## 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

Ref: II I M/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.

SI.	Descripti	M/s F5 Netwo Tender Condition	Queries by the	Clarification	Recommended
No.	on		Bidders	cial incation	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)"	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	requirement is for L7 DDOS only.		The Committee clarified that there is NO CHANGE in the tender condition
55	Pg.No.15	Centralized Management using a dedicated centralized management	Full fledged management is buil-in to the same appliance and hence requesting to modify this clause for wider participation.	we need	The Committee clarified that there is NO CHANGE in the tender condition

## M/s F5 Networks

57		The solution	should he	able to	This feature is	required or	<sup>y</sup> This is not a	The Committee
57	Pg.N0.15	offload user	suthenticat	ion from	for VPN and a	as per indust		
		user		ion nom	best practise	it is n	intranet vpn use	clarified that
		backend applic	ations. It s	should be	recommended	to have VI	N case. Offloading	there is NO
		possible to spec		-	hence kindly			CHANGE in the
		logout pages for	r user authe	entication.	clause	Tennove ti	Authentication	tender condition
							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.	
58	Pg.No.15	The authenticat	ion module	should be	This feature is	required or	<sup>y</sup> This is not a	The Committee
58	Pg.No.15	The authenticat able to integ	ion module grate with	should be external	This feature is for VPN and a	required or s per indust	y This is not a y intranet vpn use	The Committee clarified that
58	Pg.No.15	able to integ	grate with	external	for VPN and a	it is n	<sup>y</sup> intranet vpn use	
58	Pg.No.15	The authenticat able to integ authentication LDAP, Radius et	grate with directories	external such as	for VPN and a best practise recommended built-in WAF	it is n it is n to have VI Appliance a	<sup>y</sup> intranet vpn use N case. Offloading	clarified that
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI	<sup>y</sup> intranet vpn use N case. Offloading <sup>d</sup> User	clarified that there is NO
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF	it is n it is n to have VI Appliance a	y intranet vpn use n case. Offloading d User	clarified that there is NO CHANGE in the
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y intranet vpn use case. Offloading d User s Authentication	clarified that there is NO CHANGE in the
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y intranet vpn use case. Offloading d User s Authentication from server to	clarified that there is NO CHANGE in the
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y intranet vpn use case. Offloading d User s Authentication from server to WAF allows	clarified that there is NO CHANGE in the
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	<ul> <li>intranet vpn use</li> <li>case. Offloading</li> <li>User</li> <li>Authentication</li> <li>from server to</li> <li>WAF allows</li> <li>granular access</li> </ul>	clarified that there is NO CHANGE in the
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y intranet vpn use case. Offloading User s Authentication from server to WAF allows granular access control of	clarified that there is NO CHANGE in the
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y intranet vpn use case. Offloading User Authentication from server to WAF allows granular access control of http/https traffic	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y intranet vpn use case. Offloading d User Authentication from server to WAF allows granular access control of http/https traffic of users to web	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y 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	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y 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	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y 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	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	<ul> <li>intranet vpn use</li> <li>case. Offloading</li> <li>User</li> <li>Authentication</li> <li>from server to</li> <li>WAF allows</li> <li>granular access</li> <li>control of</li> <li>http/https traffic</li> <li>of users to web</li> <li>servers like allow</li> <li>access to specific</li> <li>links for an</li> <li>authenticated</li> </ul>	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	<ul> <li>intranet vpn use</li> <li>case. Offloading</li> <li>User</li> <li>Authentication</li> <li>from server to</li> <li>WAF allows</li> <li>granular access</li> <li>control of</li> <li>http/https traffic</li> <li>of users to web</li> <li>servers like allow</li> <li>access to specific</li> <li>links for an</li> <li>authenticated</li> <li>users and also</li> </ul>	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	<ul> <li>intranet vpn use</li> <li>case. Offloading</li> <li>User</li> <li>Authentication</li> <li>from server to</li> <li>WAF allows</li> <li>granular access</li> <li>control of</li> <li>http/https traffic</li> <li>of users to web</li> <li>servers like allow</li> <li>access to specific</li> <li>links for an</li> <li>authenticated</li> <li>users and also</li> <li>restricting him to</li> </ul>	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	<ul> <li>intranet vpn use</li> <li>case. Offloading</li> <li>User</li> <li>Authentication</li> <li>from server to</li> <li>WAF allows</li> <li>granular access</li> <li>control of</li> <li>http/https traffic</li> <li>of users to web</li> <li>servers like allow</li> <li>access to specific</li> <li>links for an</li> <li>authenticated</li> <li>users and also</li> <li>restricting him to</li> <li>specific http</li> </ul>	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y 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	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y 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	clarified that there is NO CHANGE in the tender condition
58	Pg.No.15	able to integ authentication	grate with directories	external such as	for VPN and a best practise recommended built-in WAF hence kindly	it is n it is n to have VI Appliance a	y 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	clarified that there is NO CHANGE in the tender condition

		The colution should be able arouid. This feature is required only my	
59	Pg.No.15	The solution should be able provide This feature is required only This is not a for VPN and as per industry	
		for two factor authentication for VPN and as per industry intranet vp	
		mechanisms, e.g. using client SSL recommended to have VPN case. Offloa	
		certificates and passwords or bybuilt-in WAF Appliance and User	CHANGE in the
		integrating with RSA "SecurID". hence kindly remove this Authenticat	tion tender condition
		from server	r to
		WAF allows	S
		granular ac	cess
		control of	
		http/https	traffic
		of users to	web
		servers like	allow
		access to sp	pecific
		links for an	
		authenticat	
		users and a	
		restricting	
		specific htt	
		methods or	
		and many r	
		attributes of	
		customisati	
		under the h	ittp
		request.	
60	Pg.No.16	5 It should be possible to specify This feature is required only This is not a	
		different authorization policies for the practise it is not intranet vp	
		different parts of the web sites, post recommended to have VPN case. Offloa	
		authentication. built-in WAF Appliance and User hence kindly remove this Authoritication	CHANGE in the
		clause	
		from server	
		WAF allows	
		granular ac	ccess
		control of	
		http/https	
		of users to	
		servers like	
		access to sp	
		links for an	
		authenticat	
		users and a	
		restricting	
		specific http://www.specific.com/action	
		methods or	
		and many r	
		attributes of	
		customisati	ion
		under the h	nttp

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

6.0	D N 44	The solution should si	support This feature is required onl		
63.	Pg.No.16			1 mo io noca	The Committee
		authenticating user traffic		t intranet vpn use	clarified that
			recommended to have vP		there is NO
		supporting SAML	built-in WAF Appliance an hence kindly remove thi		CHANGE in the
			clause	Authentication	tender condition
				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.	
( )	D= N= 16	The solution should support	Single This feature is required onl		The Committee
64.	Pg.No.16	Sign on and Single	Logout	17	The Committee clarified that
		functionality for	Dest Diacuse it is in	y *	there is NO
		authentication	SAML built-in WAF Appliance an	0	CHANGE in the
		authentication	hence kindly remove thi		tender condition
			clause	from server to	tender condition
				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	
				and many more attributes of	
				attributes of	

	D. NO.44	The solution	n should	cupport	This feature is	required	only	<b>m</b> 1 · · ·	<b>m c</b>
65.	Pg.NO.16	authenticating					ustry	This is not a	The Committee
					for VPN and a best practise	it is	not	intranet vpn use	clarified that
		ADFS ident	ity and	access	recommended	to nave		case. Offloading	there is NO
		management			built-in WAF hence kindly	remove	and this	User	CHANGE in the
					clause	Teniove	uns	Authentication	tender condition
								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.	
66.	Pg.No.16	The solutior		support	This feature is	required	only	This is not a	The Committee
		authenticating		c using	for VPN and a best practise	it is	not	intranet vpn use	clarified that
		OKTA identity r	nanagement		recommended			case. Offloading	there is NO
					built-in WAF			User	CHANGE in the
					hence kindly clause	remove	this	Authentication	tender condition
					ciuuse			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	
		1						users and also	
					1			restricting him to	
								specific http	
								methods only	
								methods only and many more	
								methods only and many more attributes of	
								methods only and many more attributes of customisation	
								methods only and many more attributes of	

## M/S. Halt Dos Com Pvt.,

SI. No.	Descripti on	Tender Condition	Queries by the Bidders	Clarified / Recommended by the Committee
1.		Proposed solution sh have the support for ICSA Lab Certified WAF day 1 on same appliance	IOUIdAs 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.	clarified to submit Indian

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.	Descripti on	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.	us. However we have successfully deployed the on-	Tender conditions prevails.

-sd-Chairman Tender Committee