The Controller/Container Plugin shall support Application Delivery Controller orchestration to dynamically create and manage WAF objects.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
148	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 4	The Controller/Container Plugin shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
149	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 5	The Web Application Firewall shall be capable to forward traffic to container cluster via NodePort and ClusterIP.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
150	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 6	The Controller/Container Plugin shall support the configuration of advanced services like Web application firewalls through declarative syntax.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
151	Technical Specification for WAF , Page 25, Native and Kubernetes Integration Features, Serial Number 7	The Controller/Container Plugin shall support integration using latest Container network interface (CNI) for the container platform.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

152	Technical Specification for WAF , Page 25,, Native and Kubernetes Integration Features, Serial Number 8	The Web Application Firewall shall support NodePort mechanism for integration with kubernetes services.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
153	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 9	The Web Application Firewall shall support BGP for integration with kubernetes services.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
154	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 10	The Web Application Firewall shall support overlay network like VxLAN/Geneve for integration with kubernetes services	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
155	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 11	WAF should integrates with REDHAT Openshift container orchestration environments to dynamically create L4/L7 services on WAF, and load balance network traffic across the services. Monitoring the orchstration API server, Solution should be able to modify the WAF configuration based on changes made to containerized	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
156	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 12	Installation of Controller/Container Plugin should be using Operators on OpenShift Cluster and Helm charts.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

157	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 13	Controller/Container Plugin should use open shift route resources and support route annotations.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
158	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 14	Controller/Container Plugin should use multiple Virtual IP addresses	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
159	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 15	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should registers to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource Queue	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
160	Technical Specification for WAF , Page 25 ,Web Application Firewall Solution Functional Requirements , Serial Number 2	The Web Application Firewall Solution shall support the following Load Balancing Features: Support for 200 servers Support load balancing algorithms Least connection Ratio Round Robin	These are related to load balancing and not WAF. We request you to remove thise clause.	Tender Clause Stands.
161	Technical Specification for WAF , Page 29 , Web Application Firewall Functional Requirements , Serial Number 27	The proposed solution should have server stress based L7 Behavioural DOS detection and mitigation including the ability to create real time L7 DOS signatures.	This is a vendor specific ask. We request you to remove this.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

162	Technical Specification for WAF , Page 29 , Web Application Firewall Functional Requirements , Serial Number 27	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.	WAF inspects HTTP and HTTPS Traffic. We request you to modify the cluase to - The solution must protect against HTTP, HTTPS, and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks. Also can you please clarify what the is the feature that you are looking in Single Sign On.	FTP and SMTP are also L7 protocol which need to protect from attacks as these ports and protocols are open to outside world. Single sign on feature should be used, so that all internal users can access number of internal applications through one time username and password authentication. This feature is optional and should be
163	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 31	System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be	This is feature is not realted to WAF. This should be done by End Point Solutions We request you to remove thi clause as this is vendor specific.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
164	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 33	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the	This is a vendor specific ask. We request you to remove it.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
165	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 35	System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be	This is feature is not realted to WAF. This should be done by End Point Solutions We request you to remove thi clause as this is vendor specific.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

166	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 37	WAF should provide ability to enforce a given user to follow a sequences of pages while accessing	This is not a WAF feature. We request you to remove this as this a vendor specific ask.	No change in clause. This is minimum technical requirement. Bidders are free to quote similar features.
167	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 37	WAF should provide the application visibility and reporting with the below metrics and entity for each application: • Client IP addresses/subnets as well as geographical regions • Total Transactions as well as Average and Max Transactions/sec • Most commonly requested URLs • Server Latency and Page Load times • Virtual Server and Pool server performance • Page Load Time • Response code • OS and Browser • URL details		No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
168	Technical Specification for WAF , Page 32 , Users Access for Management ,	The Web Application Firewall shall generate alarms w.r.t. health status of Server/s, security alarms for TCP SYN attacks, DoS	These alarms are related to Load Balancer and ADC and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders may provide better

169	Technical Specification for WAF , Page 32 , Users Access for Management , Serial Number 8	The Web Application Firewall shall provide comprehensive reports (both real-time as well as Historical for at least 03 months) that can be customized as per requirement. Following are a few examples of the reports: Client side concurrent TCP connections per virtual server/application/URL. Client side new TCP connections per second per virtual server/application/URL. Server side concurrent TCP connections per server. Server side new TCP connections per second per server. Total Input as well as Output "Bytes per second" OR "Bits per second" per vserver/application/URL in order to have the usage of Internet Bandwidth. Total Input as well as Output "Bytes per second" OR "Bits per second" between the equipment and a particular Server. Server Uptime and downtime reports. CPU and Memory utilization of the equipment. Dozens of predefined Web application security reports such as session hijacking, non-valid XML structure, CCN leakage Reports detailing learned application resources Audit and access reports PCI compliance reports allow to drill down to relevant PCI DSS section providing system compliance information	Most of these reports are related to Load Balancer and ADC and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
170	Regulatory Compliance of each WAF device , Page 33 , Users Access for Management , Serial Number 1	The Web Application Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standards like IS-13252 (Part 1):2010 for Safety requirements of Information Technology Equipment.	These are vendor specific ceritficates. We request you to modify the clause to - The Web Application Firewall shall conform to CE or BIS or UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standards like IS-13252 (Part 1):2010 for Safety requirements of Information	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.

171	Regulatory Compliance of each WAF device , Page 33 , Users Access for Management , Serial Number 2	The Web Application Firewall shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standards like IS 6873(Part 7):2012 for EMC (Electro Magnetic Compatibility) requirements.	These are vendor specific ceritficates. We request you to modify the clause to - The Web Application Firewall shall conform to CE or BIS or EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standards like IS 6873(Part 7):2012 for EMC (Electro	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
172	Product / OEM Evaluation Criteria WAF device , Page 33 , Users Access for Management , Serial Number 1	WAF / WAF's Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions or under Indian Common Criteria Certification Scheme (IC3S) by STQC, MeitY, Govt. of	WAF / WAF's Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
173	Product / OEM Evaluation Criteria WAF device , Page 33 , Users Access for Management , Serial	The WAF solution should be in the Gartner's Magic Quadrant of Latest published Gartner Report "Web Application and API Protection"	Request you to remove this clause as no gartner report has been asked in DDoS specifications.	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
174	Page No. 20/ Point No. 4/ ANNEXURE II Technical Specification DDOS	Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP	Request you to please increase the ports and write it as Inspection Ports: 8 x 10 SFP+ and 8 x 1G SFP, the devices will be on HA and it has required min. 2 ports for connectivity and for feature expansion also.	No change in clause. This is minimum technical requirement. Bidders may provide better options accordingly.
175	Page No. 21/ Point No.15/ ANNEXURE II Technical Specification DDOS	The Proposed Solution should protect against Zero Day DDoS Attacks within few seconds, without any manual intervention.	Request you to please do the amendment and write it as "The Proposed Solution should protect against Zero Day DDoS Attacks in real time signature/footprint creation within 20 seconds, without any	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.

176	Page No. 21/ Point No.21/ ANNEXURE II Technical Specification DDOS	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	Request you to please do the amendment and write it as "For Future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks. OEM own scrubbing Centre should based in INDIA". Also OEM should have its own scrubbing centre in INDIA, it should not be from third party. It will help to keep baseline information in sync between appliance and scrubbing centre in INDIA only which will	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
177	Page No:20/Clause No: 3	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or IPS or any StateFul Appliance). IPS is missing out of this. IPS are layer 2 devices which works on signatures and should be from a different oem to have a multi layer security architecuture. Request	Stateless hardware has already been asked to address DDoS attack. No change in clause. This is minimum technical requirement.
178	Page No:20/Clause No: 4	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Mitigation Throughput: 20Gbps Legitimate throughput handling: 2Gbps from day-1 and scalable up to 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) scalable to 35 mpps In terms of asked thropughpt scalability mpps scalability should be available with the appliance to avoid any future replacement of appliance for upgrade purposes. This should be given either as scalable or from day 1	Bypass is only relevant in case of single appliance requirement whereas here appliance has been asekd in HA. Bypass feature will bypass the traffic throught same appliance if it fails which will create security hole despite another HA appliance is still working in the network. Mitigation thoughput is asked to mitigate Attack traffic as appliance is asked with 10G port, attack traffic till 10G can easily come via each 10G connectivity.

179		Mitigation Throughput: 20Gbps	request to remove this Attack size cant be defined. We do not mention the mitigation size as the practicality is legitimate throughput irrespective of the attack size. As asked 2 Gbps of clean traffic always will be given	As per the RFP
180		Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps	Legitimate throughput handling: 2Gbps from day-1 and scalable upto 20Gbps with web 3.0/4.0 the internet bandwidths will be going way high then the asked. 20 Gbps will be supporting a bandwidth of 10 Gbps in future which will be a normal scalability ask, Else the appliance replacement will be required. Request you	As per the RFP
181		Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP	Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP supporting internal bypass for sofware and hardware failure on all the inspection interfaces to achieve faster network convergence in High Availability/Resilient Deployment Being an inline layer 2 device in case any failure with the device occurs it should have capability to bypass the device to	No change in clause. This is minimum technical requirement. Bidders are free to add additional features.
182	Page No:20/Clause No: 6	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms and stateless solution to detect and defend against threats at L3-7.	BEHAVIORAL ANALYSIS using behavioral algorithms/challange-response/http authentication to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms/challange response/http authentication and stateless solution to detect and defend against threats at L3-7. OEM specific language as every oem has its own way of preventing the attacks.	The asked requirement is minimum, vendor can quote accordingly. No Change, As per the RFP

183	Page No:20/Clause No: 7	Behavioral DoS (Behavioral Denial of Service) Protection should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection should include: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood • ICMP flood	Behavioral DoS (Behavioral Denial of Service) Protection/challenge response/http auth should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. OEM specific language as every oem has its own way of preventing the attacks.	DDoS appliance should be capable enough to address all kinds of attack including TCP, UDP, ICMP and IGMP. No change in clause. This is minimum technical requirement.
184	Page No:21/Clause No: 9	Positive Security Model should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic	Positive Security Model should have advanced behavior-analysis/challenge response/http authentication technologies to separate malicious threats from legitimate traffic OEM specific language as every oem has its own way of preventing the attacks.	Accepted Clause can be read as "Positive Security Model should have advanced behavior-analysis/challenge response/http authentication technologies to separate malicious threats from
185	Page No:21/Clause No: 13	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures apart from custom Signatures from Day 1.	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures/IOCs apart from custom Signatures from Day 1. DDOS solutions works on the IOCs where signature r are part of IPS/FW devices. We being the global leader in DDOS do specific research on the DDOS IOCs which are not limited to 5k but are approx 1 million.	Sufficient number of signature is very important to address known attacks. The asked deployment mode is minimum requirement. Clause Amended. Clause can be read as "System should support In-Line/Bridge, SPAN Port/TAP Mode, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt

186	Page No:21/Clause No: 16	The appliance should have below Security Protection Profiles: 1. BDOS Protection 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection	The appliance should have the capability to create multiple security protection profile groups to protect different type of server types by creating different granular countermeasures for them. OEM specific names, however it should have the granularity to create different groups of servers like ftp, dns , web for their specific thresholds etc	This clasue to be read as solution must provide proetection against following types of attacks: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection There are different kinds of attacks which falls under DDoS attack, in order to mitigate these attacks vendor should have dedicated security engines. This is minimum technical requirement. Bidders may provide
187	Page No:21/Clause No: 20	The solution should provide Geo-Location blocking, Active Attacker Feeds and Signature Update Service from day-1	The solution should provide Geo-Location blocking, Active Attacker Feeds and Signature/IOC Update Service from day-1 DDOS solutions works on the IOCs where signature r are part of IPS/FW devices. We being the global leader in DDOS do specific research on the DDOS IOCs which are not limited to 5k but are approx 1 million.	No change in clause. This is minimum technical requirement. Bidders may provide better options accordingly.

188	Page No:21/Clause No: 21	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	The solution should support Integration with cleanpipe service of atleast 4 ISPs in India and OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks where DDOS appliance should support cloud singalling to singal upstream ISP to start the mitigation in case of saturation attacks. cloud based is not a practical solution as that requires customer to own their /24 subnet from ISP along with the BGP AS to route the traffic to any cloud in case of an attack. Customers use cleanpipe service where this routing is not required and in case of attack is seen by the on prem ddos it sends the singal back to the ISP cleanpipe for starting the mitigation. This should be available from day 1 as that is	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
189	Missing Important Clause	Missing Important Clause	Pls add the clause as " Supports over 3 Million IOC Blocking via integration with 3rd Party TIP" next gen DDOS supports protection to the first entry to the organization and the last exit for the internal network. Where it should support millions IOCs via third party platforms integrations for the most effective security framwork and protection. CERT-IN too provides IOCs for the same purposes where that integration	As per the RFP

190	Missing Important Clause	Missing Important Clause	Pls add the clause as " The proposed system must support automatic cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation." It is important for organization to have Automatic Cloud Signaling between On-Premise and Cloud Scrubbing Service. In this context organization should have flexibility to choose from maximum possible ISP that support Automatic Cloud Signaling with On-Premise appliance rather	As per the RFP
191	Missing Important Clause	Missing Important Clause	Pls add the clause as " OEM Anti-DDoS Solution should be deployed and used by at least 4 Tier 1 (class A) Internet service providers (ISPs) in India to protect their own Core infrastructure from DDoS attacks" as the bandwidth is provided by the ISPs where scrubbing should be possible at the ISP front which are Teir 1 ISPs in India to have the volumetric layer 4 attacks at their level itself. It is always recommended to have clean pipe from ISP and on prem	As per the RFP
192	Missing Important Clause	Missing Important Clause	Please add the clause as " System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability . STIX/TAXII are open standards to get the feeds for more richness of security devices and is openly supported by the security OEMs. This is a must to have function for any security device and is also supported by CERT-IN for providing their IOCs/Feeds which can be automatically ingested using	As per the RFP

193	1.3. Calendar of Events	Last date and time of receipt of Bids: 30.10.20	In view of the upcoming Dussehra holidays and the size & complexity of the requirement we would request TPCODL to kindly extend the bid submission date to	CCG need to response
194	1.7 Qualification Criteria	3) The bidder should have executed similar works (DDOS / WAF) for Supply, installation, Testing & commissioning for a single order value of Rs. 3 Cr. or Rs. 5 Cr. for cumulative 2 orders or for Rs.10 Crore for cumulative 5 orders each during the last 3 years. Copy of work order / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL / TPCODL / TPNODL / TPSODL / TPWODL for supply of similar product, performance feedback of the same will be solely	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request TPCODL to kindly consider the relevant project experience of both the Parent Company and the Subsidiary Company (Bidder) for Qualification Criteria compliance.	Accepted but in such cases all relevent documets must be furnished during BID submission.
195	7.1. Special Conditions of Contract	Delivery period shall be 60 days from date of	Currently the IT industry is facing multiple challenges such as shortage of micro-processor chips, international conflicts, disruption of supply chain etc. due to which there is a world wide crisis of availability of IT equipment. In view of the above, we would request TPCODL to kindly extend the delivery timeline to 180 days from date of receipt	As per the RFP
196	7.1. Special Conditions of Contract	Delivery location: as mentioned in price sched	Please provide the complete address of all the locations where the appliances has to be supplied & implemented.	At TP Odisha Discoms' DC & DR Locations (BBSR/Berhampur/Sambalpur/Bale
197	7.1. Special Conditions of Contract	Late delivery(LD) clause will be applicable as p	We would request TPCODL to kindly introduce a overall cap of the penalty charges. Please confirm that the cumulative maximum penalty charges for the project will be a maximum of 5% of the contract value of the undelivered part of the ordered solution.	It will be applicable as per GCC - respective Odisha Discom. LD Clause is celarly mentioned in GCC parts for respective discoms.

198	ANNEXURE VII SCOPE OF WORK / SERVICE LEVEL AGREEMENT	7. Delivery Time: The devices should be delivered within 6-8 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (Client will intimate date to bidder for installation of equipment's).	Currently the IT industry is facing multiple challenges such as shortage of micro-processor chips, international conflicts, disruption of supply chain etc. due to which there is a world wide crisis of availability of IT equipment. In view of the above, we would request TPCODL to kindly extend the delivery	As per the RFP
199	ANNEXURE VII SCOPE OF WORK / SERVICE LEVEL AGREEMENT	Incase uptime commitment of device (as men	We would request TPCODL to kindly introduce an overall cap of the penalty charges. Please confirm that the cumulative maximum penalty charges for the project will be a maximum of 5% of the contract value.	Subject to maximum 10% of the total contract value.
200	ANNEXURE VII SCOPE OF WORK / SERVICE LEVEL AGREEMENT	SLA Timelines Configuration / Call Response Time: 2 Hours response time. Resolution Time: 4 hours from the time of call registration.	In view of the complexity of the project we would request TPCODL to kindly amend the call response & call resolution SLA as requested herewith: SLA Timelines Configuration / Call Response Time: 4 Hours response time. Resolution Time: 8 hours from the time of call	As per the RFP
201	17. DDoS	System should protect from DDoS attacks beh	Please provide the details of the existing CD	CDN details will be shared during project implementation. DDOS should support both L2 and L3
202	3. Scope of Work	e) Complete configuration of the device to int	Please provide the details of the existing network architecture.	We will share the existing network architecture during project implementation. DDOS should support both L2 and L3 mode
203	3. Scope of Work	h) Provide Hands on Training to TP Odisha dis	Kindly confirm that Training will be in single batch. Also, confirm the training location i.e. Bidder or TPCODL office premise.	Training will be conducted in phases (a minimum of 02 batches). The training locations will either be in the TP Odisha Discom area or

204	3. Scope of Work	j)OEM Team/Engineer should do the impleme	We would request TPCODL to kindly amend the clause as suggested below: "OEM Team/Engineer or OEM certified partner should do the implementation services at site (TPSODL / TPCODL /	As per the RFP
205	3. Scope of Work	K) Supply and installation of necessary cables , accessories (Power cord for Indian standard, cable tie etc..)(Optical patch card/Cat6) & SFP for interconnecting to Firewall / Router / Servers / Leaf switches / Management switches with sufficient quantity. Quantity	Please provide the details of the existing network architecture and device type which are required to be integrated with DDoS and WAF solution.	Bidder will visit and survey for required accessories post award of the order.
206	4. Maintenance Services	TP Odisha discoms will allow vendor to carry out required Preventive Maintenance of the device. The down time required for Preventive Maintenance will be included in total down time of system to calculate quarterly uptime and communicated to TP	We would request TPCODL not to consider Preventive Maintenance down time for SLA calculation as it comes under planned downtime. Please confirm the acceptance of our	Accepted
207	5. Spares Availability/ Suppo	Access to OEM Diagnostic Solutions Database	Kindly elaborate this clause as we log call with OEM for any support during the	OEM Support portal access and all the fault ticket update should
208	7. Delivery Time	The devices should be delivered within 6-8 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (Client will intimate date to	Please let us know what will be the tentative time gap between devices delivery and intimation of the date for installation of equipment.	As per RFP
209	9. Level of specialist assistan	The vendor will ensure that all required specialist /Technical Support will be provided to his engineer so that the	Kindly confirm if onsite manpower support	It depends upon the bidder to maintain the RFP SLA
210	10 of 40	The bids will be evaluated commercially on an individual item basis (all-inclusive lowest cost at itemlevel) for the complete tender as calculated in Schedule of Items[Annexure I].	We Request you to Amend this Clause as" The Bidder can quote in Lot wise, & the bid will be evaluated commercially on Lot wise. Since DDOS and WAP are two different Operational Products and Process, also could be different OEM's , request for different Lot wise participation Either/or basis	The Clause will be amended as The Bidder should quote in Lot wise & the combination of the Lots will be as follows- Lot-1 :DDOS Lot-2: WAF 1. OEM should Submit Complainence & Unpriced BoQ on

211	General Query		Request for maximum 2 Bidders per OEM for more clarity and participation	It will be as per NIT. CCG always encourages maximum number of participations.
212	17 of 40	On delivery of the materials in good condition and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original in the name of respective Odisha discom to Invoice Desk. The payment shall be released within 45 days from the date of submission of error free certified bills/ invoices Any change in statutory taxes, duties and levies during the	Kindly amend as " 80% Payment shall be release within 45days against delivery and rest 20% will be released after complete installation, being MSME.	Payment terms will be as per NIT.
213	20 of 40	4. Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP	Kindly Amend this Clause as "Inspection Ports: 8 x 10 SFP+ and 8 x 1G SFP". Remark : As appliance will be installed in transparent mode, minimum two ports will be used for each connectivity i,e One for incoming and Another for outgoing. Appliance should have sufficient port to cater current as well as future requirements.	No change in clause. This is minimum technical requirement. Bidders are free to add additional features.
214	21 of 40	15. The Proposed Solution should protect against Zero Day DDoS Attacks within few seconds, without any manual intervention.	Kindly Amend this Clause as "The Proposed Solution should protect against Zero Day DDoS Attacks with real time signature/footprint creation within 20 seconds, without any manual intervention". Remark: Time must to be defined in order to effectively and faster block zero day	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.

215	21 of 40	21. For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	Kindly Amend this Clause as "For Future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks. OEM own scrubbing Centre should based in INDIA". Remark : OEM should have its own scrubbing centre in INDIA, it should not be from third party. It will help to keep baseline information in sync between appliance and scrubbing centre in INDIA	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
216	28 of 40	18. The Web Application Firewall Solution shall support server cloaking which hides error pages and application error	Kindly Delete. Remark :Server Cloaking is load balancer feature. Kindly remove for WAF OEM's to	No change in clause. This is minimum technical requirement.
217	29 of 40	27 The proposed WAF solution should protect from automated attacks on Web and mobile apps, and against bots that emulate human behavior	Kindly Amend this clause as " The proposed WAF solution should protect from automated attacks on Web or mobile apps, and against bots that emulate human behavior ". Remark: Kindly allow Web based protection for BOT traffic as mobile apps will need SDK integration which is not	No change in clause. This is minimum technical requirement.
218	30 of 40	31. System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user’s browsers. Necessary logs to be	Kindly Delete. Remark:Clause 31 and 35 is repeative. Kindly look in to it.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

219	33 of 40	The authentication between the management server & WAF shall be based on username, password & restricted to a specific IP address. In case software-based Management Server BL will provide requisite hardware or virtual machine as per software requirement.	Kindly Amend this Clause as ""The authentication between the management server & WAF shall be based on username, password & restricted to a specific IP address. In case software-based Management Server Tata power Odisha will provide requisite hardware or virtual machine as per software requirement". Remark:Please clarify who will provide required hardware/server, virtual machine	Accepted
220	Evaluation Criteria (Page 10 of 40)	The bids will be evaluated commercially on an individual item basis (all-inclusive lowest cost at itemlevel) for the complete tender as calculated in Schedule of Items[Annexure I].	Kindly Amend this Clause as "The Bidder shall be quote in Lot wise, & the over all bid will be evaluated commercially on Lot wise.	The Clause will be amended as The Bidder should quote in Lot wise & the combination of the Lots will be as follows- Lot-1 :DDOS Lot-2: WAF 1. OEM should Submit Complainence & Unpriced BoQ on their own Letter Head. 2. Maximum 2 nos. of Authorized Partner/Bidder per OEM can be
221	Technical Specification DDOS (Page 20 of 40)	Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP	As appliance will be installed in transparent mode, minimum two ports will be used for each connectivity i,e One for incoming and Another for outgoing. Appliance should have sufficient port to cater current as well as future requirements.	No change in clause. This is minimum technical requirement. Bidders are free to add additional features.

222	Technical Specification DDOS (Page 21 of 40)	The Proposed Solution should protect against Zero Day DDoS Attacks within few seconds, without any manual intervention.	Time must to be defined in order to effectively and faster block zero day attack with automatic footprint/siganture creation. Suggested Clause: The Proposed Solution should protect against Zero Day DDoS Attacks with real time signature/footprint creation within 20	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
223	Technical Specification DDOS (Page 21 of 40)	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	OEM should have its own scrubbing centre in INDIA, it should not be from third party. It will help to keep baseline information in sync between appliance and scrubbing centre in INDIA only which will further ensure the effective mitigation in case fo large DDoS attacks. Suggested Clause: For Future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks. OEM own	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
224	Technical Specification for Ddos , Page 20 , Serial Number 3	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).	The Proposed solution should be a Dedicated appliance (NOT a part of Router,UTM, Application Delivery Controller,Proxy based architecture or IPS or any StateFul Appliance). IPS is missing out of this. IPS are layer 2 devices which works on signatures and should be from a different oem to have a multi layer security architecuture. Request	Stateless hardware has already been asked to address DDoS attack. No change in clause. This is minimum technical requirement.

225	Technical Specification for Ddos , Page 20 , Serial Number 4	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Mitigation Throughput: 20Gbps Legitimate throughput handling: 2Gbps from day-1 and scalable up to 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) scalable to 35 mpps In terms of asked thropughpt scalability mpps scalability should be available with the appliance to avoid any future replacement of appliance for upgrade purposes. This should be given either as scalable or from day 1	Bypass is only relevant in case of single appliance requirement whereas here appliance has been asekd in HA. Bypass feature will bypass the traffic throught same appliance if it fails which will create security hole despite another HA appliance is still working in the network. Mitigation thoughput is asked to mitigate Attack traffic as appliance is asked with 10G port, attack traffic till 10G can easily come via each 10G connectivity.
226		Mitigation Throughput: 20Gbps	request to remove this Attack size cant be defined. We do not mention the mitigation size as the practicality is legitimate throughput irrespective of the attack size. As asked 2 Gbps of clean traffic always will be given	As per the RFP
227		Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps	Legitimate throughput handling: 2Gbps from day-1 and scalable upto 20Gbps with web 3.0/4.0 the internet bandwidths will be going way high then the asked. 20 Gbps will be supporting a bandwidth of 10 Gbps in future which will be a normal scalability ask, Else the appliance replacement will be required. Request you	As per the RFP
228		Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP	Inspection Ports: 4 x 10 SFP+ and 8 x 1G SFP supporting internal bypass for sofware and hardware failure on all the inspection interfaces to achieve faster network convergence in High Availability/Resilient Deployment Being an inline layer 2 device in case any failure with the device occurs it should have capability to bypass the device to	No change in clause. This is minimum technical requirement. Bidders are free to add additional features.

229	Technical Specification for Ddos , Page 20 , Serial Number6	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms and stateless solution to detect and defend against threats at L3-7.	BEHAVIORAL ANALYSIS using behavioral algorithms/challange-response/http authentication to defend against IoT botnet threats, including Mirai DNS Water Torture, Burst and Randomized attacks. The solution should utilize behavioral algorithms/challange response/http authentication and stateless solution to detect and defend against threats at L3-7. OEM specific language as every oem has its own way of preventing the attacks.	The asked requirement is minimum, vendor can quote accordingly. No Change, As per the RFP
230	Technical Specification for Ddos , Page 20 , Serial Number7	Behavioral DoS (Behavioral Denial of Service) Protection should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection should include: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood • ICMP flood	Behavioral DoS (Behavioral Denial of Service) Protection/challenge response/http auth should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. OEM specific language as every oem has its own way of preventing the attacks.	DDoS appliance should be capable enough to address all kinds of attack including TCP, UDP, ICMP and IGMP. No change in clause. This is minimum technical requirement.
231	Technical Specification for Ddos , Page 21 , Serial Number 9	Positive Security Model should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic	Positive Security Model should have advanced behavior-analysis/challenge response/http authentication technologies to separate malicious threats from legitimate traffic OEM specific language as every oem has its own way of preventing the attacks.	Accepted Clause can be read as "Positive Security Model should have advanced behavior-analysis/challenge response/http authentication technologies to separate malicious threats from

232	Technical Specification for Ddos , Page 21 , Serial Number 13	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures apart from custom Signatures from Day 1.	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt Signatures/IOCs apart from custom Signatures from Day 1. DDOS solutions works on the IOCs where signature r are part of IPS/FW devices. We being the global leader in DDOS do specific research on the DDOS IOCs which are not limited to 5k but are approx 1 million.	Sufficient number of signature is very important to address known attacks. The asked deployment mode is minimum requirement. Clause Amended. Clause can be read as "System should support In-Line/Bridge, SPAN Port/TAP Mode, Out-of-Path deployment modes from day 1. The proposed device should also support 5000+ inbuilt
233	Technical Specification for Ddos , Page 21 , Serial 16	The appliance should have below Security Protection Profiles: 1. BDOS Protection 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection	The appliance should have the capability to create multiple security protection profile groups to protect different type of server types by creating different granular countermeasures for them. OEM specific names, however it should have the granularity to create different groups of servers like ftp, dns , web for their specific thresholds etc	This clasue to be read as solution must provide proetection against following types of attacks: 1. BDoS Protection. 2. DNS Protections. 3. SYN-Flood Protection. 4. Traffic Filters. 5. Out-of-State Protection There are different kinds of attacks which falls under DDoS attack, in order to mitigate these attacks vendor should have dedicated security engines. This is minimum technical requirement. Bidders may provide
234	Technical Specification for Ddos , Page 21 , Serial 20	The solution should provide Geo-Location blocking, Active Attacker Feeds and Signature Update Service from day-1	The solution should provide Geo-Location blocking, Active Attacker Feeds and Signature/IOC Update Service from day-1 DDOS solutions works on the IOCs where signature r are part of IPS/FW devices. We being the global leader in DDOS do specific research on the DDOS IOCs which are not limited to 5k but are approx 1 million.	No change in clause. This is minimum technical requirement. Bidders may provide better options accordingly.

235	Technical Specification for Ddos , Page 22 , Serial 21	For future Use: The solution should support Integration with OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks.	The solution should support Integration with cleanpipe service of atleast 4 ISPs in India and OEM own Cloud based Scrubbing Centers in case of Bandwidth Saturation attacks where DDOS appliance should support cloud singalling to singal upstream ISP to start the mitigation in case of saturation attacks. cloud based is not a practical solution as that requires customer to own their /24 subnet from ISP along with the BGP AS to route the traffic to any cloud in case of an attack. Customers use cleanpipe service where this routing is not required and in case of attack is seen by the on prem ddos it sends the singal back to the ISP cleanpipe for starting the mitigation. This should be available from day 1 as that is	No change in clause. This is minimum technical requirement. Bidders are free to offer additional features.
236	Missing Important Clause		Pls add the clause as " Supports over 3 Million IOC Blocking via integration with 3rd Party TIP" next gen DDOS supports protection to the first entry to the organization and the last exit for the internal network. Where it should support millions IOCs via third party platforms integrations for the most effective security framwork and protection. CERT-IN too provides IOCs for the same purposes where that integration	As per the RFP

237	Missing Important Clause		Pls add the clause as " The proposed system must support automatic cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation." It is important for organization to have Automatic Cloud Signaling between On-Premise and Cloud Scrubbing Service. In this context organization should have flexibility to choose from maximum possible ISP that support Automatic Cloud Signaling with On-Premise appliance rather	As per the RFP
238	Missing Important Clause		Pls add the clause as " OEM Anti-DDoS Solution should be deployed and used by at least 4 Tier 1 (class A) Internet service providers (ISPs) in India to protect their own Core infrastructure from DDoS attacks" as the bandwidth is provided by the ISPs where scrubbing should be possible at the ISP front which are Teir 1 ISPs in India to have the volumetric layer 4 attacks at their level itself. It is always recommended to have clean pipe from ISP and on prem	As per the RFP
239	Missing Important Clause		Please add the clause as " System should have capability to consume and integrate with 3rd Party feeds (IOCs) via STIX/TAXII inbuilt integration capability . STIX/TAXII are open standards to get the feeds for more richness of security devices and is openly supported by the security OEMs. This is a must to have function for any security device and is also supported by CERT-IN for providing their IOCs/Feeds which can be automatically ingested using	As per the RFP
240	1.7 Qualification Criteria	OEM should have presence in INDIA for last 8 years. Company incorporation needs to be	Please clarify this clause is applicable for WAF & DDoS both OEMs or not.	Applicable for both OEMs.

241	1.7 Qualification Criteria	The bidder should have executed similar works (DDOS / WAF) for Supply, installation, Testing &	The bidder should have executed Cyber Security Project for cumulative 6 Crore INR during last 5 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer. Request you to kindly amend the clause for larger participation and fair	It will be as per NIT but complete of at least 1 Project of WAP / DDOS in DC Implementation environment should be present in previous work experience. **In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other**
242	Technical Specification for WAF , Page 22 , Serial Number 1	Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security with integrated functionalities of Application Load Balancer and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not	Since the ask in the RFP is of a WAF we request you to modify the cluase to - Proposed hardware platform should be of high performance, highly scalable, and purpose-built Web Application Firewall. Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
243	Technical Specification for WAF , Page 22 , Serial Number 4	The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be complete in all respect. 10gig interface should be upgradeable to 25Gig by changing transceivers only.	The modules present in WAF is fixed. Upgradeable modules are vendor spcific. Hence we reqeust yout to modify the clause to - The Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber. The hardware of all these ports should be	Accepted: This clause to be read as "Web Application Firewall shall have at least 04 nos. 10G base-X ports complying to IEEE 802.3ae standard which is able to drive the link up to 250 Meter at speed of 10 Gbps on Multi Mode fiber."
244	Technical Specification for WAF , Page 22 , Serial Number 5	The Web Application Firewall shall have minimum 02 nos. 40Gig ports and at least 02 nos. 25Gig ports from day 01	We request you to remove this clause is this is specific to ADC vendors	Tender Clause Stands. Follow ammended clause 4.

245	Technical Specification for WAF , Page 22 , Serial Number 6	The Web Application Firewall shall have 4 x 10G : 2 x 25G: 2 x 40G Transceivers module/SFP populated from day 01	The Web Application Firewall shall have 4 x 10G SFP populated from Day 1.	Tender Clause Stands. Follow ammended clause 4.
246	Technical Specification for WAF , Page 23 , Serial Number 9	The number of ports specified vide item no. 2, 3, 4, & 5 are excluding the physical ports required for High Availability Cluster.	Please update the port requirements as per the pre bid queries.	This clause can be read as "The number of ports specified vide item no. 4, 5 & 6 are excluding the physical ports required for High
247	Technical Specification for WAF , Page 23 , Serial Number 14	The Web Application Firewall shall support 19” Rack mounting with 1U form factor.	The Web Application Firewall shall support Rack mounting with 2U form factor.	Accepted. Tender clause is to be read as follows : "The Web Application Firewall shall support 19” Rack mounting with
248	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number 1	The Solution shall have minimum 40 Gbps L4-L7 throughput.	The solution shall have a minimum WAF throughput of 2Gbps. If any OEM has L4/L7 throughput mentioned then the L4/L7 throughput should be 40Gbps	Accepted Tender clause is to be read as follows : "The Solution shall have minimum 40 Gbps L4-L7 throughput or WAF
249	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Web Application Firewall Solution shall have minimum 50 Million concurrent TCP connections.	Please remove this clause as this is applicalbe for ADC Specifications and not need for WAF.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional
250	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Web Application Firewall Solution shall have minimum 04 Lakh L4 TCP connections / second.	Please remove this clause as this is applicalbe for ADC Specifications and not need for WAF.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional
251	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Web Application Firewall Solution shall have minimum 10 Million HTTP request / second.	Please remove this clause as this is applicalbe for ADC Specifications and not need for WAF.	No change in clause. This is minimum technical requirement. Bidders may provide better
252	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number 5	The WAF shall support minimum 60,000 RSA and 30,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	The WAF shall support minimum 22,000 RSA OR 30,000 ECC SSL transactions per second. SLL TPS rating specify the number of new SSL connections (Key exchanges) per second without session key reuse.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
253	Technical Specification for WAF , Page 23 , Solution Capabilities, Serial Number	The Application Delivery Controller shall support minimum of 30 Gbps SSL throughput and hardware compression of	We request you to remove this clause as this is not needed for WAF. This is used for ADC.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional

254	Technical Specification for WAF , Page 24 , Solution Capabilities, Serial Number 9	The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration withautomation and CI/CD tools including	We request you to remove this clause as this is a vendor specific ask.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
255	Technical Specification for WAF , Page 24 , Solution Capabilities, Serial Number 10	Should support virtualization with its own hypervisor (NOT any third party or open source) that virtualizes the Device resources—including CPU, memory, management and configuration.The proposed device should have 8 Virtual	Since the ask is for a Hardware WAF, there is no reason to ask for virtualization. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
256	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 1	The Web Application Firewall shall have integration with REDHAT OpenShift Kubernetes Platforms and requisite controller/license/container plugin shall be provided with WAF solution from day one. Controller/Plug-in should be from same make as WAF. It should not be third party or	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
257	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 2	The Controller/Container Plugin shall support both Nodeport and ClusterIP mode of deployment and also as an Ingress service.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
258	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 3	The Controller/Container Plugin shall support Application Delivery Controller orchestration to dynamically create and manage WAF objects.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
259	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 4	The Controller/Container Plugin shall support PER NAMESPACE operations with the capability to run Ingress service plugins on a PER NAMESPACE basis	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

260	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 5	The Web Application Firewall shall be capable to forward traffic to container cluster via NodePort and ClusterIP.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
261	Technical Specification for WAF , Page 24 , Native and Kubernetes Integration Features, Serial Number 6	The Controller/Container Plugin shall support the configuration of advanced services like Web application firewalls through declarative syntax.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
262	Technical Specification for WAF , Page 25, Native and Kubernetes Integration Features, Serial Number 7	The Controller/Container Plugin shall support integration using latest Container network interface (CNI) for the container platform.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
263	Technical Specification for WAF , Page 25,, Native and Kubernetes Integration Features, Serial Number 8	The Web Application Firewall shall support NodePort mechanism for integration with kubernetes services.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
264	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 9	The Web Application Firewall shall support BGP for integration with kubernetes services.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

265	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 10	The Web Application Firewall shall support overlay network like VxLAN/Geneve for integration with kubernetes services	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
266	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 11	WAF should integrates with REDHAT Openshift container orchestration environments to dynamically create L4/L7 services on WAF, and load balance network traffic across the services. Monitoring the orchstration API server, Solution should be able to modify the WAF configuration based on changes made to containerized	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
267	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 12	Installation of Controller/Container Plugin should be using Operators on OpenShift Cluster and Helm charts.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
268	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 13	Controller/Container Plugin should use open shift route resources and support route annotations.	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
269	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 14	Controller/Container Plugin should use multiple Virtual IP addresses	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.

270	Technical Specification for WAF , Page 25 , Native and Kubernetes Integration Features, Serial Number 15	Controller/Container Plugin should use Custom resources extensions of the Kubernetes API. It should registers to the Kubernetes client-go using informers to retrieve Virtual Server, TLSProfile, Service, Endpoint and Node create, update, and delete events. Resources identified from such events are pushed to a Resource Queue	These is a vendor specific clausse for container security and not related to WAF. We request you to remove this clause.	As per our solution requirement, It is imporatant for WAF Software integration with REDHAT openshift and Kubernetes platform. No change in clause. This is minimum technical requirement.
271	Technical Specification for WAF , Page 25 ,Web Application Firewall Solution Functional Requirements , Serial Number 2	The Web Application Firewall Solution shall support the following Load Balancing Features: Support for 200 servers Support load balancing algorithms Least connection Ratio Round Robin	These are related to load balancing and not WAF. We request you to remove thise clause.	Tender Clause Stands.
272	Technical Specification for WAF , Page 29 , Web Application Firewall Functional Requirements , Serial Number 27	The proposed solution should have server stress based L7 Behavioural DOS detection and mitigation including the ability to create real time L7 DOS signatures.	This is a vendor specific ask. We request you to remove this.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
273	Technical Specification for WAF , Page 29 , Web Application Firewall Functional Requirements , Serial Number 27	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.	WAF inspects HTTP and HTTPS Traffic. We request you to modify the cluase to - The solution must protect against HTTP, HTTPS, and Application layer Dos and DDOS attacks including stress based DOS and Heavy URL attacks. Also can you please clarify what the is the feature that you are looking in Single Sign On.	FTP and SMTP are also L7 protocol which need to protect from attacks as these ports and protocols are open to outside world. Single sign on feature should be used, so that all internal users can access number of internal applications through one time username and password authentication. This feature is optional and should be

274	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 31	System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be	This is feature is not realted to WAF. This should be done by End Point Solutions We request you to remove thi clause as this is vendor specific.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
275	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 33	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the	This is a vendor specific ask. We request you to remove it.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
276	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 35	System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be	This is feature is not realted to WAF. This should be done by End Point Solutions We request you to remove thi clause as this is vendor specific.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
277	Technical Specification for WAF , Page 30 , Web Application Firewall Functional Requirements , Serial Number 37	WAF should provide ability to enforce a given user to follow a sequences of pages while accessing	This is not a WAF feature. We request you to remove this as this a vendor specific ask.	No change in clause. This is minimum technical requirement. Bidders are free to quote similar features.

278	Technical Specification for WAF , Page 31 , Management and Reporting , Serial Number 5	WAF should provide the application visibility and reporting with the below metrics and entity for each application: • Client IP addresses/subnets as well as geographical regions • Total Transactions as well as Average and Max Transactions/sec • Most commonly requested URLs • Server Latency and Page Load times • Virtual Server and Pool server performance • Page Load Time • Response code • OS and Browser • URL details	Most of these reports are related to Load Balancer and ADC and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders may provide better solutions accordingly.
279	Technical Specification for WAF , Page 32 , Users Access for Management ,	The Web Application Firewall shall generate alarms w.r.t. health status of Server/s, security alarms for TCP SYN attacks, DoS	These alarms are related to Load Balancer and ADC and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders may provide better

280	Technical Specification for WAF , Page 32 , Users Access for Management , Serial Number 8	The Web Application Firewall shall provide comprehensive reports (both real-time as well as Historical for at least 03 months) that can be customized as per requirement. Following are a few examples of the reports: Client side concurrent TCP connections per virtual server/application/URL. Client side new TCP connections per second per virtual server/application/URL. Server side concurrent TCP connections per server. Server side new TCP connections per second per server. Total Input as well as Output "Bytes per second" OR "Bits per second" per vserver/application/URL in order to have the usage of Internet Bandwidth. Total Input as well as Output "Bytes per second" OR "Bits per second" between the equipment and a particular Server. Server Uptime and downtime reports. CPU and Memory utilization of the equipment. Dozens of predefined Web application security reports such as session hijacking, non-valid XML structure, CCN leakage Reports detailing learned application resources Audit and access reports PCI compliance reports allow to drill down to relevant PCI DSS section providing system	Most of these reports are related to Load Balancer and ADC and not related to WAF. We request you to remove this clause.	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
281	Regulatory Compliance of each WAF device, Point-1	The Web Application Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standards like IS-13252 (Part 1):2010 for Safety requirements of Information Technology Equipment.	These are vendor specific ceritficates. We request you to modify the clause to - The Web Application Firewall shall conform to CE or BIS or UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standards like IS-13252 (Part 1):2010 for Safety requirements of Information	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.

282	Regulatory Compliance of each WAF device, Point-2	The Web Application Firewall shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standards like IS 6873(Part 7):2012 for EMC (Electro Magnetic Compatibility) requirements.	These are vendor specific ceritficates. We request you to modify the clause to - The Web Application Firewall shall conform to CE or BIS or EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standards like IS 6873(Part 7):2012 for EMC (Electro	No change in clause. This is minimum technical requirement. Bidders are free to quote additional features.
283	NA	NA	As per RFP specs, we didn't find any Data Base Activity Monitoring points while we have seen that most of the power (North Bihar Power, UP Power, UK Power, MP Power) and all other SOC RFPs like NIC/NICSI etc. have asked for DAM solution as well. Database Activity Monitoring is a critical security measure that helps protect sensitive data, ensure regulatory compliance, and maintain the	As per the RFP
284	Reverse Auction Process	How many Bidders will be allowed ?		Number of bidders to be allowed in RA process shall be : Total No of bidders on whom tender would be split PLUS 2 more bidders Illustrative example: Total no of qualified bidders is 10 & tender needs to split amongst 4 bidders. PLUS 2 means (04 + 02 = 06) means lowest 6 bidders i.e., L1 to L6 bidders would be allowed in the RA process. Balance, H1 to H4 bidders would not be allowed in the RA
285	Splitting of Tender			Split criteria will be finalized later on, Splitting will be done minimum within two(2) Bas and it will be depending upon the total number of OEM/ BA participation, agremment with BA after RA and final negoiation, BA's turnover vs order issued on BA from TP odisha