MINUTES OF THE PRE-BID MEETING FOR "Web Application-Firewall" held on 29.01.2024 AT 03.30 P.M. THROUGH GOOGLE MEET
Ref: IITM/SPS/Web Application-Firewall 2023-24/23/SPL

An Open Tender was floated on 22.01.2024 for "Web Application –Firewall". The pre-bid meeting was held on 29.01.2024 (Monday) at 3.30 pm through Google Meet.

The representatives of the following 4 firms have participated in the pre-bid meeting, namely:

1. Mr. Vivek Gupta, **M/s. Prophaze**
2. Mr. Vishal Kondhalkar, **M/s.Vara Technologies**
3. Ms.Hema Bisht, **M/s.Halt Dos.Com Pvt.Ltd**
4. Mr.Vijay Babu, **M/s.Vertix**

The queries received from the prospective bidders were discussed by the Committee and clarified the same as tabulated below.

M/s F5 Networks

Sl. No.	Description	Tender Condition	Queries by the Bidders	Clarification	Recommended by the Committee
13.	**Pg. no.12**	"The solution should allow enforcing the following protocol related restrictions on the requests and these should be specifiable on an individual URL basis: a. HTTP method length b. Request line length c. URI length d. Query string length e. Protocol length f. Header name, value, and number g. Request body length h. Cookie name, value and number. i. Parameter name, value and number j. Max length (per file) and number for uploaded files (via POST)"	Upload of files should define the maximum length and hence "number for" to be removed.	Yes the upload files should define maximum length and hence "number for is not a major factor no issue if this paramter is not compiling	The Committee clarified that there is NO CHANGE in the tender condition
17	**Pg.No.13**	The solution should provide Volumetric DDOS protection for web assets of a network	Please clarify that this requirement is for L7 DDOS only.	Yes this is for L7 DDoS	The Committee clarified that there is NO CHANGE in the tender condition
55	**Pg.No.15**	The solution should support Centralized Management using a dedicated centralized management server or using a cloud Service	Full fledged management is buil-in to the same appliance and hence requesting to modify this clause for wider participation.	Cant be changed we need centralised management either through a management server or through a cloud service for easy access.	The Committee clarified that there is NO CHANGE in the tender condition

57	**Pg.No.15**	The solution should be able to offload user authentication from backend applications. It should be possible to specify custom login and logout pages for user authentication.	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition
58	**Pg.No.15**	The authentication module should be able to integrate with external authentication directories such as LDAP, Radius etc	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition

59	**Pg.No.15**	The solution should be able provide for two factor authentication mechanisms, e.g. using client SSL certificates and passwords or by integrating with RSA "SecurID".	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition
60	**Pg.No.16**	It should be possible to specify different authorization policies for different parts of the web sites, post authentication.	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition

61.	**Pg.No.16**	The solution should allow for single sign on across different protected web applications. The user once authenticated should be able to browse through different applications across single and multiple cookie domains without having to re-login.	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition
62.	**Pg.No.16**	It should be possible to track full user sessions (complete request and response bodies) and activity by a user id for auditing/troubleshooting purposes as required.	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition

63.	**Pg.No.16**	The solution should support authenticating user traffic using authentication mechanisms supporting SAML	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition
64.	**Pg.No.16**	The solution should support Single Sign on and Single Logout functionality for SAML authentication	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition

65.	**Pg.NO.16**	The solution should support authenticating user traffic using ADFS identity and access management	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition
66.	**Pg.No.16**	The solution should support authenticating user traffic using OKTA identity management	This feature is required only for VPN and as per industry best practise it is not recommended to have VPN built-in WAF Appliance and hence kindly remove this clause	This is not a intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic of users to web servers like allow access to specific links for an authenticated users and also restricting him to specific http methods only and many more attributes of customisation under the http request.	The Committee clarified that there is NO CHANGE in the tender condition

M/S. Halt Dos Com Pvt.,

Sl. No.	Description	Tender Condition	Queries by the Bidders	Clarified / Recommended by the Committee
1.	**Pg. no.12**	Proposed solution should have the support for ICSA Lab Certified WAF from day 1 on same appliance	As per the govt. guidelines, international certifications are not applicable for 'Make in India' companies. Kindly consider removing this clause in accordance with the specified notification.	The committee clarified to submit Indian Certification.

2.	**Pg.No.12**		Web applications that support file upload are left vulnerable if these files are not inspected against Sandboxing or AV scan. We recommend the addition of the following clause: Suggestive clause: The solution should enforce file upload restrictions based on file extension, file size and support scanning file against built-in AV scanning engine as well as have option to support external Sandboxing / AV engine.	The Committee clarified that there is NO CHANGE in the tender condition
3.	**Pg.No.13**		Bot attacks are one of the fastest growing attacks on web applications. Advanced bots are capable in solving captcha and can result in creating disruption to web applications. We recommend the addition of the following clause to provide protection against Bot attacks: Suggestive clause: The solution should have advanced Anti-Bot capabilities to detect and block advanced AI bots including deception capability to implant decoys (fake links and forms) in any application without any changes to application or client. In addition, the Anti-Bot should support Mobile SDK from same OEM to protect APIs and Mobile Apps from getting compromised.	The Committee clarified that there is NO CHANGE in the tender condition
4.	**Pg.No.14**		Company want to integrate the threat feed from other resources to protect the organsation and infra as well. We recommend to add the following clause in WAF. Suggestive Clause The proposed solution should have 3rd party threat feed integration to allow bulk IP blacklisting using API, FTP and schedule task etc.	The Committee clarified that there is NO CHANGE in the tender condition

M/S.Prophaze .,

Sl. No.	Description	Tender Condition	Queries by the Bidders	Clarified / Recommended by the Committee
1.		The firm should have an experience of supplying, installing, configuring, implementing and maintaining more than 200 websites out of which at least one should be in educational or Research Institute in India in the past 2 years.	This could be a challenge for us. However we have successfully deployed the on-premises WAF & DDoS solution for the Indian Manufacturing Company (Ramco) and we have the capacity to deploy the same solution through an appliance. We believe this experience qualifies us for participation and we kindly request your flexibility in considering our application.	Tender conditions prevails.

-sd-
Chairman
Tender Committee