

## Bid Corrigendum

GEM/2025/B/6181079-C1

Following terms and conditions supersede all existing "Buyer added Bid Specific Terms and conditions" given in the bid document or any previous corrigendum. Prospective bidders are advised to bid as per following Terms and Conditions:

### Buyer Added Bid Specific Additional Terms and Conditions

1. Installation, Commissioning, Testing, Configuration, Training (if any - which ever is applicable as per scope of supply) is to be carried out by OEM / OEM Certified resource or OEM authorised Reseller.
2. Bidder Turn Over Criteria: The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March of the previous financial year, should be as indicated in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution / incorporation of the bidder is less than 3 year old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria.
3. OEM Turn Over Criteria: The minimum average annual financial turnover of the OEM of the offered product during the last three years, ending on 31st March of the previous financial year, should be as indicated in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution / incorporation of the OEM is less than 3 year old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria. In case of bunch bids, the OEM of CATEGORY RELATED TO primary product having highest bid value should meet this criterion.
4. Availability of Service Centres: Bidder/OEM must have a Functional Service Centre in the State of each Consignee's Location in case of carry-in warranty. (Not applicable in case of goods having on-site warranty). If service center is not already there at the time of bidding, successful bidder / OEM shall have to establish one within 30 days of award of contract. Payment shall be released only after submission of documentary evidence of having Functional Service Centre.
5. Dedicated /toll Free Telephone No. for Service Support : BIDDER/OEM must have Dedicated/toll Free Telephone No. for Service Support.
6. Buyer uploaded ATC document [Click here to view the file.](#)
7. Buyer Added text based ATC clauses

Payment Shall be Made after receipt of goods at site and on the production of all required documents. 100 % of Total contract value will be paid after successful installation, functional test, completion of training, commissioning and acceptance of System

The Supplier is required to complete the delivery of all items within 3 months from date of issue of supply order

LD as per RFP

## Disclaimer

The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization, whereby Buyer organization is solely responsible for the impact of these clauses

on the bidding process, its outcome, and consequences thereof including any eccentricity / restriction arising in the bidding process due to these ATCs and due to modification of technical specifications and / or terms and conditions governing the bid. If any clause(s) is / are incorporated by the Buyer regarding following, the bid and resultant contracts shall be treated as null and void and such bids may be cancelled by GeM at any stage of bidding process without any notice:-

1. Definition of Class I and Class II suppliers in the bid not in line with the extant Order / Office Memorandum issued by DPIIT in this regard.
2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.
3. Publishing Custom / BOQ bids for items for which regular GeM categories are available without any Category item bunched with it.
4. Creating BoQ bid for single item.
5. Mentioning specific Brand or Make or Model or Manufacturer or Dealer name.
6. Mandating submission of documents in physical form as a pre-requisite to qualify bidders.
7. Floating / creation of work contracts as Custom Bids in Services.
8. Seeking sample with bid or approval of samples during bid evaluation process. (However, in bids for [attached categories](#), trials are allowed as per approved procurement policy of the buyer nodal Ministries)
9. Mandating foreign / international certifications even in case of existence of Indian Standards without specifying equivalent Indian Certification / standards.
10. Seeking experience from specific organization / department / institute only or from foreign / export experience.
11. Creating bid for items from irrelevant categories.
12. Incorporating any clause against the MSME policy and Preference to Make in India Policy.
13. Reference of conditions published on any external site or reference to external documents/clauses.
14. Asking for any Tender fee / Bid Participation fee / Auction fee in case of Bids / Forward Auction, as the case may be.
15. Buyer added ATC Clauses which are in contravention of clauses defined by buyer in system generated bid template as indicated above in the Bid Details section, EMD Detail, ePBG Detail and MII and MSE Purchase Preference sections of the bid, unless otherwise allowed by GeM GTC.
16. In a category based bid, adding additional items, through buyer added additional scope of work/ additional terms and conditions/or any other document. If buyer needs more items along with the main item, the same must be added through bunching category based items or by bunching custom catalogs or bunching a BoQ with the main category based item, the same must not be done through ATC or Scope of Work.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller within 4 days of bid publication on GeM. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

\*This document shall overwrite all previous versions of Bid Specific Additional Terms and Conditions.

[This Bid is also governed by the General Terms and Conditions](#)

## MINUTES OF PRE BID MEETING HELD ON 27-05-2025 AT CONFERENCE HALL, DGM BUILDING, MAUSAM BHAWAN, IMD HQ

The India Meteorological Department (IMD) has invited bids vide Bid GEM/2025/B/6181079 dated 17.05.2025 (with latest provisions in Buyer Added Bid Specific ATC on Page 6) for procurement of 02 UTM/ Firewall of 25 Gbps. The pre bid meeting was held on 27.05.2025 and about 20 representatives from 8 prospective firms participated in the meeting. The queries received have been addressed and detailed below.

### Response to queries received from M/s Airtel

Sno	Section	Clause	Original Clause	Requested Change	IMD's Response
1	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.1 Architecture Clause 5	Minimum interface Required in Firewall: 12 x 10 G BASE-T Ethernet interfaces (RJ-45), 10 x 10 Gigabit (SFP+), 4 x 1 Gigabit.	Minimum Interface Required in Firewall: 16 x 1G BASE-T Ethernet interfaces (RJ-45), 8 x 10 Gigabit (SFP+), 8 x 1 Gigabit (SFP) with dedicated HA port	The clause has been revised as "Minimum interface required in Firewall - 8x10 G Base-T Ethernet Interfaces (RJ 45), 8x10 Gigabit (SFP+), 4x1 Gigabit"
2	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.1 Architecture Clause 8	The firewall should have minimum system memory 480 GB SSD + 2 TB additional for logs storage and minimum of 48 GB of RAM from day one.	The firewall should have minimum system memory 900 GB SSD with minimum of 32 GB of RAM from day one. Additionally, a separate on-premises solution with 2 TB of storage must be provided specifically for logging and analytics.	As per RFP only
3	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.2 Performance Clause 12	Firewall should support at least 20,00,000 concurrent sessions at L7.	Firewall should support at least 15,00,000 concurrent sessions.	As per RFP only
4	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.2 Performance Clause 13	Firewall should support at least 2,00,000 connections per second at L7.	Firewall should support at least 5,00,000 connections per second	As per RFP only



5	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.3 Firewall Features Clause 21	21. Firewall should support more than 20,000 IPS and 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Firewall should support more than 15,000 IPS and 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	The clause has been revised as "Firewall should support more than 15000 IPS and 3000 application layer and risk based controls"
6	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.3 Firewall Features Clause 34	Firewall Solution should have Standard and extended ACLs support.	As discussed during prebid, request to remove the clause	The clause has been revised as "Firewall solution should have ACL support"
7	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.6 Certification Clause 79	Firewall should be FCC Class A, CE Class A, VCCI Class A, CB, and Common Criteria Certified NDPP/NDCPP certified.	Firewall should be FCC Class A, CE Class A, VCCI Class A, CB, and Common Criteria Certified NDPP/NDCPP/EAL4 certified.	The clause has been revised as "Firewall should be FCC Class A, CE Class A, VCCI Class A, CB, and Common Criteria Certified NDPP/NDCPP/EAL4 certified"
8	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.6 Additional Provisions Clause 82	The OEM must have a "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Documentary proof to be attached.	The OEM must have a "Recommended" rating with min 95% Evasion proof capability as per 2019 NSS lab Breach Prevention Systems (BPS) report and min 90% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Documentary proof to be attached.	The clause is removed
9	Section VII: Technical Specifications and Quality Assurance Schedule 1	Item 1.6 Additional Provisions Clause 83	The OEM Protection License with updates for Application Visibility & Control, Layer3-Layer 4, NAT, Wireless, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided	The OEM Protection License with updates for Application Visibility & Control, Layer3-Layer 4, NAT, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of	The clause has been revised as "The OEM Protection License with updates for Application Visibility & Control, Layer3-Layer 4, NAT, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat

*Rashed*

*Shah*

*Shah*

*Shikany*

*Shah*



			during warranty and CAMC period of the contract.	the contract.	Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract."
10	Section Vi: Schedule of Requirement			CAMC for 1st, 2nd and 3rd year. Is a dedicated resource required for Support and monitoring? What all is expected in CAMC	A dedicated resource is not mandatory. During complaints SLA should be maintained. Secondly, the quarterly performance monitoring report should be submitted as per RFP.

### Response to queries received from M/s. Saffron Networks

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
11	5	Minimum Interface Required on the Firewall 12X 10G BASE T Ethernet Interface (RJ45) 10X10G Gigabit (SFP+) 4 X 1 Gigabit	Minimum Interface Required on the Firewall : 8X 10G BASE T Ethernet Interface (RJ45) 4X10G Gigabit (SFP+) 4 X 1 Gigabit	Refer to SNo 1
12	7	The firewall should include perpetual license to meet all the required RFP specifications without any dependency on the Internet during the warranty and AMC period.	The firewall should include perpetual/ subscription based license to meet all the required RFP specifications without any dependency on the Internet ( other than for update and threat intel) during the warranty and AMC period.	The clause has been revised as  "The firewall should include perpetual/ subscription based license to meet all the required RFP specifications without any dependency on the Internet ( other than for update and threat intel) during the warranty and AMC period without any financial implications to the purchaser (IMD)"

Rashid

Shikhar

SM

Shikhar

Shikhar

13	8	The firewall should have minimum system memory 480GB SSD + 2TB additional for logs storage and minimum 48GB of RAM from day 1.	The firewall solution should have a minimum memory of 900 GB from day one with capability to integrate with external storage like syslog and minimum 48GB of RAM from day 1.	Refer to SNo 2
14	35	Firewall solution should support AAA and RADIUS , TACACS+ authentication	Firewall solution should support AAA and RADIUS /TACACS+ authentication	The clause has been revised as "Firewall solution should support AAA and RADIUS /TACACS+ authentication"
15	37	Firewall should incorporate Sandbox solution license and should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript. Adobe Flash files. MAC OS and DMG file types.	Firewall should incorporate Sandbox solution license and should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript. Adobe Flash files.	The clause has been revised as " Firewall should incorporate Sandbox solution license and should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript. Adobe Flash files"
16	53	Firewall Solution should block web plug-ins such as ActiveX, Java Applet, and Cookies.	Please remove the clause	As per RFP only
17	78	Firewall should obtain minimum ICASA certification	Firewall should obtain minimum ICASA certification or equivalent	This clause is removed
18	82	The OEM must have "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Documentary proof to be attached.	As discussed during prebid, request to remove the clause	Refer to SNo 8

*Prasanth*

*Shikhar*

*(Signature)*

*Shikhar*

*(Signature)*

19	83	The OEM Protection License with updates for Application Visibility & Control, Layer3 - Layer 4. NAT, Wireless, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract.	The OEM Protection License with updates for Application Visibility & Control, Layer3 - Layer 4. NAT, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract.	Refer to SNo 9
----	----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------

### Response to Email received from M/s. Check Point

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
20	5	Minimum interface required in Firewall - 12x10 G Base-T Ethernet Interfaces (RJ 45), 10x10 Gigabit (SFP+), 4x1 Gigabit	"Minimum interface required in Firewall - 8x10 G Base-T Ethernet Interfaces (RJ 45), 8x10 Gigabit (SFP+), 4x1 Gigabit"	Refer to SNo 1
21	7	The Firewall solution should include perpetual licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	" The Firewall solution should include perpetual/subscription licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	Refer to SNo 12
22	8	The Firewall should have minimum system memory 480 GB SSD+ 2TB additional for logs storage and minimum of 48 GB of RAM from day 1.	" The Firewall should have minimum system memory 950 GB SSD & minimum 2 TB storage at centralized management for log storage and minimum of 48 GB of RAM from day 1 & RAM should be expandable to 64 GB for future requirement in same appliance."	Refer to SNo 2



23	10	The Firewall Throughput with all services enable should support minimum 25 GBPS real-world/ production/ Enterprise Testing Performance/ or with 64 Bytes of packets NGFW (FW, IPS, VPN Web filtering) performance throughput or higher.	" The Firewall Throughput with all services enable should support minimum 50 Gbps real-world/ production/ Enterprise Testing Performance."	As per RFP only
24	11	Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malware, File blocking, advanced DNS security and logging security threat protection features enabled - minimum 15 Gbps considering 95% HTTP/ Application mix flows with 64 KB transaction size.	" Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malwar, URL Filtering, DNS security and logging security threat protection features enabled - minimum 15 Gbps in Enterprise Testing Condition."	As per RFP only
25	12	Firewall should support at least 2000000 concurrent session at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least 6000000 concurrent session at Layer 7".	Refer to SNo 3
26	13	Firewall should support at least 200000 connection per second at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least Firewall should support at least 500000 connection per second at Layer 7".	Refer to SNo 4
27	20	Firewall should be capable of dynamically tuning IPS sensors (e.g. selection rules, configuration policies, updation policies) with minimal human intervention.	As discussed during prebid, request to remove the clause	This clause is removed
28	21	Firewall should support more than 20000 IPS and 3000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	" Firewall should support more than 15000 IPS and 10000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Refer to SNo 5

*Reshant*

*Shilpa*

*Shikhar*

*Shikhar*

*Shikhar*






29	46	The firewall should support for SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall should support for SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	This clause has been revised as "The firewall should support for SSL VPN tunnel mode that supports all major operating system like Windows Linux"
30	47	The firewall systems should provide SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall systems should provide SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	This clause has been revised as "The firewall systems should provide SSL VPN tunnel mode that supports all major operating system like Windows Linux"
31	61	Firewall solutions should provide on devices as well as centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/machine with the required software license bundle from day one	Firewall solutions should provide on devices or centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/physical with the required software license bundle along with hardware in case of virtual appliance from day one	Agreed subject to arranging of all H/W and S/W for centralised management console without any financial liability to the purchaser.
32	71	Bidder may provide the additional hardware/software to achieve complete visibility, automation and centralised management of the devices along with other features specified under monitoring management and upgradation	" Bidder may provide the additional hardware/software to achieve complete visibility, monitoring and centralised management of the devices along with other features specified under monitoring management and upgradation"	This clause has been revised as "Bidder may provide the additional hardware/software to achieve complete visibility, monitoring and centralised management of the devices along with other features specified under monitoring management and upgradation"
33	83	The OEM protection license with update for application visibility & control, Layer 3-Layer 4, NAT, wireless, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam	The OEM protection license with update for application visibility & control, Layer 3-Layer 4, NAT, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and	Refer to SNo 9



		to be provided during warranty and CAMC period of the contract	CAMC period of the contract	
--	--	----------------------------------------------------------------	-----------------------------	--

## Response to Email received from M/s. CISCO

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
34	5	Minimum Interface Required on the Firewall 12X 10G BASE T Ethernet Interface (RJ45) 10X10G Gigabit (SFP+) 4 X 1 Gigabit	Minimum Interface Required on the Firewall : 8X 10G BASE T Ethernet Interface (RJ45) 4X10G Gigabit (SFP+) 4 X 1 Gigabit	Refer to SNo 1
35	7	The firewall should include perpetual license to meet all the required RFP specifications without any dependency on the Internet during the warranty and AMC period.	The firewall should include perpetual/ subscription based license to meet all the required RFP specifications without any dependency on the Internet ( other than for update and threat intel) during the warranty and AMC period.	Refer to SNo 12
36	8	The firewall should have minimum system memory 480GB SSD + 2TB additional for logs storage and minimum 48GB of RAM from day 1.	The firewall solution should have a minimum memory of 900 GB from day one and minimum 48GB of RAM from day 1.	Refer to SNo 2
37	35	Firewall solution should support AAA and RADIUS , TACACS+ authentication	Firewall solution should support AAA and RADIUS /TACACS+ authentication	Refer to SNo 14
38	37	Firewall should incorporate Sandbox solution license and should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like	Firewall should incorporate Sandbox solution license and should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript. Adobe Flash files.	Refer to SNo 15



		JavaScript. Adobe Flash files. MAC OS and DMG file types.		
39	53	3. Firewall Solution should block web plug-ins such as ActiveX, Java Applet, and Cookies.	Please remove the clause, The asked capability is a very old technology blocked by default by web browsers and is hence irrelevant in today's time.	Refer to SNo 16
40	78	Firewall should obtain minimum ICSA certification	As discussed during prebid, request to remove the clause	Refer to SNo 17
41	82	The OEM must have "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Documentary proof to be attached.	As discussed during prebid, request to remove the clause	Refer to SNo 8
42	83	The OEM Protection License with updates for Application Visibility & Control, Layer3 - Layer 4. NAT, Wireless, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract.	The OEM Protection License with updates for Application Visibility & Control, Layer3 - Layer 4. NAT, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract.	Refer to SNo 9

### Response to Email received from M/s. Aura Emanating Teknology

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
43	5	Minimum interface required in Firewall - 12x10 G Base-T Ethernet Interfaces (RJ 45), 10x10 Gigabit (SFP+), 4x1 Gigabit	"Minimum interface required in Firewall - 8x10 G Base-T Ethernet Interfaces (RJ 45), 8x10 Gigabit (SFP+), 4x1 Gigabit	Refer to SNo 1

44	7	The Firewall solution should include perpetual licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	As per industry standard majority of leading OEM offers subscription model only, Hence we request to please modify this point as " The Firewall solution should include perpetual/subsorption licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	Refer to SNo 12
45	8	The Firewall should have minimum system memory 480 GB SSD+ 2TB additional for logs storage and minimum of 48 GB of RAM from day 1.	As per industry standard majority of leading OEM offers fixed SSD options in firewall, for addtional logs storage centralized management is leveraged, Hence we request to please modify this point as " The Firewall should have minimum system memory 950 GB SSD & minimum 2 TB storage at centralized management for log storage and minimum of 48 GB of RAM from day 1 & RAM should be expandable to 64 GB for future requirement in same appliance."	Refer to SNo 2
46	10	The Firewall Throughput with all services enable should support minimum 25 GBPS real-world/ production/ Enterprise Testing Performance/ or with 64 Bytes of packets NGFW (FW, IPS, VPN Web filtering) performance throughput or higher.	" The Firewall Throughput with all services enable should support minimum 50 Gbps real-world/ production/ Enterprise Testing Performance."	Refer to SNo 23
47	11	Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malware, File blocking, advanced DNS security and logging security threat protection features enabled - minimum 15 Gbps considering 95% HTTP/ Application mix flows with 64 KB transaction size.	" Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malwar, URL Filtering, DNS security and logging security threat protection features enabled - minimum 15 Gbps in Enterprise Testing Condition."	Refer to SNo 24
48	12	Firewall should support at least 2000000 concurrent session at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least 6000000 concurrent session at Layer 7".	Refer to SNo 3
49	13	Firewall should support at least 200000 connection per second at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least Firewall should support at least 500000 connection per second at Layer 7".	Refer to SNo 4



50	20	Firewall should be capable of dynamically tuning IPS sensors (e.g. selection rules, configuration policies, updation policies) with minimal human intervention.	As discussed during prebid, request to remove the clause	Refer to SNo 27
51	21	Firewall should support more than 20000 IPS and 3000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Firewall should support more than 15000 IPS and 10000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Refer to SNo 5
52	46	The firewall should support for SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall should support for SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 29
53	47	The firewall systems should provide SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall systems should provide SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 30
54	61	Firewall solutions should provide on devices as well as centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/machine with the required software license bundle from day one	"Firewall solutions should provide on devices or centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/physical with the required software license bundle along with hardware in case of virtual appliance from day one	Refer to SNo 31
55	71	Bidder may provide the additional hardware/software to achieve complete visibility, automation and centralised management of the devices along with other features specified under monitoring management and upgradation	Bidder may provide the additional hardware/software to achieve complete visibility, monitoring and centralised management of the devices along with other features specified under monitoring management and upgradation	Refer to SNo 32
56	83	The OEM protection license with update for application visuality & control, Layer 3-Layer 4, NAT, wireless, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Wireless is not a feature of Enterprise firewall, hence we request to please modify this point as The OEM protection license with update for application visuality & control, Layer 3-Layer 4, NAT, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Refer to SNo 9



## Response to Email received from M/s. Resseaux Technology Pvt. Ltd.

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
57	5	Minimum interface required in Firewall - 12x10 G Base-T Ethernet Interfaces (RJ 45), 10x10 Gigabit (SFP+), 4x1 Gigabit	"Minimum interface required in Firewall - 8x10 G Base-T Ethernet Interfaces (RJ 45), 8x10 Gigabit (SFP+), 4x1 Gigabit"	Refer to SNo 1
58	7	The Firewall solution should include perpetual licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	" The Firewall solution should include perpetual/subscription licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period."	Refer to SNo 12
59	8	The Firewall should have minimum system memory 480 GB SSD+ 2TB additional for logs storage and minimum of 48 GB of RAM from day 1.	As per industry standard majority of leading OEM offers fixed SSD options in firewall, for additional logs storage centralized management is leveraged, Hence we request to please modify this point as " The Firewall should have minimum system memory 950 GB SSD & minimum 2 TB storage at centralized management for log storage and minimum of 48 GB of RAM from day 1 & RAM should be expandable to 64 GB for future requirement in same appliance."	Refer to SNo 2
60	10	The Firewall Throughput with all services enable should support minimum 25 GBPS real-world/ production/ Enterprise Testing Performance/ or with 64 Bytes of packets NGFW (FW, IPS, VPN Web filtering) performance throughput or higher.	" The Firewall Throughput with all services enable should support minimum 50 Gbps real-world/ production/ Enterprise Testing Performance."	Refer to SNo 23
61	11	Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malware, File blocking, advanced DNS security and logging security threat protection features enabled - minimum 15 Gbps considering	" Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malwar, URL Filtering, DNS security and logging security threat protection features enabled - minimum 15 Gbps in Enterprise Testing Condition."	Refer to SNo 24

		95% HTTP/ Application mix flows with 64 KB transaction size.		
62	12	Firewall should support at least 2000000 concurrent session at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least 6000000 concurrent session at Layer 7".	Refer to SNo 3
63	13	Firewall should support at least 200000 connection per second at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least Firewall should support at least 500000 connection per second at Layer 7".	Refer to SNo 4
64	20	Firewall should be capable of dynamically tuning IPS sensors (e.g. selection rules, configuration policies, updation policies) with minimal human intervention.	As discussed during prebid, request to remove the clause	Refer to SNo 27
65	21	Firewall should support more than 20000 IPS and 3000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	"Firewall should support more than 15000 IPS and 10000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Refer to SNo 5
66	46	The firewall should support for SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall should support for SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 29
67	47	The firewall systems should provide SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall systems should provide SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 30
68	61	Firewall solutions should provide on devices as well as centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/machine with the required software license bundle from day one	" Firewall solutions should provide on devices or centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/physical with the required software license bundle along with hardware in case of virtual appliance from day one	Refer to SNo 31
69	71	Bidder may provide the additional hardware/software to achieve complete visibility, automation and centralised management of the devices along with other features specified under monitoring management and upgradation	" Bidder may provide the additional hardware/software to achieve complete visibility, monitoring and centralised management of the devices along with other features specified under monitoring management and upgradation"	Refer to SNo 32









70	83	The OEM protection license with update for application visibility & control, Layer 3-Layer 4, NAT, wireless, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Wireless is not a feature of Enterprise firewall, hence we request to please modify this point as The OEM protection license with update for application visibility & control, Layer 3-Layer 4, NAT, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Refer to SNo 9
----	----	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------

### Response to Email received from M/s. Esconet Technology

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
71	5	Minimum interface required in Firewall - 12x10 G Base-T Ethernet Interfaces (RJ 45), 10x10 Gigabit (SFP+), 4x1 Gigabit	"Minimum interface required in Firewall - 8x10 G Base-T Ethernet Interfaces (RJ 45), 8x10 Gigabit (SFP+), 4x1 Gigabit"	Refer to SNo 1
72	7	The Firewall solution should include perpetual licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	" The Firewall solution should include perpetual/subscription licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	Refer to SNo 12
73	8	The Firewall should have minimum system memory 480 GB SSD+ 2TB additional for logs storage and minimum of 48 GB of RAM from day 1.	" The Firewall should have minimum system memory 950 GB SSD & minimum 2 TB storage at centralized management for log storage and minimum of 48 GB of RAM from day 1 & RAM should be expandable to 64 GB for future requirement in same appliance."	Refer to SNo 2



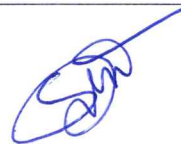










74	10	The Firewall Throughput with all services enable should support minimum 25 GBPS real-world/ production/ Enterprise Testing Performance/ or with 64 Bytes of packets NGFW (FW, IPS, VPN Web filtering) performance throughput or higher.	" The Firewall Throughput with all services enable should support minimum 50 Gbps real-world/ production/ Enterprise Testing Performance."	Refer to SNo 23
75	11	Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malware, File blocking, advanced DNS security and logging security threat protection features enabled - minimum 15 Gbps considering 95% HTTP/ Application mix flows with 64 KB transaction size.	" Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malwar, URL Filtering, DNS security and logging security threat protection features enabled - minimum 15 Gbps in Enterprise Testing Condition."	Refer to SNo 24
76	12	Firewall should support at least 2000000 concurrent session at L7.	" Firewall should support at least 6000000 concurrent session at Layer 7".	Refer to SNo 3
77	13	Firewall should support at least 200000 connection per second at L7.	" Firewall should support at least Firewall should support at least 500000 connection per second at Layer 7".	Refer to SNo 4
78	20	Firewall should be capable of dynamically tuning IPS sensors (e.g. selection rules, configuration policies, updation policies) with minimal human intervention.	As discussed in prebid, request to please remove this point.	Refer to SNo 27
79	21	Firewall should support more than 20000 IPS and 3000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Firewall should support more than 15000 IPS and 10000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Refer to SNo 5
80	46	The firewall should support for SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall should support for SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 29
81	47	The firewall systems should provide SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall systems should provide SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 30



82	61	Firewall solutions should provide on devices as well as centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/machine with the required software license bundle from day one	" Firewall solutions should provide on devices or centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/physical with the required software license bundle along with hardware in case of virtual appliance from day one	Refer to SNo 31
83	71	Bidder may provide the additional hardware/software to achieve complete visibility, automation and centralised management of the devices along with other features specified under monitoring management and upgradation	" Bidder may provide the additional hardware/software to achieve complete visibility, monitoring and centralised management of the devices along with other features specified under monitoring management and upgradation"	Refer to SNo 32
84	83	The OEM protection license with update for application visuality & control, Layer 3-Layer 4, NAT, wireless, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Wireless is not a feature of Enterprise firewall, hence we request to please modify this point as The OEM protection license with update for application visuality & control, Layer 3-Layer 4, NAT, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Refer to SNo 9

### Response to Email received from M/s. Cyber Force Digital

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
85	5	Minimum interface required in Firewall - 12x10 G Base-T Ethernet Interfaces (RJ 45), 10x10 Gigabit (SFP+), 4x1 Gigabit	"Minimum interface required in Firewall - 8x10 G Base-T Ethernet Interfaces (RJ 45), 8x10 Gigabit (SFP+), 4x1 Gigabit"	Refer to SNo 1
86	7	The Firewall solution should include perpetual licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	" The Firewall solution should include perpetual/subscription licenses to meet all the required RFP specification without any dependency on the internet during warranty and CAMC period.	Refer to SNo 12

*Handwritten signature*

*Handwritten signature*

*Handwritten signature*

*Handwritten signature*

*Handwritten signature*



87	8	The Firewall should have minimum system memory 480 GB SSD+ 2TB additional for logs storage and minimum of 48 GB of RAM from day 1.	" The Firewall should have minimum system memory 950 GB SSD & minimum 2 TB storage at centralized management for log storage and minimum of 48 GB of RAM from day 1 & RAM should be expandable to 64 GB for future requirement in same appliance."	Refer to SNo 2
88	10	The Firewall Throughput with all services enable should support minimum 25 GBPS real-world/ production/ Enterprise Testing Performance/ or with 64 Bytes of packets NGFW (FW, IPS, VPN Web filtering) performance throughput or higher.	The Firewall Throughput with all services enable should support minimum 50 Gbps real-world/ production/ Enterprise Testing Performance."	Refer to SNo 23
89	11	Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malware, File blocking, advanced DNS security and logging security threat protection features enabled - minimum 15 Gbps considering 95% HTTP/ Application mix flows with 64 KB transaction size.	Minimum NGFW Threat protection throughput by enabling and measured with Application-ID/AVC/, User ID/ Agent ID/ NGIPS/, Antivirus, Anti- spyware, Anti Malwar, URL Filtering, DNS security and logging security threat protection features enabled - minimum 15 Gbps in Enterprise Testing Condition."	Refer to SNo 24
90	12	Firewall should support at least 2000000 concurrent session at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least 6000000 concurrent session at Layer 7".	Refer to SNo 3
91	13	Firewall should support at least 200000 connection per second at L7.	For optimal sizing and performance we request to please modify this point as" Firewall should support at least Firewall should support at least 500000 connection per second at Layer 7".	Refer to SNo 4
92	20	Firewall should be capable of dynamically tuning IPS sensors (e.g. selection rules, configuration policies, updation policies) with minimal human intervention.	As discussed during prebid, request to remove the clause	Refer to SNo 27
93	21	Firewall should support more than 20000 IPS and 3000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	" Firewall should support more than 15000 IPS and 10000 application layer risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Refer to SNo 5



94	46	The firewall should support for SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall should support for SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 29
95	47	The firewall systems should provide SSL VPN tunnel mode that supports all operating systems.	We request to please modify this point as" The firewall systems should provide SSL VPN tunnel mode that supports all known OS like Windows, macOS, and Linux .	Refer to SNo 30
96	61	Firewall solutions should provide on devices as well as centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/machine with the required software license bundle from day one	" Firewall solutions should provide on devices or centralised management and recruiting solution with complete feature priority on firewall administration the central management and reporting solutions should be a dedicated OEM appliance virtual/physical with the required software license bundle along with hardware in case of virtual appliance from day one	Refer to SNo 31
97	71	Bidder may provide the additional hardware/software to achieve complete visibility, automation and centralised management of the devices along with other features specified under monitoring management and upgradation	Bidder may provide the additional hardware/software to achieve complete visibility, monitoring and centralised management of the devices along with other features specified under monitoring management and upgradation"	Refer to SNo 32
98	83	The OEM protection license with update for application visibility & control, Layer 3-Layer 4, NAT, wireless, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Wireless is not a feature of Enterprise firewall, hence we request to please modify this point as The OEM protection license with update for application visibility & control, Layer 3-Layer 4, NAT, IPS, user identity, VPN (IPSEC and SSL for the user mentioned) Web security essential/URL filtering. Advanced Malware/Threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract	Refer to SNo 9

*Rashid*

*Shilpa*

*[Signature]*

*Shikhar*

*[Signature]*

## Response to Email received from M/s. Fortinet

S. No.	Clause No.	Technical Specification	Suggested Change	IMD's Response
99	Item 1.1 Architecture Clause 5	Minimum interface Required in Firewall: 12 x 10 G BASE-T Ethernet interfaces (RJ-45), 10 x 10 Gigabit (SFP+), 4 x 1 Gigabit.	Minimum Interface Required in Firewall: 12 x 1G BASE-T Ethernet interfaces (RJ-45), 8 x 1G /10 SFP+ ports	Refer to SNo 1
100	Item 1.1 Architecture Clause 8	The firewall should have minimum system memory 480 GB SSD + 2 TB additional for logs storage and minimum of 48 GB of RAM from day one.	The firewall should have minimum system memory of 32 GB of RAM from day one. The solution should provide on-premise 4 TB additional for logs storage.	Refer to SNo 2
101	Item 1.2 Performance Clause 12	Firewall should support at least 20,00,000 concurrent sessions at L7.	Firewall should support at least 2 Million concurrent sessions.	Refer to SNo 3
102	Item 1.2 Performance Clause 13	Firewall should support at least 2,00,000 connections per second at L7.	Firewall should support at least 2,00,000 connections per second.	Refer to SNo 4
103	Item 1.3 Firewall Features Clause 21	21. Firewall should support more than 20,000 IPS and 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Firewall should support more than 15,000 IPS and 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.	Refer to SNo 5
104	Item 1.3 Firewall Features Clause 34	Firewall Solution should have Standard and extended ACLs support.	Firewall Solution should have ACL support.	Refer to SNo 6

*For Shah*

*Amir Khan*

*Salim*

*Shikhar*

*Shah*

105	Item 1.6 Certification Clause 79	Firewall should be FCC Class A, CE Class A, VCCI Class A, CB, and Common Criteria Certified NDPP/ND CPP certified.	Firewall should be FCC Class A, CE Class A, VCCI Class A, CB, and Common Criteria Certified DPP/ND CPP/EAL4 certified.	Refer to SNo 7
106	Item 1.6 Additional Provisions Clause 82	The OEM must have a "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Documentary proof to be attached.	The OEM must have a "Recommended" rating with min 95% Evasion proof capability as per 2019 NSS lab Breach Prevention Systems (BPS) report and min 90% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Documentary proof to be attached.	Refer to SNo 8
107	Item 1.6 Additional Provisions Clause 83	The OEM Protection License with updates for Application Visibility & Control, Layer3-Layer 4, NAT, Wireless, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract.	The OEM Protection License with updates for Application Visibility & Control, Layer3-Layer 4, NAT, IPS, User Identity, VPN (IPSEC & SSL-for the users mentioned), Web Security Essentials/URL Filtering, Advance Malware/threat Protection, Antivirus, Antispam to be provided during warranty and CAMC period of the contract.	Refer to SNo 9

### Response to Email received from M/s. Velocis Systems

S. No.	Clause	Section/Chapter	RFP Page No.	Change Request	IMD's Response
108	Relevant Eligible Experience  Number of UTM / Firewall deployments of value at least Rs. 1 Cr and above (single order) each completed in last 5 years from the date of publishing of this RFP	Section VIII: Qualification Criteria Table A (TCM)	112	Kindly amend/modify as - "Number of UTM / Firewall deployments of value at least Rs. 1 Cr and above (single order) each completed in last 7 years from the date of publishing of this RFP in India/Globally"	As per RFP



109	Experience in successfully completing network security implementations / installation specifically related to UTM/Firewall in PSU / Govt. organisations in the last 3 years in India/Globally.	Section VIII: Qualification Criteria Table A (TCM)	112	Kindly amend/modify as - "Experience in successfully completing network security implementations / installation specifically related to UTM/Firewall in PSU / Govt. organisations in the last 7 years from the date of publishing of this RFP in India/Globally. "	As per RFP
110	Performance Security - Applicable at 10% of the Order Value	10.0 Documents relating to Bid Security (ITB Clause 9.4) and Performance Security (ITB Clause 13.2.4)	8	Request to change the same to @5% as mentioned as e-PBG percentage of GeM Bid No. GEM/2025/B/6181079	As per latest GFR rules, this may be treated as 5%
111	EMD - Applicable @ 2% of Order Value	10.0 Documents relating to Bid Security (ITB Clause 9.4) and Performance Security (ITB Clause 13.2.4)	8	Kindly confirm exemption of EMD in line with exemption clauses mentioned at Page 18, 19, 20 of General Terms and Conditions on GeM 4.0 (Version 1.24) dt 5th May 2025 - governing this bid. Kindly also refer in GeM Bid No. GEM/2025/B/6181079 - Disclaimer 2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.	As per latest rules.

Shikhar

Roshal

Shikhar

Shikhar

Shikhar

## Response to Email received from M/s. Arch Network Technologies

S. No.	Clause	Section/Chapter	RFP Page No.	Change Request	IMD's Response
112	Number of UTM/Firewall deployment of value atleast Rs.1 Cr and above (single order) each completed in last 5 years from the date of publishing of RFP.	Section VIII: Qualification Criteria Table A (TCM)	112	Kindly amend/modify as - Number of UTM/Firewall deployments with a value of at least Rs. 25 Lakh (single order), each completed within the last 7 years from the date of publishing of the RFP, either in India or globally.	Please see response at Sno 108
113	Experience I successfully completing network security implementation / installation specifically related to UTM/Firewall in PSU/Govt. organisations in the last 3 years in India/globally.	Section VIII: Qualification Criteria Table A (TCM)	112	Kindly amend/modify as- Experience I successfully completing network security implementation / installation specifically related to UTM/Firewall in PSU/Govt. organisations in the last 7 years in India/globally.	Please see response at Sno 109
114	Performance Security - Applicable at 10% of the order value	10.0 Document related to Bid Security (ITB Clause 9.4) and performance security (ITB Clause 13.2.4)	8	Request to change the same to @5% as mentioned as ePBG percentage of Gem Bid No. GEM/2025/B/6181079	Please see response at Sno 110
115	EMD - Applicable @ 2% of Order value	10.0 Document related to Bid Security (ITB Clause 9.4) and performance security (ITB Clause 13.2.4)	8	Kindly confirm exemption of EMD in line with exemption clause mentioned at Page 18, 19, 20 of General terms and condition on Gem4.0 (Version 1.24) dt. 25th May 2025 - governing this bid.  Kindly also refer in GeM Bid No. GEM/2025/B/6181079 - Disclaimer 2. Seeking EMD submission from bidder (s), including via Additional Term & Conditions.	Please see response at Sno 111

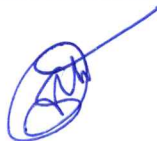
## Response to Email received from M/s. Esconet

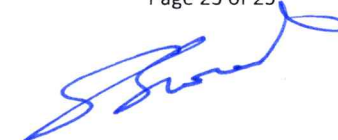
S. No.	Clause	Change Request	IMD's Response
116	Number of UTM/ Firewall deployments of value at least Rs.1Cr. & above (single order) each completed in last 5 years from the date of publishing of this RFP.	Number of UTM/ Firewall/ WAF deployments of value at least Rs.1Cr. & above (single order) each completed in last 5 years from the date of publishing of this RFP.	Please see response at Sno 108
117	Experience in successfully completing network security implementations/ installation specifically related to UTM/ Firewall in PSU/ Govt. organizations in the last 3 years in India/ Globally.	Experience in successfully completing network security implementations/ installation specifically related to UTM/ Firewall/WAF in PSU/ Govt. organizations in the last 3 years in India/ Globally.	Please see response at Sno 109

## Response to Email received from M/s. Resseaux Tech

S. No.	Clause	Change Request	IMD's Response
118	Number of UTM / Firewall deployments of value at least Rs. 1 Cr. & above (Single Order) each completed in the last 5 years from the date of publishing of this RFP.	Number of UTM / Firewall deployments of value at least Rs. 1 Cr. & above (Single Order) each completed in the last 7 years from the date of publishing of this RFP.	Please see response at Sno 108
119	Experience in successfully completing network security implementations / installation specifically related to UTM/Firewall in PSU/Govt. organizations in the last 3 years in India/Globally.	Experience in successfully completing network security implementations / installation specifically related to UTM/Firewall in PSU/Govt. organizations in the last 7 years in India/Globally.	Please see response at Sno 109









120	Number of qualified experts in network security and UTM/Firewall solutions employed from last 3 years in same organization. Min. 2 experts: 05 marks 3-5 experts: 08 marks >5 experts: 10 marks	The clause regarding certification specific to one OEM needs to be removed, as no firewall OEM certifies an engineer for having certifications from different OEMs for their respective hardware. So, having certification from a particular OEM doesn't mean that the certified person is certified for other OEM's hardware also	As per RFP
121	MII Purchase Preference	Gartner Firewall does not fall under MII with this specification.	The marks against this clause will be awarded to each participating bidder/vendor.

### Representation through GEM on Bid Number: GEM/2025/B/6181079

GeM Query No	Bid/RA Section	Seller Query/Representation	IMD's Response
1	Section VII Clause 5	Respected Officials, 1. Regarding Point No. 8 of Item 1.1 (Architecture) in the technical specifications of the firewall:- Could you kindly clarify the requirement for the additional 2 TB of storage? Is this storage intended to be integrated into the firewall in addition to the existing 480 GB SSD, or is it required as a separate device?	Agreed, If external all the HW and SW for accessibility to be provided by the bidder without any financial implications to the purchaser.
2		Regarding Point No. 61 of Item 1.7 (Monitoring, Management, and Upgradation) in the technical specifications of the firewall:- A centralized management and reporting solution is typically necessary when managing five or more firewalls from the same OEM. Since this project involves only two firewalls, such a solution does not appear necessary. Moreover, the Bill of Quantities (BoQ) does not mention a separate central management solution. Including it would unnecessarily increase the overall cost of the solution. Therefore, we kindly request the removal of this clause from the technical specifications.	Refer to SNo 31
3		Regarding Point No. 82 of Item 1.10 in the technical specifications of the firewall:- We respectfully request the reconsideration and removal of the NSS Labs testing requirement	Refer to SNo 8

*Prashant*

*[Signature]*

*[Signature]*

*Shikhar*

*[Signature]*

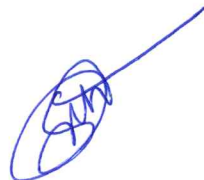
		<p>from the evaluation criteria. It is important to note that NSS Labs ceased operations in 2019. Consequently, the certification standards they issued are now outdated and no longer reflect the current landscape of evolving cyber threats and attack methodologies.</p> <p>Furthermore, we would like to highlight that local suppliers and Indian Cyber Security Product companies are exempt from foreign/international standard certifications, such as 'NSS Labs,' in accordance with Clause 8 of the Public Procurement (Preference to Make in India) Order, 2019, pertaining to Cyber Security Products.</p>	
4		The firewall device should be compatible with existing network types of equipment. Please confirm what type of existing devices are there?	The logical diagram has been attached in Annexure 1 of the tender document.
5		<p>Minimum interface required in Firewall:</p> <p>12 x 10 G BASE-T Ethernet Interfaces (RJ-45)</p> <p>10 x 10 Gigabit (SFP+)</p> <p>4 x 1 Gigabit</p> <p>Please confirm port numbers once</p>	Refer to SNo 1
6		The Firewall should have minimum system memory 480 GB SSD + 2 TB for additional for logs storage and minimum of 48 GB of RAM from day 1.	Refer to SNo 2



(Shri Prashant Bansal)



(Shri Amul Batra)



(Dr Sankar Nath)



(Shri Sourav Adhikary)



(Dr G. Suresh)