INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY DELHI
(*A state university established by Govt. of NCT of Delhi*)
Okhla Industrial Estate, Phase III , New Delhi-110020, INDIA
Telephone: +91 11 26907400 Website: http://www.iiitd.ac.in

CORRIGENDUM -I

Tender No:- IIIT-D/IT/NGFW/017/2021-22 **Date: 27-10-2021**

Sub:-Corrigendum to Tender No:- IIIT-D/IT/NGFW/017/2021-22,dated:- 08-Oct-2021 for "Supply and installation of Next Generation Firewall".

Below are the amended requirements in the tender specification

Features	Amendment/New Requirement
Hardware I. The offered NGFW product should be supplied with at least 8x 1GE RJ-45 interfaces and 8x 10G SFP+ SR interfaces slot, 4x 40GE QSFP slot, 4x 1G SFP slot or if offered 10G SFP+ can work on 1Gbps then no need to offer separate 4x 1G SFP slots.8x10G SFP+ SR and 4x40GE QSFP+ SR transceiver should be provided and 4x 1G SFP optical transceivers should be provided if offered SFP+ transceivers can't work on 1Gbps.	**Hardware** I. The offered NGFW Solution should be supplied with at least 8x 1GE RJ-45 interfaces and 8x 10G SFP+ SR interfaces slot, 4x 40GE QSFP slot, 4x 1G SFP slot or if offered 10G SFP+ can work on 1Gbps then no need to offer separate 4x 1G SFP slots.8x10G SFP+ SR and 4x40GE QSFP+ SR transceiver should be provided and 4x 1G SFP optical transceivers should be provided if offered SFP+ transceivers can't work on 1Gbps.
Management/Monitoring, Logging, Reporting and Log Analyser:- xx. There must be support in NGFW and log analyser for multiple report formats, such as PDF, HTML, and CSV.	**Management/Monitoring, Logging, Reporting and Log Analyser:-** xx. There must be support in NGFW and log analyser for multiple report formats, such as PDF, and CSV.
Next Generation Firewall:- vi. Offered NGFW product must have inbuilt Capabilities to identify port-protocol based policies and convert the same into true application based policies. For example-Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/Rapid share etc.) traffic going through the same policy, then the firewall should automatically identify those risky applications and help to add more application specific security policies which might be using the same ports (80/443). This will help us to tighten the application flow control and reduce the attack surface area.	**Next Generation Firewall:-** Offered NGFW solution must have inbuilt Capabilities to identify applications and map them to respective ports **OR** Offered NGFW product must have inbuilt option for policy optimization to identify port-protocol and application based policies. For example-Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/Rapid share etc.) traffic going through the same policy, then the firewall should automatically identify those risky applications and reduce the attack surface area
URL/Webfilter,Content filter, Application filter:- Xi. The DNS filtering solution should	**URL/Webfilter,Content filter, Application filter:-** xi. The DNS filtering solution should have the following features:

have the following features: • Filters the DNS request based on the domain rating. • Should block the DNS request for the known botnet C&C domains. • Should allow to define own domain category. • Should support DNS safe search to enforce Google, Bing, and YouTube safe addresses for parental controls. • Should allow users to define own domain list to block or allow. • Should support DNS translation that can map the resolved result to another IP that user can define	• Filters the DNS request based on the domain rating. • Should block the DNS request for the known botnet C&C domains. • Should allow to define own domain category • Should allow users to define own domain list to block or allow. **Optional** • Should support DNS safe search to enforce Google, Bing, and YouTube safe addresses for parental controls. • Should support DNS translation that can map the resolved result to another IP that user can define
Zero Day threat protection :- i. Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware. Sand box analysis should be done for Windows family OS and applications, Mac OS and applications, Linux OS and applications, Android OS and applications, IOS and applications. ii. Offered Sandboxing Throughput should be (VM based) 100 files/Hr., Real-world Effective Throughput (Files/Hr.) 500, Number of VMs 6, It should provide option to customize VMs with our own Windows and Linux OS, applications.	**Zero Day threat protection :-** i. Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM- aware malware to detect and protect from virtual sandbox evading advance unknown malware. Sand box analysis should be done for Windows family OS and applications, Mac OS and applications, Linux OS and applications, Android OS and applications, IOS and applications or The emulation and zero-day inspection should be OS agnostic. ii. Offered Sandboxing Throughput should be (VM based) 100 files/Hr., Real-world Effective Throughput (Files/Hr.) 500,Number of VMs 6 , It should provide option to customize VMs with our own Windows and Linux OS, applications or The emulation and zero-day inspection should be OS agnostic.
Technical eligibility Offered NGFW Product by L1 bidder will be installed at IIITD campus for initial period of 3 months on evaluation basis. If IIITD finds the offered product's performance satisfactory then payment will be released. If there are major issues found or product not performing as per the technical specification	**Technical eligibility** Offered NGFW Product by L1 bidder will be installed at IIITD campus for initial period of 2 months on evaluation basis. If IIITD finds the offered product's performance satisfactory then payment will be released. If there are major issues found or product not performing as per the technical specification mentioned in the RFP then IIITD will cancel the order and will contact L2 bidder/OEM product for the same and so on.

mentioned in the RFP then IIITD will cancel the order and will contact L2 bidder/OEM product for the same and so on.	

The Last date for submission of Tender has been extended from **29th October 2021 to 8th November, 2021 till 03:00 P.M.**

Date for **Technical Bid opening** has been extended **29th October 2021 to 8th November, 2021 till 03:00 P.M.** For any technical queries bidders can email to bhawani@iiitd.ac.in and adarsh@iiitd.ac.in for any other clarification regarding the tender, the bidders are requested to contact our office through e-mail: ajay@iiitd.ac.in

All other terms and conditions remain the same.