INDRAPRASTHA GAS

Replies to pre bid queries against Tender no. IGL/ET2/CP/CM18824 for
PROCUREMENT OF NEXT-GENERATION OF FIREWALLS
& SUPPORTIVE INFRA WITH SOFTWARE SUBSCRIPTION, IMPLEMENTATION & PARTNER SUPPORT SERVICES

S.No.	Page No	Point No.	Section	Specification	Bidder Queries	Bidder Remarks	IGL Responses
1			Techincal Specification - I - PERIMETER FIREWALL General requirement Point#14	The Proposed NGFW product should support integration with standard Network Security Policy Management tools for future requirements. Declaration by OEM and supporting document to be submitted.	Kinldy specify the policy management tool for integartion support requested		Clarification: Currenly we are not using netwok security policy management tool, it is for future requirement. The NGFW should support for integration if required.
2			H. Zero-day Prevention/ Sandboxing Point#5	Sandboxing solution should be able INSPECT ENCRYPTED COMMUNICATIONS.	Sandbox solution does not do traffic inspection, it however do file alaysis. Hence request you to change this to " Sandboxing solution should be inspect files within encrpyted traffic using decryption by proposed solution"		Clarification: The Sandboxing solution should be able to inspect files for analysis within the encrypted traffic
3			F. URL Filtering Point#3	The Proposed NGFW should be able Guard against credential phishing.	Can you specify the requirement mentioned here		Clarification:- NGFW should be able to guard against credential phishing like advanced, inline, and automated capabilities that go beyond traditional port/protocol .
4			I. DNS Security Point#2	Solutions should be able Safeguard user privacy by encrypting DNS traffic and preventing third parties from intercepting or tracking DNS queries.	Can you specify if this requirement requires integration with DNS security while forwarding DNS traffic to DNS security solution? If Yes, can you specify DNS security solution in use		Clarification:- The soution should have the mentioned feature.
5			I. DNS Security Point# 5	Solutions should be able use digital signatures to verify the authenticity of DNS responses.	Kindly confirm whether DNSSEC validation is expected to be performed at the firewall level or via a centralized DNS resolver/DNS security service		Clarification:- Solutions should be able use digital signatures to verify the authenticity of DNS responses at Firewall level.
6			I. DNS Security Point# 8	Solutions should be able performs full inspection of DNS traffic to detect DNSbased application, volumetric, and anomaly attacks.	Please confirm whether DNS security capabilities are expected to be delivered solely via the on-premises NGFW, or if integration with external/cloud-based DNS security platforms is acceptable.		Clarification :- Solutions should be able performs full inspection of DNS traffic to detect DNSbased application, volumetric, and anomaly attacks at Firewall level.
7			B. Hardware, Interface & Performance Requirement Point#1	2 Nos in HA mode (DC) - NG Firewall appliance should have at least 12 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 2x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage, rack mountable etc.Firewall Throughput: minimum 30 GbpsNGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc.IPS throughput: Minimum 7 Gbps or higher real-worldApp control Throughput : Minimum 7 Gbps or higher real-worldThreat Protection throughput: Minimum 7 Gbps or higherConcurrent connections: Minimum 5 MillionNew sessions per second: Minimum 150000	The number of interface is not aligned with total throughput requirement. Request you to modify the clause to "2 Nos in HA mode (DC) - NG Firewall appliance should have at least 8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 8 x 1/10/25 Gigabit (SFP) Ethernet interfaces, with optional interface to support 4 x 40G,1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage, rack mountable etc.Firewall Throughput: minimum 30 GbpsNGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc.IPS throughput: Minimum 7 Gbps or higher real-worldApp control Throughput : Minimum 7 Gbps or higher real-worldThreat Protection throughput: Minimum 7 Gbps or higherConcurrent connections: Minimum 5 MillionNew sessions per second: Minimum 150000"		Tender Conditon Prevails
8			B. Hardware, Interface & Performance Requirement Point#2	03 nos (2- Kaka Nagar HA mode & 1- DR site SA mode) - NG Firewall appliance should have at least 8 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 4 Gbps or higher real-world App control Throughput : Minimum 4 Gbps or higher real-world Threat Protection throughput: Minimum 4 Gbps or higher concurrent connections: Minimum 3 Million New sessions per second: Minimum 100000	The number of interface is not aligned with total throughput requirement. Request you to modify the clause to "03 nos (2- Kaka Nagar HA mode & 1- DR site SA mode) - NG Firewall appliance should have at least 8 x 10M/100M/ 1GBASE-T Ethernet interfaces with (RJ- 45), 8 x 1/10 Gigabit (SFP) Ethernet interfaces with optional interface to support 8 x 1/10G & 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc.Firewall Throughput: minimum 25 GbpsNGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc.IPS throughput: Minimum 4 Gbps or higher real-worldApp control Throughput : Minimum 4 Gbps or higher real-worldThreat Protection throughput: Minimum 4 Gbps or higherconcurrent connections: Minimum 3 MillionNew sessions per second: Minimum 100000		Tender Conditon Prevails

9			B. Hardware, Interface & Performance Requirement Point#3	2 Nos in HA mode (2- IGL WTC office) - NG Firewall appliance should have at least 4 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc.Firewall Throughput: minimum 25 GbpsNGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc.IPS throughput: Minimum 3 Gbps or higher real-worldApp control Throughput : Minimum 3 Gbps or higher real-worldThreat Protection throughput: Minimum 3 Gbps or higherconcurrent connections: Minimum 2 MillionNew sessions per second: Minimum 100000	The number of interface is not aligned with total throughput requirement. Request you to modify the clause to "2 Nos in HA mode (2- IGL WTC office) - NG Firewall appliance should have at least 8 x 10M/100M/ 1GBASE-T Ethernet interfaces with (RJ- 45), 8 x 1/10 Gigabit (SFP) Ethernet interfaces with optional interface to support 8 x 1/10G & 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc.Firewall Throughput: minimum 25 GbpsNGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc.IPS throughput: Minimum 4 Gbps or higher real-worldApp control Throughput : Minimum 4 Gbps or higher real-worldThreat Protection throughput: Minimum 4 Gbps or higherconcurrent connections: Minimum 3 MillionNew sessions per second: Minimum 100000		Tender Conditon Prevails
10			B. Hardware, Interface & Performance Requirement Point#4	Firewall manager Qty. 01 - Centralized monitoring, management with sufficient number of interfaces , manage upto 10 firewall appliances. Firewall Analyzer Qty. 01 - Log analyzer appliance / high end server (min 16 core/ 64 Gb RAM) should have at least 2 TB storage with expansion options, minimum 10 GB logs per day capacity and sufficient number of interfaces.	Request to modify following clause as below to provide best solution as per requirement. Also specify number of daily samples required to be analysed. "Firewall manager Qty. 01 - Centralized monitoring, management with sufficient number of interfaces , manage upto 10 firewall appliances. Firewall Analyzer Qty. 01 - with sufficient number of interfaces, cpu and ram. "		
11			New Suggestion	Device should support Dual Redundant and Hot swappable (1+1) power supply	Dual Power Supply is Critical for Critical Infra but Only Dual Power Supply means nothing because if one supply goes bad, the devices either has to be shut down to replace the bad power supply or the device itself is replaced so in any case the down time is imminent, hence the ask has to be a hot swappable which allows for the bad part to be replaced while continuing operations.		Tender Condition Prevails
12			New Suggestion	Device memory should be minimum of 32 GB from day 1 with capability to expand to 64 GB in future in the same appliance.	With the ask full fledged threat portoection and Malware analytics it is very crucuial that we ask a committed amount of RAM , every Firewall OEM is able to supply this to ensure there are no performance issues.		Tender Condition Prevails
13	7			The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA.		The hardware delivery should be done within 08-10 weeks from the date of first notification of award/LOA.	Tender Condition Prevails
14	9			The bidder should have its own operational NOC/SOC during the last five years along with a support centre in India for 24*7 support.		Request to amend OEM/Bidder should have its own operational NOC/SOC during the last five years along with a support centre in India for 24*7 support.	Tender Condition Prevails

15	69		TECHNICAL SPECIFICATIONS I- PERIMETER FIREWALL's B. Hardware, Interface & Performance Requirement Point No 4	Firewall manager Qty. 01 - Centralized monitoring, management with sufficient number of interfaces , manage upto 10 firewall appliances. Firewall Analyzer Qty. 01 - Log analyzer appliance / high end server (min 16 core/ 64 Gb RAM) should have at least 2 TB storage with expansion options, minimum 10 GB logs per day capacity and sufficient number of interfaces. Bidders may propose higher configuration appliance / server also. The devices should be rack mountable.	For the firewall Manager/Analyzer reuired infra will be provided by IGL Team Or Bidder needs to address		Clarification :- Any hardware/software, component etc. required for the execution of this project to be supplied by the bidder only.
16	72		TECHNICAL SPECIFICATIONS I- PERIMETER FIREWALL's H. Zero-day Prevention/ Sandboxing Point No.4	The Sandboxing solution proposed by the OEM can be cloud based or appliance based solution. Cloud should be based in India if Cloud based sandboxing solutionis proposed by the OEM. Solution should be provided from day-1. The Communication to cloud based sandboxing solution should be over encrypted channel.	In case OEM sandbox cloud is not in India and sandboxing being a passive solution. The OEM ensures that the communication is encrypted via SSL with a 2048-bit BIOS-generated certificate. Objects will be discarded after certain time, once the analysis is completed. Majorly suspicious unkown files & URLs are sent for analysis and this does not share any customers known data files. Only logs/event will be stored for reporting.		Clarification: We have asked cloud based / appliance based sandboxing solution. In case the bidder is proposing cloud based solution, it should be in India due to data security issues. However, the point may be considered, bidder to provide undertaking from the proposed OEM that there will not be any data / file stored on sandbox cloud & will be released after analysis if found clean. Only logs/ event of malicious, unknown files will be stored for reporting purpose.
17	73		TECHNICAL SPECIFICATIONS I- PERIMETER FIREWALL's H. Zero-day Prevention/ Sandboxing Point No.8	In case OEM is proposing hardware based sandboxing solution then the hardware should be provided at DC with required network ports populated from day-1. The hardware should be rack mountable and should have redundant power supplies.	Sandboxing is a passive solution which is only scanning unknown Files or URLs sent by Firewall. Firewalls are the critical & primary solution to inspect the inline traffic in real time which already have redundant power supply. In case Sandbox solution is having single power supply will not impact any production because it is only sharing verdict to Firewalls to take necessary actions.		Clarification: Yes, the Sandboxing is passive component of the solution which scan the unknown & malicious files. There is no direct impact on Firewalls operation. The redundant supply is asked to minimize the downtime due to power supply failure. If the bidder supplied sandbox with single power supply, the device should be replaced in advancded RMA which is 6 CTR. Bidder to provide the undertaking from the respective OEM regarding the same.
18	69		TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's B. Hardware, Interface & Performance Requirement Point No 1	2 Nos in HA mode (DC) - NG Firewall appliance should have at least 12 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 2x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 30 Gbps NGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 7 Gbps or higher real-world App control Throughput : Minimum 7 Gbps or higher real-world Threat Protection throughput: Minimum 7 Gbps or higher Concurrent connections: Minimum 5 Million New sessions per second: Minimum 150000	We Request to please change the below parameters as IPS & NGFW throughput should be higher than Threat Prevention Throughput as per industry standard for optimal performance of the appliance and IGL Security controls NGFW throughput: Minimum 18 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 27 Gbps or higher real-world		Tender Conditon Prevails
19			TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's B. Hardware, Interface & Performance Requirement Point No 2	03 nos (2- Kaka Nagar HA mode & 1- DR site SA mode) - NG Firewall appliance should have at least 8 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 4 Gbps or higher real-world App control Throughput : Minimum 4 Gbps or higher real-world Threat Protection throughput: Minimum 4 Gbps or higher concurrent connections: Minimum 3 Million New sessions per second: Minimum 100000	We Request to please change the below parameters as IPS & NGFW throughput should be higher than Threat Prevention Throughput as per industry standard for optimal performance of the appliance and IGL Security controls NGFW throughput: Minimum 10 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 15 Gbps or higher real-world		Tender Conditon Prevails

20			TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's B. Hardware, Interface & Performance Requirement Point No 3	2 Nos in HA mode (2- IGL WTC office) - NG Firewall appliance should have at least 4 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 3 Gbps or higher real-world App control Throughput : Minimum 3 Gbps or higher real-world Threat Protection throughput: Minimum 3 Gbps or higher concurrent connections: Minimum 2 Million New sessions per second: Minimum 100000	We Request to please change the below parameters as IPS & NGFW throughput should be higher than Threat Prevention Throughput as per industry standard for optimal performance of the appliance and IGL Security controls NGFW throughput: Minimum 10 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 15 Gbps or higher real-world		Tender Conditon Prevails
21			TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's H. Zero-day Prevention/ Sandboxing Point No 7	Sandboxing solution should be to analyze 5000 files/day.	We request to please modify the below clause as below for optimal sizing of the solution:- Sandboxing solution should be to analyze 2000 files/day.		Tender Condition Prevails
22	9		SECTION I NOTICE FOR INVITATION FOR BIDS (IFB) PROCUREMENT OF NEXT-GENERATION OF FIREWALLS & SUPPORTIVE INFRA WITH SOFTWARE SUBSCRIPTION, IMPLEMENTATION & PARTNER SUPPORT SERVICES FOR A PERIOD OF 03 YEARS AT IGL TENDER DOCUMENT NO. IGL/ET2/CP/CM18754	The bidder/OEM should have its own operational NOC/SOC during the last five years along with a support centre in India for 24*7 support.	the bidder should have managed SOC past 3 years with 25000 EPS Minimum customer 3 in central/ PSU/ Cards/ Large enterprise		Tender Condition Prevails
23	7		SECTION I NOTICE FOR INVITATION FOR BIDS (IFB) Point No.3	Delivery Period : The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA.	Due to Global shortage of hardware of supply we request you to extend the hardware delivery from 04 weeks to 02 months		Tender Conditions Prevails

24			TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's J. Administration, Centralized Management and Logging Point No 4	The Management functions, Log server and Reporting server of the proposed NGFW can be inbuilt into the hardware appliance (to be supplied by the bidder). No Separate 3rd party hardware/solution shall be used for management, log server and reporting. All required licenses including OS, software components, databases etc. for running the solution have to be provided by the bidder for the entire duration of the project	We request to please modify this point as below to allow both Hardware appliance and software, as software deployment on Virtual machine or modular server provides expansion, scalability & failover capabilities for future use:- The Management functions, Log server and Reporting server of the proposed NGFW can be inbuilt into the hardware appliance or Software hosted on server with virtualization if required (to be supplied by the bidder). No Separate 3rd party solution/software shall be used for management, log server and reporting. All required licenses including OS, software components, databases etc. for running the solution have to be provided by the bidder for the entire duration of the project		Tender Conditions Prevails
25			TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's J. Administration, Centralized Management and Logging Point No 14	Centralized Management Solution must have option of creating multiple logical management administrator access (minimum 5 logical groups) to provide granular management control to respective administrators.	We request to kindly confirm, the requirment from this point is to have different administrator with different rights to manage features of firewall, or control/restriction on administartor to manage the specific firewall is required.		Clarification: The requirement is to have different administrator with differenet rights based on roles / profile like (super user, read only etc) to manage firewalls.
26			TECHNICAL SPECIFICATIONS II - INTERNAL FIREWALL B. Hardware, Interface & Performance Requirement Point No 1	2 Nos in HA mode (DC) - NG Firewall appliance should have at least 8 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 4x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage etc. Firewall Throughput: minimum 30 Gbps NGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 7 Gbps or higher real-world App control Throughput : Minimum 7 Gbps or higher real-world Threat Protection throughput: Minimum 7 Gbps or higher Concurrent connections: Minimum 5 Million New sessions per second: Minimum 150000 The OEM must publish performance claims on a public domain like websites, and datasheets. Letterhead performance claims signed by authorized signatory of the OEM can be accepted for the parameters, which are not mentioned in the product data sheet. Bidders may propose higher configuration appliance also. All interface modules to provided from day -1.	We Request to please change the below parameters as IPS & NGFW throughput should be higher than Threat Prevention Throughput as per industry standard for optimal performance of the appliance and IGL Security controls NGFW throughput: Minimum 18 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 27 Gbps or higher real-world		Tender Conditon Prevails
27			TECHNICAL SPECIFICATIONS II - EXTERNAL FIREWALL G. Firewall Manager/Analyzer Point No 4	Firewall manager Qty. 01 - Centralized monitoring, management with sufficient number of interfaces , manage upto 10 firewall appliances. Firewall Analyzer Qty. 01 - Log analyzer appliance / high end server (min 16 core/ 64 Gb RAM) should have at least 2 TB storage with expansion options, minimum 10 GB logs per day capacity and sufficient number of interfaces. Bidders may propose higher configuration appliance / server also. The devices should be rack mountable.	For the firewall Manager/Analyzer reuired infra will be provided by IGL Team Or Bidder needs to address		Clarification :- Any hardware/software required for the same should be supplied by the bidder only.
28	7	3	DURATION OF CONTRACT / DELIVERY PERIOD / INSTALLATION AND MIGRATION	Delivery Period : The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA. Installation and migration: Installation and migration should completed within 02 weeks after the delivery of hardware.	Request to please increase the delievery time to 8 weeks and implimentaion to 6 weeks as this is multi location deployment and delieveries are taking average 8-10 weeks for the high end devices asked in the RFP.		Tender Conditions Prevails

29	80		BUY BACK	Bidder to submit the quote for the buy-back of the old security appliances and supporting devices which shall be released /handover to bidder after successful installation and migration in "As is Where is" condition without any cables/connectors , accessories etc. Bidder to arrange for the pickup of the old equipment / appliance at its own cost from the respective location. The cost of the buy-back items shall be adjusted while release the purchase order to bidder. Bidder to decommission the old devices & ensure there is not any data stored on devices. The list of the buy-back items along with the location has been attached.	Request to please remove this clause as buyback favours the existing OEM and these equipments will not be of any use by bidders who wants to quote for the other competing OEM and will give commmerical benefit to the incumbent vendor.		Tender Conditions Prevails
30	69		Technical Specifications	B. Hardware, Interface & Performance Requirement_Perimeter Firewall 2 Nos in HA mode (DC) - NG Firewall appliance should have at least 12 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 2x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage, rack mountable etc.	IGL has specified the interface for respective locations, but for Bengaluru it isn't mentioned. Kindly confirm if it will be same for Bengaluru location as it is for DC?		Please refer page no. 69, point no.02 (B. Hardware, Interface & Performance Requirement)
31	80		SLA	Monthly minimum two onsite visit for preventive and health checkup.	24*7 comprehensive OEM support has been asked. Monthly 2 visits for health checkup would increase unnecessay cost to the IGL, hence we request to modify the clause as "**Yearly** minimum two onsite visit for preventive and health checkup."		Tender Condition Prevails
32	80		SLA	During the contract period if any site changed where equipment's installed, bidder to provide necessary support & services at new location(in India) without any additional cost including accommodation, food & transportation etc	In future, if any IGL site is changed, it will be the bidder's responsibility to support. 1. Please clarify that in such case, if bidder needs to perform complete installation, configuration, testing etc? 2. Also confirm how many times throughout the contract period, there is tentative possibility of site change? Replies against above 2 points would enable us to estimate resource efforts accordingly		Clarification :- If in case any site location changed, IGL shall transport the hardware to the new location. However, the bidder needs to send an engineer to the new location for installation and other support.
33	65		1.0 Scope of Work	The proposed solution shall provide advanced threat protection, improved performance, higher scalability, and seamless integration with the existing network and security ecosystem, ensuring secure, resilient, and uninterrupted service delivery to internal and external stakeholders.	We hereby request to provide inventory details available with IGL to ensure compatibility and integration.		Clarification :- Inventory details shall be provided to the L1 bidder
34	66		1.0 Scope of Work	Supply of Enterprise class next generation Firewall appliances (physical) with **migration** / installation, warranty, software subscription, and documentation etc.	It is understood that bidder has to perform migration of existing Fortinet firewalls from Data Center(IGL Bhawan), Kaka Nagar & DR site Bengaluru. Kindly confirm if our understanding is correct?		Clarification :- The bidder should provide support for the installation,migration of the services from existing firewall, warranty, software subscription, and documentation etc.
35	9		7.1 Technical BEC:	IV. The bidder should have its own operational NOC/SOC during the last five years along with a support centre in India for 24*7 support.	As per our understanding the project involves supply, installation and commissioning of NGFW and related H/W or S/W. Whereas, NOC/SOC is very broad term and comprises of several components related to Network Security, Data Security, App Security, Cloud Security, Theat Intelligence, GRC, VAPT etc. However, the requirement for bidder having their NOC/SOC is not directly relevant to the scope of this RFP and does not add value in assessing the bidder's capability for on-premise NGFW implementation. **In the interest of encouraging wider and more competitive participation, we kindly request that this clause be deleted from the evaluation criteria**		Tender Condition Prevails
36	67		Support services from bidder - 3 years	1. Bidder to deploy its skilled experienced resource on the supplied product & solution, on site at IGL HO for 6 months after the successful implementation for handholding support.	1. Kindly confirm number of resources required at IGL HO? 2. L1 or L2? 3. If any particular certitication is expected from the resource?		Clarification :- OEM certified L2 level resource is required for smooth transition and for troubleshooting the issues during the initial phase of the project.

37	7		DURATION OF CONTRACT / DELIVERY PERIOD / INSTALLATION AND MIGRATION	**Delivery Period** : The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA.	Considering global geopolitical tensions, delivery of hardware is impacted, hence we request to modify the delivery timeline as per below. "Delivery Period : The hardware delivery should be done within **10-12 weeks** from the date of first notification of award/LOA."		Tender Conditions Prevails
38	7		DURATION OF CONTRACT / DELIVERY PERIOD / INSTALLATION AND MIGRATION	**Installation and migration**: Installation and migration should completed within 02 weeks after the delivery of hardware.	Since migration is also part of complete installation activity, it is requested to modify the clause as below "Installation and migration should completed within **04** weeks after the delivery of hardware."		Tender Conditions Prevails
39	73		TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's J. Administration, Centralized Management and Logging Point No 4	The Management functions, Log server and Reporting server of the proposed NGFW can be inbuilt into the hardware appliance (to be supplied by the bidder). No Separate 3rd party hardware/solution shall be used for management, log server and reporting. All required licenses including OS, software components, databases etc. for running the solution have to be provided by the bidder for the entire duration of the project	We request to please modify this point as below to allow both Hardware appliance and software, as software deployment on Virtual machine or modular server provides expansion, scalability & failover capabilities for future use:- The Management functions, Log server and Reporting server of the proposed NGFW can be inbuilt into the hardware appliance or Software hosted on server with virtualization if required (to be supplied by the bidder). No Separate 3rd party solution/software shall be used for management, log server and reporting. All required licenses including OS, software components, databases etc. for running the solution have to be provided by the bidder for the entire duration of the project		Tender Condition Prevails
40	75		TECHNICAL SPECIFICATIONS II - INTERNAL FIREWALL B. Hardware, Interface & Performance Requirement Point No 1	2 Nos in HA mode (DC) - NG Firewall appliance should have at least 8 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 4x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage etc. Firewall Throughput: minimum 30 Gbps NGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 7 Gbps or higher real-world App control Throughput : Minimum 7 Gbps or higher real-world Threat Protection throughput: Minimum 7 Gbps or higher Concurrent connections: Minimum 5 Million New sessions per second: Minimum 150000 The OEM must publish performance claims on a public domain like websites, and datasheets. Letterhead performance claims signed by authorized signatory of the OEM can be accepted for the parameters, which are not mentioned in the product data sheet. Bidders may propose higher configuration appliance also. All interface modules to provided from day -1.	We Request to please change the below parameters as IPS & NGFW throughput should be higher than Threat Prevention Throughput as per industry standard for optimal performance of the appliance and IGL Security controls NGFW throughput: Minimum 18 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 27 Gbps or higher real-world		Tender condition prevails
41	77		TECHNICAL SPECIFICATIONS II - INTERNAL FIREWALL C. Next Generation Firewall (NGFW) Features Point No 17	There shall be no requirement for a separate firewall manager. The NGFW must have sufficient onboard disk space /storage to retain logs for a minimum of 180 days. If the firewall's storage is insufficient to meet this requirement, the bidder shall provide an OEM-supported cloud-based analyzer / appliance to ensure compliance as part of solution.	OEM restricting clause, hence we request to kindly modify this point as below :- Firewall offered shall be managed locally or via on premise central management. The NGFW must have sufficient onboard disk space /storage to retain logs for a minimum of 180 days. If the firewall's storage is insufficient to meet this requirement, the bidder shall provide an OEM-supported cloud-based analyzer / appliance to ensure compliance as part of solution.		Clarification: Since the internal firewalls are only 2 in qty. and in HA as well & can be managed locally, so no sepaerate firewall manager not required. We also have SOC services where we are collecting logs of devices, so the NGFW should have sufficent storage / disk space to retain logs foa a minimum of 180 days. If the firewall's storage is insufficient to meet this requirement, the bidder shall provide an OEM-supported cloud-based analyzer / appliance to ensure compliance as part of solution.

42	73		TECHNICAL SPECIFICATIONS I - PERIMETER FIREWALL's J. Administration, Centralized Management and Logging Point No 4	The Management functions, Log server and Reporting server of the proposed NGFW can be inbuilt into the hardware appliance (to be supplied by the bidder). No Separate 3rd party hardware/solution shall be used for management, log server and reporting. All required licenses including OS, software components, databases etc. for running the solution have to be provided by the bidder for the entire duration of the project	We request to please modify this point as below to allow both Hardware appliance and software, as software deployment on Virtual machine or modular server provides expansion, scalability & failover capabilities for future use:- The Management functions, Log server and Reporting server of the proposed NGFW can be inbuilt into the hardware appliance or Software hosted on server with virtualization if required (to be supplied by the bidder). No Separate 3rd party solution/software shall be used for management, log server and reporting. All required licenses including OS, software components, databases etc. for running the solution have to be provided by the bidder for the entire duration of the project		Tender Condition Prevails
43	78		TECHNICAL SPECIFICATIONS II - INTERNAL FIREWALL G. Zero-day Prevention/ Sandboxing Point No 7	Sandboxing solution should be to analyze 5000 files/day.	We request to please modify the below clause as below for optimal sizing of the solution:- Sandboxing solution should be to analyze 2000 files/day.		Tender Condition Prevails
44	7	3	1	**Delivery Period** : The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA.	**Delivery Period**: We Request you to extend delivery period from 04 Weeks to 08 Weeks rom the date of first notification of award/LOA.	After placement of the order to OEM/Disti, the minimum lead time required will be around 8 weeks to cover all activities such as order loading, logistics, transit, and other associated processes.Therefore, we request you to kindly extend the delivery timeline accordingly.	Tender Condition Prevails

45	7	3	1	Installation and migration: Installation and migration should completed within 02 weeks after the delivery of hardware	Installation and migration : Installation and migration should completed within 08 weeks after the delivery of hardware	Justification : After verification of the products, the installation and migration activities are critical and require detailed understanding of the existing site infrastructure and network environment. Since the migration activity involves careful planning and execution to avoid any service disruption, it will require adequate time for smooth implementation. Therefore, considering order loading, logistics, transit, installation, verification, and migration activities, a delivery and implementation timeline of 8 weeks would be appropriate.	Tender Condition Prevails
46	57	10	IV	Payment Terms : 1. Material a. Material delivery: 80% payment towards material delivery (hardware appliance) shall be released within 45 days of successful delivery, power on and verification of BOM. b. Material delivery: Balance 20 % payment towards material delivery (hardware appliance) shall be released within 45 days of successful installation & migration, documentation and on certification by engineer-in charge. 2. Licenses / software's Subscription 100% Payment towards software subscription / licenses shall be released within 45 days of installation & migration and on receiving of licenses certificate with relevant documents and certification by engineer-in charge. 3. Installation & migration: 100% Payment towards installation & migration shall be released within 45 days of successful completion of installation & migration activity and on certification by engineer-in charge. 4. Support services Payment towards support services from partner shall be released on half yearly basis on completion of six months and on certification by engineer-in charge. Payment towards support services shall be released within 45 days after the submission of invoices with relevant documents	Payment Terms : 1. Material a. Material delivery: 85% payment towards material delivery (hardware appliance) shall be released within 45 days of successful delivery, power on and verification of BOM. 4. Support services Payment towards support services from partner shall be released on Quarterly basis on completion of six months and on certification by engineer-in charge. Payment towards support services shall be released within 45 days after the submission of invoices with relevant documents	Since 100% payment needs to be released upfront to the OEM/Distributor, it will create a negative cash flow impact from our end.Therefore, we request you to kindly revise the payment terms to “Payment against Material Delivery” to maintain smooth financial execution of the project.	Tender Conditions Prevails

47	57	10	IV	Partial Payment Clause	Payment Against Parrtially Delivery	We would like to highlight that the current RFP does not mention provisions for partial delivery and partial payment, which are critical in a scenario involving multiple vendors and staggered deliveries. In complex procurements where items are supplied by different parties, enabling partial deliveries along with corresponding payments ensures smoother execution, better coordination, and timely fulfillment of project milestones. We therefore request you to kindly include a clause allowing partial delivery and partial payment in the RFP to reflect practical execution needs and	Tender Conditon Prevails
48	80	13	V	SLA(Support & maintenance) 365X24X7 telephonic and ticket support(TAC)	Not mentioned in RFP if any break down or inerupt in services who will raise Ticket either Bidder Or Customer.	Need clarification on the process for opening the service ticket. Please confirm whether the customer will directly raise the service ticket, or if an onsite Resident Engineer (RE) is required for initiating the same.	Please refer page no. 68, point no.16 (Support services from bidder - 3 years)

49	69	1	B	2 Nos in HA mode (DC) - NG Firewall appliance should have at least 12 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 2x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSDinternal storage, rack mountable etc. Firewall Throughput: minimum 30 Gbps NGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 7 Gbps or higher real-world App control Throughput : Minimum 7 Gbps or higher real-world Threat Protection throughput: Minimum 7 Gbps or higher Concurrent connections: Minimum 5 Million New sessions per second: Minimum 150000	2 Nos in HA mode (DC) - NG Firewall appliance should have at least 12 x 10/100/1000 GE interfaces, 1 HA port, 8x 10/100/1000 SFP, 2x 10G SFP+, 1x 1GE management & 1 Console interface, redundant power supplies, min 480 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 30 Gbps NGFW throughput: Minimum **10 Gbps** or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum **8 Gbps** or higher real-world App control Throughput : Minimum **8 Gbps** or higher real-world Threat Protection throughput: Minimum **8 Gbps** or higher **SSL Inspection throughput: Minimum 8 Gbps or higher** Concurrent connections: Minimum 5 Million New sessions per second: Minimum 150000	Considering Datacenter Firewall requirement some throughput parameters shall be increased to handle agentic AI related IPS & App control rules. These are perimeter firewalls which will majorly inspect internet traffic so Deep packet inspection needs to be enabled for encrypted (https) traffic on the internet so we request to add parameter of SSL Inspection Throughput as well.	Tender Conditon Prevails
50	69	2	B	03 nos (2- Kaka Nagar HA mode & 1- DR site SA mode) - NG Firewall appliance should have at least 8 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 4 Gbps or higher real-world App control Throughput : Minimum 4 Gbps or higher real-world Threat Protection throughput: Minimum 4 Gbps or higher concurrent connections: Minimum 3 Million New sessions per second: Minimum 100000	03 nos (2- Kaka Nagar HA mode & 1- DR site SA mode) - NG Firewall appliance should have at least 8 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 4 Gbps or higher real-world App control Throughput : Minimum 4 Gbps or higher real-world Threat Protection throughput: Minimum 4 Gbps or higher **SSL Inspection throughput: Minimum 4 Gbps or higher** concurrent connections: Minimum 3 Million New sessions per second: Minimum 100000	These are perimeter firewalls which will majorly inspect internet traffic so Deep packet inspection needs to be enabled for encrypted (https) traffic on the internet so we request to add parameter of SSL Inspection Throughput as well.	Tender Conditon Prevails
51	69	3	B	2 Nos in HA mode (2- IGL WTC office) - NG Firewall appliance should have at least 4 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 3 Gbps or higher real-world App control Throughput : Minimum 3 Gbps or higher real-world Threat Protection throughput: Minimum 3 Gbps or higher concurrent connections: Minimum 2 Million New sessions per second: Minimum 100000	2 Nos in HA mode (2- IGL WTC office) - NG Firewall appliance should have at least 4 x 10/100/1000 GE interfaces, 1 HA port, 4x 10/100/1000 SFP, 1x 1GE management & 1 Console interface, redundant power supplies, min 240 GB SSD internal storage, rack mountable etc. Firewall Throughput: minimum 25 Gbps NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc. IPS throughput: Minimum 3 Gbps or higher real-world App control Throughput : Minimum 3 Gbps or higher real-world Threat Protection throughput: Minimum **2.5 Gbps or higher** **SSL Inspection throughput: Minimum 2.5 Gbps or higher** concurrent connections: Minimum 2 Million New sessions per second: Minimum 100000	10/100/1000 GE interfaces asked in this location are half the capacity of Kaka Nagar and DR locations respectively the throughput can also be considered nearly half as well. These are perimeter firewalls which will majorly inspect internet traffic so Deep packet inspection needs to be enabled for encrypted (https) traffic on the internet so we request to add parameter of SSL Inspection Throughput as well.	Tender Conditon Prevails

52	58	Section	11.SCC S.no 14 Para II	During the last 5 years from the date of this RFP, the proposed Next Generation Firewall (NGFW) solution (Cisco/ Fortinet/ Checkpoint/ Palo Alto) should have been implemented in multi-site environment at least at 02 (two) organization in PSU/Government / Private / Oil & Gas Sector in India for minimum 500 employees/users in each organization. The bidder should provide purchase order copies with supporting documents.	During the last 5 years from the date of this RFP, the proposed Next Generation Firewall (NGFW) solution (Cisco/ Fortinet/ Checkpoint/ Palo Alto) should have been implemented in Single - site environment rather than Multi-site at least at 02 (two) organization in PSU/Government / Private / Oil & Gas Sector in India for minimum 500 employees/users in each organization. Justification : Many PSU/Government Education & Government Research Institutes customers do not operate on a multi-site Environment. Most of them operate from a centralized single HO site infrastructure where firewall Solutions implementation has already been successfully carried out. In view of the above, we request you to kindly amend the Special Condition Criteria from “Multi Site Environment” to “Single Site/Centralized Site Implementation” so that more experienced and capable bidders can participate in the tender. Requesting your kind consideration and approval.		Tender Condition Prevails
53			New Suggestion		Upon reviewing the RFP, we noted that the specified Firewall OEMs are restricted to Cisco, Fortinet, Check Point, and Palo Alto. We would like to formally request the inclusion of "Make in India" brands in this tender.As the OEM for DevRay (Firewalls and Switches), we possess extensive experience serving both Private and Government sectors. In alignment with the Government of India’s mandate to promote indigenous products within Govt./PSU departments, we kindly request you to allow qualified Indian OEMs to participate in this bidding process.		Tender Condition Prevails
54	10		7.4 Documents Required	Valid operational NOC/SOC certificate issued by third party authority such as Auditors / certification bodies needs to be submitted.	We have ISO Certification for our IT Operations Centre which consists of both NOC and SOC , We request to include Self certification from Service Provider along with the ISO 27000 Certificate to fulfill this requirement.		Tender Condition Prevails
55	74		II - INTERNAL FIREWALL – IGL BHAWAN (DC)	The proposed Internal NGFW must be from a different OEM than the proposed perimeter NGFW OEM.	Request to consider same OEM for both type of firewalls as this clause restricts architecture flexibility while you can Allow same OEM if logical segmentation is maintained		Tender Condition Prevails
56	5		1.0 Scope of Work	1. Bidder to supply next generation firewall appliances, central management and reporting appliance as per technical specification. Bidder may propose higher configuration appliances for all locations.	Is it mandatory to supply firewalls from a single OEM, or can we propose different OEMs for the Perimeter Firewall and Internal Firewall ?		Clarification :- As mentioned in the tender document, the Perimeter firewall OEM should be different from Internal firewall OEM. The manageability of both OEM proposed solutions should be different,.
57	72		TECHNICAL SPECIFICATIONS	H. Zero-day Prevention/ Sandboxing : The Sandboxing solution proposed by the OEM can be cloud based or appliance based solution. Cloud should be based in India if Cloud based sandboxing solution is proposed by the OEM. Solution should be provided from day-1. The Communication to cloud based sandboxing solution should be over encrypted channel.	Is it mandatory to provide the sandbox solution on the OEM cloud, or can we propose sandboxing on the bidder’s MeitY-certified private cloud ?		Clarification:- Bidder can provide sandboxing solution at OEM cloud or at IGL data center through appliance.
58			PERIMETER FIREWALL’s – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 1 Firewall Throughput: minimum 30 Gbps	We request reconsideration of the firewall performance representation clause, as throughput metrics vary significantly based on test conditions, traffic profiles, and enabled security features and all Firewall OEM's do not publish raw firewall throughput.They have application awareness natively on the firewall and hence only publish NGFW & IPS throughput. Hence request to remove this clause for wider OEM participation.		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)
59			PERIMETER FIREWALL’s – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 1 NGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc.	We Request Department to change/modify "Proposed appliance must have IPS and an Application throughput of at least 5 Gbps with Application Control, FW, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic		Tender Condition Prevails

60			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 1 IPS throughput: Minimum 7 Gbps or higher real-world	The clause is generic in terms of "higher real-world" and generally this is defined in Enterprise mix/ Application Mix. We would request the department to define exact HTTP/HTTP traffic mix (100% is recommended) so that there is no performance degradation with variation on HTTP traffic mix percentage. We Request Department to change/modify "Proposed appliance must have IPS and Application throughput of at least 4 Gbps with Application Control, FW, IPS, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic. The performance numbers must be available on public websites or datasheet or tested results on a legal letter head with Product Engineering Team.		Tender Condition Prevails
61			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 1 Concurrent connections: Minimum 5 Million	Most of the OEM based benchmarking are based on tcp/UDP flow which is layer 4 and Layer 7/http benchmarking is completely different. There is minimum 80-90% degradation when Layer 4 sessions are correlated to layer 7 session count. Request to pls. include Layer 7 benchmarking in the clause and change the clause to be " Min. 5 Mil L4 connection or 1 Mil L7 connections		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)
62			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 2 Firewall Throughput: minimum 25 Gbps	We request reconsideration of the firewall performance representation clause, as throughput metrics vary significantly based on test conditions, traffic profiles, and enabled security features and all Firewall OEM's do not publish raw firewall throughput.They have application awareness natively on the firewall and hence only publish NGFW & IPS throughput. Hence request to remove this clause for wider OEM participation.		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)
63			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 2 NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc.	We Request Department to change/modify "Proposed appliance must have IPS and Application throughput of at least 2.5 Gbps with Application Control, FW, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic. The performance numbers must be available on public websites or datasheet or tested results on a legal letter head with Product Engineering Team.		Tender Condition Prevails
64			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 2 IPS throughput: Minimum 4 Gbps or higher real-world	The clause is generic in terms of "higher real-world" and generally this is defined in Enterprise mix/ Application Mix. We would request the department to define exact HTTP/HTTP traffic mix (100% is recommended) so that there is no performance degradation with variation on HTTP traffic mix percentage. We Request Department to change/modify ""Proposed appliance must have IPS and Application throughput of at least 4 Gbps with Application Control, FW, IPS, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic . The performance numbers must be available on public websites or datasheet or tested results on a legal letter head with Product Engineering Team.POC to be conducted on the premise to validate the same during TEC"""		Tender Condition Prevails
65			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	concurrent connections: Minimum 3 Million	Most of the OEM based benchmarking are based on tcp/UDP flow which is layer 4 and Layer 7/http benchmarking is completely different. There is minimum 80-90% degradation when Layer 4 sessions are correlated to layer 7 session count. Request to pls. modify cluase as below " Min. 3 Million L4 connection or 1.0 M L7 connections		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)
66			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 3 Firewall Throughput: minimum 25 Gbps	"We request reconsideration of the firewall performance representation clause, as throughput metrics vary significantly based on test conditions, traffic profiles, and enabled security features and all Firewall OEM's do not publish raw firewall throughput.They have application awareness natively on the firewall and hence only publish NGFW & IPS throughput. Hence request to remove this clause for wider OEM participation."		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)

67			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 3 NGFW throughput: Minimum 2.5 Gbps or higher real-world inspection after after enabling IPS , app control etc.	We Request Department to change/modify "Proposed appliance must have IPS and Application throughput of at least 2.5 Gbps with Application Control, FW, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic. The performance numbers must be available on public websites or datasheet or tested results on a legal letter head with Product Engineering Team.		Tender Condition Prevails
68			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Clause: B. Hardware, Interface & Performance Requirement Pt. No. 3 IPS throughput: Minimum 3 Gbps or higher real-world	The clause is generic in terms of "higher real-world" and generally this is defined in Enterprise mix/ Application Mix. We would request the department to define exact HTTP/HTTP traffic mix (100% is recommended) so that there is no performance degradation with variation on HTTP traffic mix percentage. Also, transaction size is a mandatory attribute because packet size variation also causes lot of performance degradation on the NGFW platform We Request Department to change/modify "Proposed appliance must have IPS and Application throughput of at least 3 Gbps with Application Control, FW, IPS, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic . The performance numbers must be available on public websites or datasheet or tested results on a legal letter head with Product Engineering Team.POC to be conducted on the premise to validate the same during TEC"		Tender Condition Prevails
69			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	concurrent connections: Minimum 2 Million	"Most of the OEM based benchmarking are based on tcp/UDP flow which is layer 4 and Layer 7/http benchmarking is completely different. There is minimum 80-90% degradation when Layer 4 sessions are correlated to layer 7 session count. Request to pls. modify cluase as below Please include Layer 7 benchmarking to be " Min. 2 Mil L4 connection or 1.0 M L7 connections "		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)
70			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Firewall manager Qty. 01 - Centralized monitoring, management with sufficient number of interfaces , manage upto 10 firewall appliances.	We offer Centralized Management and Analyzer as one solution with a single license. Hence request to modify this requirement to allow OEM to have a single solution as well as multiple solution as per there licensing policy.		Clarification :- The bidder may provide one solution by meeting all the mentioned functionalities of hardware and software as per tender requirement. Furthermore, the bidder should submit the undertaking on lettrerhead regarding the same from the OEM.
71			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Firewall Analyzer Qty. 01 - Log analyzer appliance / high end server (min 16 core/ 64 Gb RAM) should have at least 2 TB storage with expansion options, minimum 10 GB logs per day capacity and sufficient number of interfaces.	We offer Centralized Management and Analyzer as one solution with a single license. Hence request to modify this requirement to allow OEM to have a single solution as well as multiple solution as per there licensing policy.		Clarification :- The bidder may provide one solution by meeting all the mentioned functionalities of hardware and software as per tender requirement. Furthermore, the bidder should submit the undertaking on lettrerhead regarding the same from the OEM.
72			PERIMETER FIREWALL's – IGL Bhawan (DC), Kaka Nagar Office, WTC Office & DR Bengaluru :-General Requirements	Recommendation	We suggest that the Firewall proposed should do complete scanning of packet & traffic and the throughput requested should not drop after scanning of complete packet & traffic. OEM should provide the undertaking regarding the same.		Tender Condition Prevails
73			INTERNAL FIREWALL – IGL BHAWAN (DC) :-General Requirements	B. Hardware, Interface & Performance Requirement S. No. 1 Firewall Throughput: minimum 30 Gbps	We request reconsideration of the firewall performance representation clause, as throughput metrics vary significantly based on test conditions, traffic profiles, and enabled security features and all Firewall OEM's do not publish raw firewall throughput.They have application awareness natively on the firewall and hence only publish NGFW & IPS throughput. Hence request to remove this clause for wider OEM participation.		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)

74			INTERNAL FIREWALL – IGL BHAWAN (DC) :- General Requirements	B. Hardware, Interface & Performance Requirement S. No. 1 NGFW throughput: Minimum 5 Gbps or higher real-world inspection after after enabling IPS , app control etc.	We Request Department to change/modify "Proposed appliance must have IPS and Application throughput of at least 5 Gbps with Application Control, FW, considering 100% HTTP/HTTPS traffic in the Enterprise Mix / Application Mix traffic. The performance numbers must be available on public websites or datasheet or tested results on a legal letter head with Product Engineering Team.		Tender Condition Prevails
75			INTERNAL FIREWALL – IGL BHAWAN (DC) :- General Requirements	B. Hardware, Interface & Performance Requirement S. No. 1 Concurrent connections: Minimum 5 Million	Most of the OEM based benchmarking are based on tcp/UDP flow which is layer 4 and Layer 7/http benchmarking is completely different. There is minimum 80-90% degradation when Layer 4 sessions are correlated to layer 7 session count. So, Please include Layer 7 benchmarking to be " Min. 5 Mil L4 connection or 1.0 M L7 connections and New sessions per second: Minimum 100000		Tender Condition Prevails (The bidder may provide any supporting document which can be verified publically or may provide undertaking from the respective OEM on their letterhead signed & stamped in compliance of the tender clause)
76			INTERNAL FIREWALL – IGL BHAWAN (DC) :- General Requirements		We suggest that the Firewall proposed should do complete scanning of packet & traffic and the throughput requested should not drop after scanning of complete packet & traffic. OEM should provide the undertaking regarding the same.		Tender Condition Prevails
77			General Requirements	Page no. 7 & Point 3.0 - DURATION OF CONTRACT / DELIVERY PERIOD / INSTALLATION AND MIGRATION	Delivery Period : The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA. Installation and migration: Installation and migration should completed within 02 weeks after the delivery of hardware.	Request to please increase the delievery time to 8 weeks and implimentaion to 6 weeks as this is multi location deployment and delieveries are taking average 8-10 weeks for the high end devices asked in the RFP	Tender Condition Prevails
78			General Requirements	Page no.80 - Buy Back	Bidder to submit the quote for the buy-back of the old security appliances and supporting devices which shall be released /handover to bidder after successful installation and migration in “As is Where is” condition without any cables/connectors , accessories etc. Bidder to arrange for the pickup of the old equipment / appliance at its own cost from the respective location. The cost of the buy-back items shall be adjusted while release the purchase order to bidder. Bidder to decommission the old devices & ensure there is not any data stored on devices. The list of the buy-back items along with the location has been attached.	Request to please remove this clause as buyback favours the existing OEM and these equipments will not be of any use by bidders who wants to quote for the other competing OEM and will give commmerical benefit to the incumbent vendor.	Tender Conditions Prevails
79			SECTION I – Invitation for Bid (IFB), Point No. 3 – TDURATION OF CONTRACT / DELIVERY PERIOD / INSTALLATION AND MIGRATION	The hardware delivery should be done within 04 weeks from the date of first notification of award/LOA.	We request you to increase the Delivery time from 04 Weeks to 12 Weeks due to Geopotical situation around the Word.		Tender Conditions Prevails
80			SECTION I – Invitation for Bid (IFB), Point No. 7.1 – Technical BEC, Point IV	The bidder should have its own operational NOC/SOC during the last five years along with a support centre in India for 24*7 support.”	for Noc/Soc requirement please consider OEM/Bidder Noc/Soc.		Tender Condition Prevails
81	10	8	4	The evaluation shall be done after deducting the quoted buyback value from the total price of SOR items and successful bidder will be declared on lowest (L1) cost basis. Tender shall be awarded to the bidder with lowest quoted amount for complete scope. Partial quotation of the SOR shall lead to rejection of bid.	Can the buyback option be removed from RFP	Fotinet firewals are already End of support from OEM. There is no use of this material for bidder. This is e-waste.	Tender Conditions Prevails
82	101		5	Power of attorney of the signatory to the bid offer on non-judicial stamp paper / Board resolution of company for authorized signatory.	can Letter of Authority be submitted instead of Power of Attorney. Kindly share format	POA is a legal document.	**Letter of authority is to be submitted along with Board resolution**

83	67	Support services from bidder - 3 years	6	Bidder to provide services during implementation & post implementation at IGL site / offices, in case of any location change or shifting of the remote site, bidder to provide necessary services at new location without any financial implication to IGL. Currently DR site is at BANGALORE, Karnataka and other sites are in NCT of Delhi.	One time charges should be paid for such shifting of location	Provision of one time charges for shifting of location	Tender Condition Prevails
84	8		I A	Single work order of at least Rs. 13.74 lakhs for supply, installation & support for enterprises class next generation firewalls appliance in previous 7 years reckoned from the date of issue of tender. OR b. Multiple orders during any 1 year in the last 7 years of at least 13.74 lakhs including at least one order for 8.24 lakhs for supply, installation & support for enterprises class next generation firewalls appliance reckoned from the date of issue of tender.	We are biding through Vodafone Idea entity name VICSL as its net worth positive, however all the relevant experince in Firewall delivery and installation is with our group entity VIL and VITSL, which are net worth negative due to AGR dues. Hence request you to cosndier showing relevant experince from of VIL and VITSL for this tender.		The bidder participating in the bid shall submit only the relevant experience of work executed by the bidding entity itself. Experience of any group entity shall not be considered Under this tender.
85	73	8		In case OEM is proposing hardware based sandboxing solution then the hardware should be provided at DC with required network ports populated from day-1. The hardware should be rack mountable and should have redundant power supplies.	Sandboxing is a passive solution which is only scanning unknown Files or URLs sent by Firewall. Firewalls are the critical & primary solution to inspect the inline traffic in real time which already have redundant power supply. In case Sandbox solution is having single power supply will not impact any production because it is only sharing verdict to Firewalls to take necessary actions. In case device Power supply is non-operational, OEM will provide 4-Hour Hardware Delivery Priority RMA Service	Need Clarification & confirmation from IGL	Clarification: Yes, the Sandboxing is passive component of the solution which scan the unknown files. There is no direct impact on Firewalls operation. The redundant supply is asked to minimize the downtime due to power supply failure. If the bidder supplied sandbox with single power supply, the device should be replaced in advancded RMA which is 6 CTR. Bidder to provide the undertaking from the respective OEM regarding the same.
86	10			7.4 Documents Required : i) Technical: 1. Single work order copy & its completion certificate defining the complete scope of work issued from the end client to the bidder duly certified by end client must be submitted along with the offer with executed value in last 7 years. 2. Copy of detailed purchase order / contract with SOR. 3. Copy of relevant document / Certificate as required in tender.	Please confirm the acceptable documentary proof for meeting the experience criteria: a. Purchase Order + Completion/Work Execution Certificate b. Client reference email, and/or c. Work Order clearly indicating firewall support/tech refresh scope.		Please refer Page 09 ; Point 7.4
87	58			11.0 SPECIAL CONDITIONS OF CONTRACT 11. The proposed firewalls must work with existing Core switch & network infra of IGL i.e. HPE devices.	RFP states proposed firewalls must work with existing HPE core/network infra—please confirm switch models, uplink types (1G/10G), and whether LACP/VLAN trunking will be used.		Clarification :- Inventory details shall be provided to the L1 bidder
88	65			1.0 Scope of Work - OEM Requirement	Please clarify, If 2 OEMs are mandatory, do you require a unified management/logging platform across both OEMs or is separate OEM console per OEM acceptable?		Clarification :- As mentioned in the tender document, the Perimeter firewall OEM should be different from Internal firewall OEM. The manageability of both OEM proposed solutions should be different,.